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, 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. 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.

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 ~~is~~ reasonable assurance that the likelihood of a CCF is comparable to other CCFs that are not considered in the UFSAR.

Commented [vxf1]: During the March 30 meeting, we discussed the use throughout the document of the terms risk significant vs. safety significant. Safety significant appears appropriate, as that process includes an assessment of risk to determine safety significance.
One way to categorize the importance of SSCs could be to view their function with respect to the 3 areas already used by the NRC staff and operating fleet:
-Initiating Events
-Mitigating Systems
-Barrier Integrity
This concept is somewhat aligned with the process described in this document on pages 6 and 7.
Please consider this for future discussions

Commented [vxf2]: Consider further developing the failure concept(s) in this document to address "single failure" as defined in RG 1.53, and the assumption that CCF is not a single failure (BTP 7-19 Section 3.3). This is an important point, in particular when considering if the postulated failure is within the design basis or not. BTP 7-19 currently states that realistic assumptions (not design basis) can be used to evaluate CCF coincident with DBEs. There was discussion in the meeting about the use, or not, of realistic assumptions (best estimate) for evaluation of effects of CCF in 50.59 space.

Commented [NGA3]: If a SSC has a UFSAR described design function, it is considered important to safety, thus the term is redundant.

Commented [NGA4]: 50.59 applies to SSCs with a UFSAR described design function. If a function is credited in the safety analysis, it likely has a UFSAR described design function thus the term is redundant.

For activities that introduce a potential CCF that meets the above conditions, the CCF would not be considered in the UFSAR.

For activities that introduce a potential CCF that do not meet the above conditions, the CCF would need to become part of the design basis. 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~~ engineered safety features actuation systems logic ~~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 safety features ~~safeguards initiation~~ actuation 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. Evidence of design attributes supporting arguments for the high reliability and dependability of the proposed modification should be described.

- Quality Processes employed in the development of the proposed modification, including software development, hardware and software integration processes, hardware design,

Commented [NGA5]: This needs clarification and perhaps alternate wording – for instance what about non-safety SSCs? There may be instances where a CCF has no consequential effect and thus there is no need to include in the design basis. We want to be clear on where a particular CCF does need to be added to the design basis

Commented [vxf6]: As an example to clarify the above comment, only certain non-safety related systems require consideration of failures. For instance, Reactivity and Control systems described in GDC 25 and 26.

Commented [NGA7]: This statement needs further work and clarification - is the intent to be limited to RPS/ESFAS logic or also to field input/end actuating devices? Does this only apply to wholesale change-out of an analog RPS with a digital RPS? We would like to see flexibility to allow some minor upgrades to parts/components of an already digital RPS.

Commented [NGA8]: Evidence of a quality development process will be different for non-safety SSCs, as they would follow commercial quality processes without a CG dedication.

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 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.

- Operating Experience: Evidence that the proposed system or component modification employs equipment 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.

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 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

Topical Area	Description

Commented [vxf9]: The term "defense in depth" was discussed during the meeting. One reference to consider for future discussions on this topic is NUREG/KM-0009, which captures the key principles. We recommend additional discussion with the industry on how this applies to I&C systems for the purposes of evaluating any impact on defense in depth due to the proposed I&C modification.

Commented [vxf10]: We discussed the use of "risk significant" in the meeting. Consider expanding on this concept to define what "risk-significant" could mean for non-nuclear applications. One example would be what is called "Safety Instrumented Systems". These are defined in the ISA "84" series of standards, and IEC-61511. We should discuss this use of OE for non-safety systems.

Commented [NGA11]: Additional discussion and clarification is needed to better define what would be expected with respect to "uncertainty".

Design Attributes	• Design Criteria – 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 NOTE: It is the staff's expectation that potential triggers of CCF in an SSC to be modified 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.
Quality	• 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	• 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)
Operating Experience	• Wide range of operating history • 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 provide a higher likelihood of resolution of potential deficiencies.

Commented [NGA12]: Industry would like staff to consider "non-concurrent triggers" as a design attribute.

Commented [vxf13]: We should discuss if, or how this RIS should align with RIS 2016-05 that was issued for Embedded Digital Devices. RIS 2016-05 does discuss the trigger concept. It also has specific scope and "requirements" that we need to discuss, so there we avoid any real or apparent conflict with the proposed scope and content RIS 2017-xx.

Commented [NGA14]: Compliance with codes and standards would be different for safety and non-safety SSCs. Perhaps quality should be broken down into two separate bullets - one for safety SSCs and one for non-safety SSCs to clarify what would be applicable.

Commented [vxf15]: Consider our comment on using the information in NUREG/KM-0009 on defense in depth. Compensatory measures and operator actions are discussed there, and may be useful in better defining the boundaries for this area.

Commented [NGA16]: Additional clarification is needed to define acceptable measures and criteria for coping in this context.

