Draft – Qualitative Assessment Framework

1 Introduction

RIS 2002-22 provided the staff's endorsement, with clarifications, of NEI Guidance document NEI 01-01, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule," for use as guidance in designing and implementing digital upgrades to instrumentation and control systems. The purpose of Revision 1 to NEI 01-01 was to assist licensees in designing and implementing digital replacements in a consistent manner. NEI 01-01 provides guidance in performing qualitative assessments of the dependability of and risk associated with I&C systems. The U.S. Nuclear Regulatory Commission (NRC) staff expects that such qualitative assessments be adequately documented with the level of detail and topical area coverage needed to support licensing decisions, while enabling staff inspectors or other licensee reviewers of such assessments to easily understand the technical basis for the assessment conclusions.

2 Purpose

This enclosure provides clarification of the staff's previous endorsement of NEI guidance for performing and documenting qualitative assessments developed in support of Title 10 of the *Code of Federal Regulations* (10 CFR) Section 50.59 evaluations of proposed digital 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 modification are consistent with the UFSAR analysis assumptions. 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 malfunction or failure of an SSC important to safety to perform its intended design functions.
- The activity does not result in the more than minimal increase in the consequences of an accident or malfunction.
- The activity does not result in a new type of accident, or a malfunction with a different result.

2.1 For activities that introduce a potential CCF that meets the above conditions, the CCF alone would <u>not</u> require the change to be approved under 50.90.

2.2 For activities that introduce a potential CCF that do not meet the above conditions, the CCF would need to become part of the licensing basis; a licensee amendment would be required. (via 10 CFR 50.90).

2.3 This qualitative assessment clarification is intended to clarify, 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)).

3 Qualitative Assessment

3.1 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.

3.2 "Quantitative vs. Qualitative"

A quantitative assessment involves the use of numbers in measurements, comparisons, or calculations. A qualitative assessment is any other assessment that is not quantitative. For example, an electrical independence requirement can be demonstrated, quantitatively, by comparing the capacity of an electrical isolation device with anticipated challenges to it. Alternatively, an electrical independence requirement can be demonstrated qualitatively by showing that the independent channels of equipment have no shared common components and have no electrical connections between them.

3.3 Qualitative Argument Cornerstones

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 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, 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 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. **See Table 1**.

Table 1 - Qualitative Argument Topical Areas	
Topical Area	Description
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 • Non-concurrent triggers • 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
Quality Design Processes	• 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 • Availability of operator intervention capabilities independent of the potential CCF, administrative controls, and sufficient time to respond • Physical restrictions external to the DI&C modification (e.g. mechanical restrictions on control valve movements, pump/turbine/vfd speed limits, rod control interlocks, etc.)
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 provides a higher likelihood of resolution of potential deficiencies.

3.3.1 Design Attributes versus Quality Process

Both “Design Attributes” and “Quality Process” are needed because to some degree they addresses different aspects, and to some degree they complement each other. For example, the surface of a weld should be appropriately cleaned (a Design Attribute) before the welding is performed, in part, to ensure a proper weld. It is generally not possible to tell, from inspecting the weld after it is completed, that the surfaces were properly cleaned. Therefore, Quality Processes ensure and document: the welder is trained in the appropriate cleaning processes, and in-process inspections are performed to ensure the weld surfaces are cleaned.

3.3.2 Design Attributes to Eliminate Consideration of CCF

Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, NUREG-0800 Chapter 7, Branch Technical Position No. 7-19 only recognizes two design attributes as sufficient to eliminate consideration of software based or software logic based CCF: Diversity or Testability. However, if CCF is considered in a larger context (i.e., software based or software logic based CCFs are not the only types of CCFs), then there are many regulatory requirements to address potential CCFs, and thereby eliminate them from further consideration. As a result, any relaxations in how these requirements are met, should screen in (i.e., require a full 50.59 evaluation). Changes in how requirements are met need to be evaluated to ensure they do not result in a need for a license amendment. In addition, there are some SSCs that have only minimal applicable criteria. These SSCs may have been implemented in a manner (i.e., relatively independently) such that only individual SSC malfunction or failure was considered in the FSAR (as updated). If these individual SSC are combined with (e.g., controlled by a common digital component) or coupled to (e.g., by digital communication) each other, then the new malfunction and/or accident must be evaluated under 50.59. NRC approved qualitative and/or quantitative methods can be used to evaluate attributes of the design to determine whether a license amendment may be required:

- Digital Communications: The introduction of digital communication (between redundancies, levels of defense, or between different safety classifications) that does not meet NRC endorsed guidance for communications independence should be reviewed and approved under a 10 CFR 50.90.

- Combination of Functions: The combination of functions (that (i) can cause a plant transient, (ii) are credited for mitigating plant transients either directly or as an auxiliary support function, or (iii) are of different layers of defense) should be evaluated under 50.59. If the evaluation determines that: (A) a new type of accident, (B) a malfunction with a new result, or (C) an unbounded malfunction or accident now exists, then a LAR is required.

