

DRAFT - Qualitative Assessment Framework

Introduction:

This draft framework outlines the NRC staff's initial thoughts on providing guidance for an improved qualitative assessment process that takes into account differences in the level of evidence needed for SSCs of varying safety significance. The NRC staff recognizes that greater clarity in guidance for documenting the technical basis supporting proposed digital I&C modifications to SSCs of lower safety significance under 10 CFR 50.59 is needed.

The term "qualitative assessment" is referenced in both NEI 96-07 (as endorsed by RG 1.187) and NEI 01-01 (as endorsed by RIS 2002-22). For example, Section 5.3.1 of NEI 01-01 states, in part, that "...reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features". Reliance on high quality development or design processes alone may not always serve as a sufficient qualitative argument. The intent of this supplemental guidance is to enable licensees to ensure that adequate qualitative arguments are presented consistently, through an evaluation of all appropriate qualitative evidence available. As I have commented before: Qualitative evidence is sufficient to conclude that the likelihood of a CCF is significantly less than that of a single failure, thereby concluding (1) the CCF is beyond design basis and (2) enabling the use of best estimate methods and acceptance criteria for the CCF malfunction result analysis. But deterministic evidence (e.g., 100% testability, internal diversity) is needed to conclude that a CCF is not credible, thereby precluding any further consideration of the CCF (i.e., no need for a CCF malfunction result analysis). If you allow qualitative evidence alone to reach a CCF not credible conclusion then you are in conflict with the SRM to SECY 93-087, BTP 7-19 and NUREG 6303.], and the use of a consistent format and rationale by which the evidence supports the conclusions needed to respond to the criteria within a 10 CFR 50.59 evaluation.

Purpose:

This enclosure to RIS 2017-XX provides guidance for performing and documenting qualitative assessments developed in support of 10 CFR 50.59 evaluations of proposed digital I&C plant modifications. Such qualitative assessments are needed to document the technical bases for concluding whether there is reasonable assurance that any failures or failure modes due to the implementation of the proposed digital I&C modification are as likely, or significantly less likely to occur as failures and failure modes already considered in the plant safety analysis. I agree with this statement, because this statement does not allow the use of qualitative assessments to reach a CCF not credible conclusion; it only allows the use of qualitative assessments to reach a conclusion of 'significantly less likely...' which would still require a CCF malfunction result analysis.] This determination is needed because a decision must be made as to whether the proposed change meets the evaluation criteria in 10 CFR 50.59(c)(2) without prior NRC staff approval, or whether a license amendment request (LAR) will be required. This statement implies that this analysis to determine the likelihood of the CCF (i.e., a CCF susceptibility analysis) is the only determination needed for the 50.59 evaluation. But this is not correct,

because if the CCF is credible (i.e., either case above – “as likely”, or “significantly less likely” but still credible), then additional analysis of the CCF malfunction result is needed to answer 50.59 Questions 5 and 6.].

The qualitative assessment is needed to support the process for making the following conclusions:

- The activity does not result in more than a minimal increase in the likelihood of failure of an SSC important to safety to perform its intended design functions as described in the UFSAR or credited in the plant safety analyses.
- For activities that could introduce a potential CCF, there is reasonable assurance that the likelihood of a CCF is much lower than the likelihood of failures that are already considered in the current plant design basis described in the UFSAR.
- For activities that could introduce a potential CCF, there reasonable assurance that the likelihood of a CCF is comparable (or less) to other CCFs that are not considered in the UFSAR.

For activities that introduce a potential CCF that meets all of the above conditions, CCF would not be considered in the UFSAR. [This is somewhat confusing, because if you meet bullet 3, then you also meet bullet 2. It would be clearer if bullet 2 is omitted from this section.]

For activities that introduce a potential CCF that do not meet all of the above conditions, the CCF would need to become part of the design basis [I agree, if you don't meet bullet 1. But if you meet bullets 1 and 2 (but not 3), then the CCF can be considered beyond design basis. This would not require the CCF malfunction to be added to the Chapter 15 safety analysis, but it would require additional CCF malfunction results analysis to determine the answers to 50.59 Questions 5 and 6.]. The licensee would be required to update the UFSAR to reflect the revised design basis accounting for the CCF and update the UFSAR safety analyses that must be revised to account for the CCF using design basis methods and acceptance criteria, as currently used in the abnormal operating occurrences and postulated accidents of the UFSAR. NRC staff approval of such a change (via 10 CFR 50.90) would be required.

This qualitative assessment clarification is intended to supplement, rather than replace the guidance provided for qualitative assessments that are described in NEI 01-01, Sections 4.4 , 5.1, 5.3 as well as Appendix A (Items Nos. 2(i) & 6(b)).