Commented [NGA17]: Consider addressing both operating system software and application software.

Table 2 - Qualitative Assessment Documentation Structure[1]

Topical Area	Description
Identification	Describe the full extent of the SSC(s) to be modified—boundaries of the design change.

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

Step 1 - Design Function	• What is the entirety of the UFSAR described design function(s) of the upgraded component(s) within the context of the plant system, subsystem, etc. • Describe what design functions were covered by the previously installed equipment, and how those same design functions will be accomplished by the modified design. Also describe any new design 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	What are the failure modes of ~~they~~ ~~for~~ the upgraded component(s), and are ~~why~~ they ~~are~~ different ~~or the same as~~ than the failure modes of the currently ~~previously~~ installed component(s)?
Step 3 - Consequences of their Failure	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)?
Step 4 - Claims and sub-claims	What are the assertions being made: • 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)? ALL claims should fully address the consequences of a postulated CCF of the SSC(s) to be modified 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.
Step 5 - Evidence (Qualitative Arguments of likelihood)	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.), as applicable considering the safety classification of the SSC. 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. wit minimal failure history, etc.) The level of evidence provided should be commensurate to the safety significance of the SSC(s) to be modified.
Step 6 - Rationale	~~Stating~~ State why the claim can be considered to be true, based on the evidence ~~described~~ provided. Include arguments both supporting and detracting (pros and cons) so that the 10 CFR 50.59 user of the ~~QA~~ qualitative analysis has a feel for the relative magnitude of the uncertainties ~~are~~ associated with each claim ~~is evident~~. Provide justification supporting the use of the rationale.

Commented [NGA18]: This bullet needs some clarification as to what would be expected.

Commented [NGA20]: Additional clarification is needed to Step 3. Does "existing safety analysis" mean the updated final safety analysis report (UFSAR) or the accident analysis (e.g., as described in Chapters 6 & 15 of the UFSAR)? If the purpose and context of this step is to support addressing 50.59 Evaluation question 6, we believe the intent is "accident analysis." Likewise, it is unclear what is meant by "enhanced safety analysis."

Commented [NGA19]: Consequences in 50.59 relates to dose. If "consequences" is not used for dose in this context, consider changing to "Results of their failure".

Commented [NGA21]: See above comment to define if this is relating to dose consequences or failure results.

Commented [NGA22]: "Postulated" = assumed. If, through our qualitative analysis we conclude CCF is not likely, then we should not have to postulate a CCF. As written, this statement seems to be saying that, even if CCF has been declared sufficiently unlikely, the licensee still needs to assume a CCF and address the results of that CCF on the plant/SSC.

Commented [NGA23]: This type of determination would be quantitative and the difference should be clarified.

Commented [NGA24]: CAE model not widely used - may require a lot of unnecessary documentation.

Need to consider a graded approach for Steps 5, 6, and 7 of this table on their applicability to non-safety systems.

Commented [NGA25]: Suggest using "numerous" or "significant number of" in place of "tens of thousands". What if a specific component has an installed base of 9,000 units without a single failure? Would that be sufficient or must there always be "tens of thousands" before this attribute can apply. Some licensees may take this literally.

Step 7 - Conclusion	Apply the results of the qualitative assessment to respond to each of the 50.59 evaluation questions.

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.

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. Critical safety functions[2] (CSFs)[3] are those safety functions that are essential to prevent direct and immediate threat to the health and safety of the public. These CSFs accomplish or maintain the following: ~~are accomplishing or maintaining of:~~

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

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

- 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?
- Postulate the failure (CCF) concurrent with an AOO/PA in the safety analyses: What's the impact on plant safety?

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. For

[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

Commented [NGA26]: See above comment to define if this is relating to dose consequences or failure results.
Suggest changing "Consequences" with "Results".

Commented [vxf27]: We discussed the use of the "CSF" terminology during the meeting. "Safety function" might be more appropriate, as that is used in NRC regulations such as Part 21 and 50.73 This concept is also tied to the previous comment on "safety significant" on page 1. We should discuss this to better define the scope of the qualitative assessment.

Commented [vxf28]: See previous comment on the BTP 7-19 treatment of CCF with respect to DBEs.

Commented [NGA29]: Our view is that postulating the CCF is only required if the qualitative analysis determines a CCF is likely. In other words, if the qualitative analysis concludes a CCF is much lower than the likelihood of failures that are already considered in the current plant design basis described in the UFSAR, then postulating the CCF should not be a requirement.

example, using CSFs to assess risk significance, and comparing them against proposed modifications could yield the following results[4]:

- 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 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.

Commented [NGA30]: Need to develop some additional clarification, for example does this statement just apply to the RPS/ESFAS logic or input/end actuating devices as well?

[4] Additional input necessary if more granularity is needed