- Defense-in-depth: Defense-in-depth is an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility. The defense-in-depth philosophy has traditionally been applied in plant design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It continues to be an effective way to account for uncertainties in equipment and human performance and, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena that, because they are unknown or unforeseen, are not reflected in either the PRA or traditional engineering analyses. The SRM on SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," provides additional information on defense-in-depth as an element of the NRC's safety philosophy.

Appendix A, “General Design Criteria for Nuclear Power Plants,” to 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” was first promulgated in 1971 and reflects the defense-in-depth principles, although Appendix A does not explicitly refer to defense-in-depth. A balance among accident prevention, accident mitigation, and limiting accident consequences is basic to the general design criteria. Specific requirements in the general design criteria exist for independence, redundancy, and diversity (oftentimes achieved by imposing the requirement to withstand a “single failure).” The general design criteria also require a level of quality commensurate with the safety functions of structures, systems, and components and require the capability for inspection and testing.

Both RG 1.174 Rev. 3 and BTP 7-19 contain criteria for determining whether adequate Defense-in-Depth has been maintained. A failure to meet either of these criteria should be reviewed and approved under a 10 CFR 50.90. That is, a failure to maintain adequate defense in depth is considered to violate a criteria that is applicable to both evaluation question 1 &2:

> “Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard.”

3.3.3 Design Specifics

It is not possible for generic guidance to anticipate all of the ways that a design can introduce failure and malfunction modes; therefore, the features of each design must be reviewed against the applicable 50.59 criteria. This is in addition to the general considerations listed above.

3.3.4 Regarding codes and standards

Design attributes credited for meeting any criteria must be stipulated and documented as being achieved (per GDC 1 - Quality Standards and Records):

(1) “Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.”

The term “quality standards” is sometimes a source of confusion. Some understand this term to mean “codes and standards;” however, this interpretation would render the first clause of the second sentence irrelevant. A better interpretation of the term would be: “specified criteria.” It is understood that not everything important to safety has been designed according to a generally recognized code or standard.

(2) “Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function.”

This sentence allows the use of “generally recognized codes and standards,” when appropriate instead of requiring application specific specifications for all important to safety aspects. That is, codes and standards can be incorporated by reference in plant specific specifications of important to safety equipment.

(3) “A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions.”

This sentence requires process controls for important to safety equipment that is not part of an Appendix B quality assurance program.

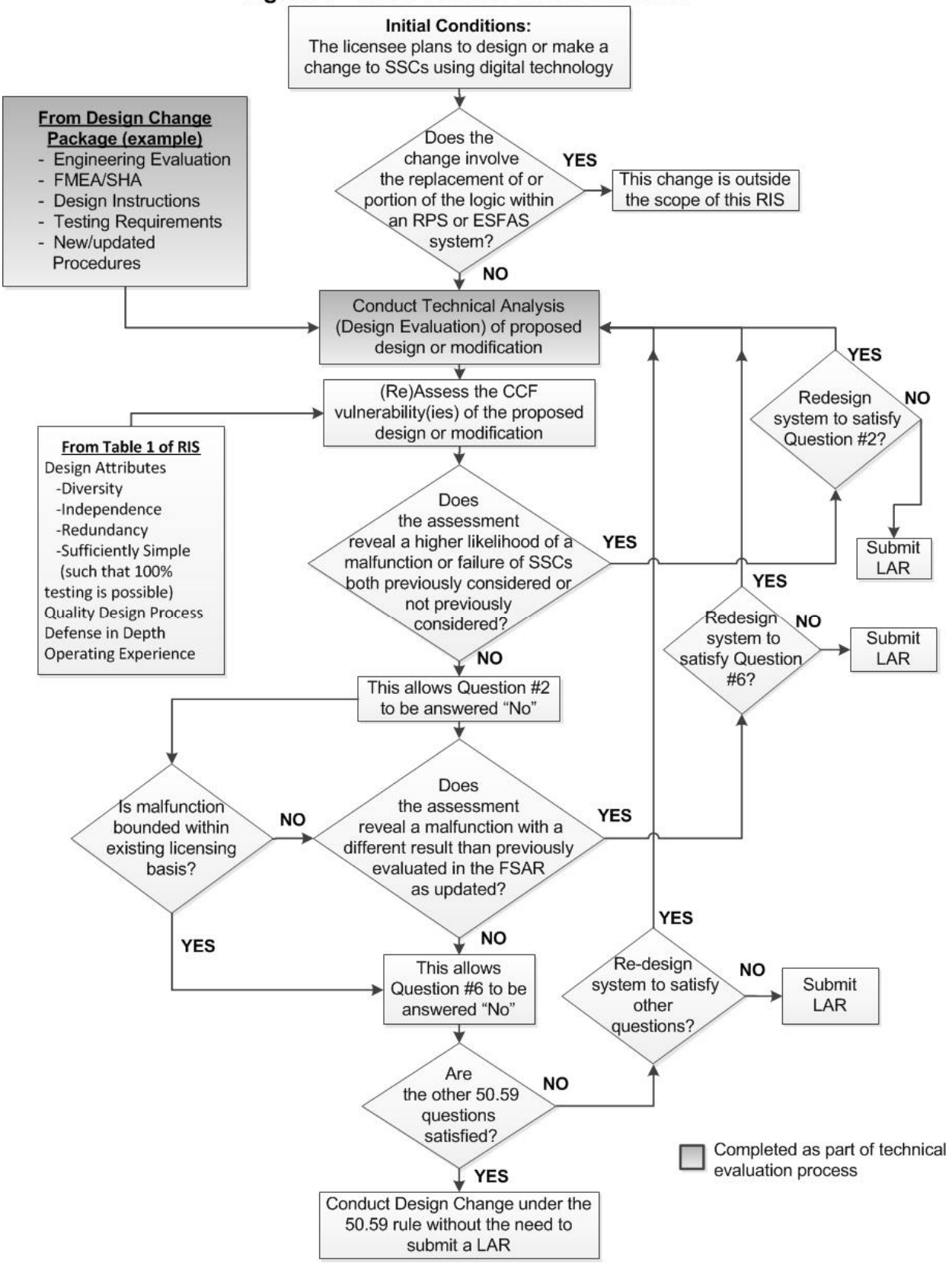
(4) “Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.”