Qualitative Assessment Scope:

The qualitative assessment process may be applied to any proposed digital I&C plant modifications to safety and non-safety systems. However, at this time, it is not intended for this RIS to apply to reactor protection or essential safety feature initiation functions. Consistent with the staff's endorsement of NEI 01-01 in RIS 2002-22, it is likely that when applying NEI 01-01 for completing the 10 CFR 50.59 evaluation process for proposed changes to reactor protection

and engineered safeguards initiation systems, it will be found that a license amendment request will be necessary to make the change.

Qualitative Arguments and Documentation: This Qualitative Assessment clarification highlights four general categories of proposed design-related characteristics, each of which need to be evaluated to formulate effective qualitative arguments deemed sufficient to address the questions posed in the “Purpose” section above. The staff finds that an evaluation of the degree to which each category of design characteristic has been addressed and weighed collectively in the design is adequate to support arguments within acceptable technical bases for responding to the 50.59 evaluation questions. These areas should be evaluated in conjunction with the supplemental questions provided in NEI 01-01, Appendix A. Those four general categories are:

- Design Attributes of the proposed modification that serve to prevent or limit failures from occurring, ~~or that mitigate the consequences of such possible failures~~ [To avoid confusion, design attributes internal to and external to the target modification should be clearly distinguished. When the CCF is not prevented by internal design attributes, the CCF malfunction result must be analyzed. Design attributes external to the target modification can be credited in that CCF malfunction result analysis to mitigate the consequences of the CCF.]. Evidence of design attributes supporting arguments for the high reliability and dependability of the proposed modification should be described. [Design attributes are the ‘deterministic evidence’ that I discussed in my first comment. It is confusing to lump these together with qualitative evidence, because qualitative evidence requires subjective judgement, design attributes are either there or they are not (this is not subjective).]
- Quality Processes employed in the development of the proposed modification, including software development, hardware and software integration processes, hardware design, and validation and testing processes that have been incorporated into the development process.
- Defense in Depth: Evidence that the proposed design incorporates both internal and external layers of defense against potential failures [This is very confusing, because external layers do not prevent or limit a CCF; they can be credited to mitigate the CCF when it occurs.] of the modified I&C system or component that could result in modes of failure not already analyzed in the UFSAR or result in the initiation of a design basis Anticipated Operational Occurrence (AOO) or Postulated Accident (PA), or new AOOs or PAs that have not been previously analyzed [This is silent on the issue of ‘bounded’]. It is very important that this RIS provide sufficient guidance to allow a digital modification to be implemented under 50.59, if that mod results in a previously unanalyzed CCF malfunction that is still bounded by previous analyses. If you don’t allow this, you will bring the use of distributed control system technology to an end, because new malfunctions are almost always credible (but in most cases can be demonstrated to be bounded).

- Operating Experience: Evidence that the proposed system or component modification employs equipment configured in the same manner [this is important because there is a lot of operating experience that is not applicable] with significant operating history in nuclear power plant applications or non-nuclear applications with comparable risk-significant performance requirements, and the suppliers of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc. [I agree this is a qualitative attribute.]

These categories are not mutually exclusive and may overlap in certain areas. Adequate qualitative arguments for systems of varying safety significance should address the degree to which the proposed modification has addressed each of the above categories. It's the staff's expectation that ALL of these categories be addressed [I disagree. For a specific source of CCF (e.g., single random hardware failure), if the modification contains sufficient deterministic attributes to reach a CCF not credible conclusion, there is no reason to assess qualitative attributes. It is much more important to say that all applicable sources of CCF need to be systematically assessed. When doing this systematic assessment of all applicable sources of CCF, it is likely that most of the areas above will be assessed. However, if a CCF not credible conclusion is reached for all applicable sources of CCF, then a defense-in-depth assessment to evaluation the capability to mitigate the CCF is not required.] to the degree possible, and that the uncertainty to the degree to which the proposed modification has or has addressed each category is identified. **See Table 1.**

Documentation:

The qualitative assessment guidance also describes the areas of consideration that should be documented in order to present a consistent explanation of likelihood arguments supporting technical bases for responding to 50.59 evaluation questions. It's the staff's expectation that ALL of these categories be addressed to the degree possible. **See Table 2.** This table provides the 'process flow' that should be followed in terms of the structure of the qualitative assessment presentation as well as specific steps that should be addressed in the process.

Table 1 - Qualitative Argument Areas

<u>Topical Area</u>	<u>Description</u>
Design Attributes	<ul style="list-style-type: none"> • Design Criteria <u>[Criteria is not an attribute. The evaluation must confirm design attributes exist to meet the criteria.]</u>– For example: Diversity (if applicable), Independence, Redundancy • Inherent Design Features for software, hardware or architectural/network – For example: external watchdog timers, isolation devices, segmentation, self-testing and self-diagnostic features • Sufficiently Simple (i.e. enabling 100% testing) • Unlikely series of events – For example, the evaluation of a given DI&C modification would necessarily have to postulate multiple independent random failures in order to arrive at a state in which a CCF is possible. • Failure state always known to be safe <p>NOTE: It is the staff's expectation that potential triggers, <u>and the basis for concluding those triggers would not be concurrent and therefore not cause a -of CCF in an SSC to be modified,</u> be specifically identified and addressed in terms of design attributes presented as an argument for demonstrating likelihoods of CCF being as unlikely as other CCFs not considered in a plant's safety analyses. <u>[I'm very happy to see that the Staff is embracing non-concurrent triggers.]</u></p>
Quality	<ul style="list-style-type: none"> • Compliance with industry codes and standards - It is the expectation that for non-NRC endorsed codes and standards, the licensee must provide an explanation for why use of the particular non-endorsed standard(s) is acceptable. • Use of Appendix B vendors, or if not Appendix B, which generally accepted industrial quality program applies • Environmental qualification (e.g. EMI/RFI, Seismic) • Development Process rigor
Defense-In-Depth	<ul style="list-style-type: none"> • Coping measures • Operator Intervention/administrative controls and sufficient time to respond available • Physical restrictions external to the DI&C modification (e.g. mechanical restrictions on control valve movements) <u>[See previous comments. We should be distinguishing deterministic and qualitative measures that prevent or limit a CCF (internal to the target digital modification), from the deterministic measures credited to cope with a CCF when it occurs (external to the target digital modification).</u>
Operating Experience	<ul style="list-style-type: none"> • Wide range of operating history <u>with the same configurations or configurations that bound the targeted modification.</u> • History of lessons learned from field experience addressed in the design • High volume production usage in different applications- Note that for software, the concern is centered on lower volume, custom or user-configurable software applications. High volume commercial products used in different applications provides a higher likelihood of resolution of potential deficiencies.

Table 2 - Qualitative Assessment Documentation Structure¹

Topical Area	Description
Identification	Describe the full extent of the SSC(s) to be modified—boundaries of the design change.
Step 1 - Design Function	<ul style="list-style-type: none"> • What is the entirety of the design function(s) of the upgraded component(s) within the context of the plant system, subsystem, etc. • Describe what functions were covered by the previously installed equipment, and how those same functions will be accomplished by the modified design. Also describe any new functions to be performed by the modified design that were not part of the original design. • Assumptions and conditions associated with the expected safety or power generation functions
Step 2 - Failure Modes	<p>What are they for the upgraded component(s), and why they are different or the same as previously installed? <u>[You can't identify failure modes without first conducting a CCF susceptibility analysis. The failure modes are quite different if a CCF is credible vs. not credible. The failure modes for a credible CCF are quite different if there are limiting measures vs. no limiting mearsures.]</u></p>
Step 3 - Consequences of their Failure	<p>In terms of existing safety analysis or in terms of an enhanced safety analysis, what are the consequences of any postulated single failures or CCF of modified SSC(s)? <u>[Why would you postulate a CCF and determine its consequences, if the CCF is not credible. The process should conduct a CCF susceptibility analysis first (to determine CCF credibility), followed by a CCF malfunction results analysis for all CCFs determined to be credible.]</u></p>
Step 4 - Claims and sub-claims	<p>What are the assertions being made: <u>[Why would you make any assertions with first conducting a CCF susceptibility analysis.]</u></p> <ul style="list-style-type: none"> • The digital component is at least as reliable, dependable, etc, as the device previously installed? • Its postulated CCF likelihood is significantly lower than single failures considered in the UFSAR or comparable to CCFs that are not considered in the safety analyses (e.g. design flaws, maintenance errors)? <p>ALL claims should fully address the consequences of a postulated CCF of the SSC(s) to be modified <u>[Why would you postulate a CCF and determine its consequences, if the CCF is not credible. The process should conduct a CCF susceptibility analysis first (to determine CCF credibility), followed by a CCF malfunction results analysis for all CCFs determined to be credible.]</u> and the likelihood status of postulated CCF. The qualitative assessment will not determine the absolute likelihood of failure in terms of failures-per-operating hour.</p>

¹ Establishes structure specifically for qualitative assessment to supplement guidance provided in NEI 01-01 Appendix B.