The sentence requires documentation for important to safety equipment that is not part of an Appendix B QA program.

3.3.5 Decision Process

Figure 1 of this qualitative assessment guidance provides a general overview of the types of considerations that should be made when using this guidance to address NEI 01-01 Appendix A (Items Nos. 2(i) & 6(b)). Individual assessments may vary depending upon the licensee using this qualitative assessment guidance.

Figure 1 - RIS Decision Tree Flowchart



4 Qualitative Assessment 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.

4.1 Responsibilities of License Holders

It is critical that the licensee document in the design modification package the design codes and standards that were used in the development of the proposed digital I&C design modification. The qualitative assessment will reference the design standards used, and provide a rationale as to why those design standards, as employed by experienced software and hardware engineering professionals, are considered adequate for demonstrating that a high quality component or system will result, as evidenced by the fact that a well-defined process for project management, software design, development, implementation, verification, validation, software safety analysis, change control, and configuration control was used. The selection of the design standards to be employed should be commensurate with the level of safety significance of the modified component or system, and the possible safety consequences that may result from its failure. They need not be the same as the industry design standards referenced within NRC regulatory guides, however the licensee should be able to demonstrate why the design standard employed is considered adequate for the proposed design modification, commensurate with the level of safety significance.

4.2 Safety Significance of SSCs and Documentation of Evidence

As stated previously, an important consideration for documentation of evidence to address 50.59 evaluation criteria is consideration of the relative safety significance of the SSC to be modified and a graded approach can be utilized to this end. There are numerous ways in which to correlate safety significance to level of documentation needed. Some considerations can include, but not limited to the following:

- Is the SSC(s) to be modified an event initiator?
- Is the SSC(s) to be modified part of an accident mitigation system?
- Is the SSC(s) to be modified important to maintaining barrier integrity?

Another means to correlate the level of documentation versus the safety significance of the SSC(s) to be modified is consideration of the SSC(s) role in accomplishing or maintaining critical safety functions[1] such as:

- Reactivity control

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

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

It is the responsibility of the 50.59 evaluator to demonstrate that the documentation of the design basis of the proposed modification is adequate based upon the safety significance of the SSC(s) to be modified and that this portion of the analysis is captured within the 50.59 evaluation.

Table 2 - Qualitative Assessment Documentation Structure[2]	
Topical Area	Description
Identification	Describe the full extent of the SSC(s) to be modified—boundaries of the design change.
Step 1 - Design Function	• What is the entirety of the UFSAR 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 the upgraded component(s), and are they different than the failure modes of the currently installed component(s)?
Step 3 – Results 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 - Assertions	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 assertions should fully address the results 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.
Step 5 – Documentation of Evidence	Evidence should support each of the assertions (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. 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 numerous applications worldwide, etc. with 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	State why the assertion can be considered to be true, based on the evidence provided. Include arguments both supporting and detracting (pros and cons) so that the 10 CFR 50.59 user of the qualitative analysis has a feel for the relative magnitude of the uncertainties are associated with each claim. Provide justification supporting the use of the rationale.
Step 7 - Conclusion	Apply the results of the qualitative assessment to respond to each of the 50.59 evaluation questions.

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