Step 5 - Evidence (Qualitative Arguments of likelihood)	<p>Should support each of the claims (e.g. evidence of the 4 qualitative assessment arguments) including codes and standards applied, qualification for the environment (e.g., seismic, EMI/RFI, ambient temperature, heat contribution, etc.) Quality Processes employed in the development (V&V processes used as evident in a traceability matrix, QA documentation, unit test and system test results, etc.), defense-in-depth (e.g. inherent internal diversity, manual back-up capability, etc.), and Operating History (e.g., platform used in tens of thousands of applications worldwide, etc. with minimal failure history, etc.)</p> <p>The level of evidence provided should be commensurate to the safety significance of the SSC(s) to be modified. <u>[This needs to be clarified, because it sounds like a risk informed assessment; I don't think that is the intent. I prefer to say that there is a graded approach in that when assessing deterministic and qualitative attributes, control systems are not expected to comply with the same codes and standards as safety systems.]</u></p>
Step 6 - Rationale	<p>Stating why the claim can be considered to be true, based on the evidence described. Include arguments both supporting and detracting (pros and cons) so that the 10 CFR 50.59 user of the QA has a feel for the relative magnitude of the uncertainties are associated with each claim is evident. Justification supporting the use of the rationale. <u>[This step seems to unnecessarily duplicate the Evidence and Consequence steps above. You either have sufficient evidence to conclude that a CCF is less likely, or you don't. For a credible CCF the consequences are either bounded or they are not. This step just adds more uncertainty and more potential for inconsistent application of the process across the industry.]</u></p>
Step 7 - Conclusion	<p>Apply the results of the qualitative assessment to respond to 50.59 evaluation questions. <u>[It is still not clear to me how you correlate the assessments above with the 50.59 questions.]</u></p>

Consequences of the Failure (Evidence Determination):

The level of evidence needed to be provided in the qualitative assessment should be commensurate with the consequences of the postulated failure of the SSC to be modified. For example, the higher the safety significance of the SSC being modified, the more evidence is necessary to be presented and evaluated [Again this sounds like a risk informed assessment. We should be discussing only a graded approach for defensive attributes, as commented above. There is no place for a risk informed assessment in a 50.59 evaluation (at least today).]

Consideration of what is the impact of a failure on the ability of the plant to continue to accomplish critical plant safety functions may provide an indication of the level of evidence needed to support effective qualitative assessments [You are completely missing the problem of control system CCFs potentially challenging critical safety functions in a manner that was not previously analyzed. This is an equal threat to plant safety.] Critical safety functions² (CSFs)³ are those safety functions that are essential to prevent direct and immediate threat to the health and safety of the public. These are accomplishing or maintaining of:

² Source: IEEE Std. 497-2002 as endorsed by RG 1.97, Revision 4.

³ For AP1000, critical safety functions are Subcriticality – Core Cooling – Heat Sink – Integrity – Containment - Inventory

- Reactivity control
- Reactor core cooling
- Reactor coolant system integrity
- Primary reactor containment integrity
- Radioactive effluent control

Additional questions that could be asked include based upon consideration of CSFs include:

[None of the question below should be asked if the CCF is not credible. Most of the questions are not relevant if the CCF malfunction result is bounded.]

- Is there an immediate safety impact to the plant?
- Is there a longer term safety impact if condition is not repaired/addressed/adequately coped with?
- Is the CCF/malfunction detectable by operators? If so, are there validated procedural actions in place (or proposed as part of the plant modification) to enable plant operators to identify the malfunction and take appropriate remedial action? [This question is relevant only if operator action is credited to either prevent the CCF or to cope with a credible CCF. Otherwise there is no reason to ask this question.]
- Postulate the failure (CCF) concurrent with an AOO/PA in the safety analyses: What's the impact on plant safety? [This should be asked only for a credible CCF that can go undetected for long periods of time (as for many CCFs in safety systems, because they are in standby operation). It does not need to be asked for a CCF that is immediately detectable (as for most CCFs in control systems, because they are in continuous operation).]

Example Applications:

In general, potential impacts on the plant critical safety functions (CSFs) require a greater level of evidence to be presented and weighed qualitatively than impacts on non-CSFs [If there is no potential challenge to CSFs then there is no need for any CCF consideration. This is why the first question in NEI 16-16 is "Is the equipment an initiator [of a transient] or credited for event mitigation"]. For example, using CSFs to assess risk significance, and comparing them against proposed modifications could yield the following results⁴:

- For RPS/ESF control and actuating logic modifications – (Considered out of scope for this guidance)
- EDG Voltage Regulators – Impacts multiple critical safety functions; therefore, one could do under 50.59 [this conclusion is unrelated to the first phrase of this sentence] but requires significantly greater level of evidence.

Main Control Room HVAC Safety Chillers – Do not appear to have any appreciable or immediate effects on the CSFs above, therefore level of evidence could be lower [Chillers are a support system credited to keep control systems, and safety I&C systems within their

⁴ Additional input necessary if more granularity is needed

qualification envelope (thereby preventing CCF of these systems). Chillers are also credited to maintain MCR habitability for plant operators. I&C systems and operators are both credited to avoid challenges to CSFs or maintain CSFs. Therefore, failure of a Chiller threatens CSFs.].

DRAFT