RIS 2002-22 Supplement 1

Neil Archambo
Principal Engineer
Duke Energy

February 19, 2019

NUCLEAR ENERGY INSTITUTE

DISCUSSION TOPICS

- Scope
- Intent
- Concept
- Qualitative Assessment Categories
- Failure Likelihood Determination
- The Role of Failure Analyses
- Defense-in-Depth Analysis
- Specific Areas of Concern
- Qualitative Assessment Structure
- Qualitative Assessment Retention
- Example Qualitative Assessment
- Industry Part
- Upcoming DI&C Industry Guidance

RIS 2002-22 SUPPLEMENT 1 SCOPE

- Like NEI 01-01, the RIS Supplement applies primarily to modifications of safety related SSCs
- The RIS Supplement can be applied to modifications of non-safety related SSCs at the discretion of the licensee
- The RIS Supplement is not intended to be used for complete RPS or ESFAS upgrades or modifications that alter the internal logic of RPS or ESFAS
- Generally, the RIS Supplement is applicable for use on all SSCs, however, more safety significant SSCs will require more qualitative assessment justification and documentation
- The RIS supplement does not provide guidance for 50.59 Screening nor does it presume that all digital modifications “screen in”
- The RIS Supplement provides examples of digital modifications where qualitative assessments would apply and highlights specific areas of concern

RIS 2002-22, SUPPLEMENT 1 INTENT

- NEI 01-01 permits the use of qualitative assessments to support a conclusion that a proposed digital I&C modification has a sufficiently low likelihood of failure
- However, NEI 01-01 provides little guidance on how to develop the qualitative assessment or how the qualitative assessment could be used to eliminate further consideration of CCF
- The pre-supplement regulatory position offered two alternatives for eliminating consideration of software CCF – (1) 100% testing of equipment or (2) use of sufficient diversity
- However, 100% testing of software using the NRC's definition is considered unachievable, even in applications that make use of very simple code
- Thus, with the current regulatory position before this supplement, the only way to eliminate further consideration of software CCF is to employ sufficient diversity

RIS 2002-22, SUPPLEMENT 1 INTENT

- RIS 2002-22 Supplement 1 provides a method, defined by and thus acceptable to the NRC, to develop and document an adequate qualitative assessment to determine digital equipment failure likelihood
- If the qualitative assessment concludes that an SSC has a sufficiently low likelihood of failure, then by extension the SSC has a sufficiently low likelihood of a CCF, including the likelihood of software CCF
- RIS 2002-22 Supplement 1 does not replace NEI 01-01 or the original RIS 2002-22 that endorsed it
- Licensees are still expected to consider the guidance provided in NEI 01-01 as appropriate per their specific administrative design procedures

RIS 2002-22, SUPPLEMENT 1 CONCEPT

- A qualitative assessment can have one of two possible outcomes:
  - Failure likelihood is “sufficiently low”
  - Failure likelihood is “not sufficiently low”
- Per NEI 01-01, “sufficiently low” means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors, equipment qualification stressors)
- If a qualitative assessment concludes that a potential failure has a sufficiently low likelihood, the 10 CFR 50.59 Evaluation does not need to consider the effects of the failure
- The following slides illustrate how the qualitative assessment can be used to address 10 CFR 50.59 questions

RIS 2002-22, SUPPLEMENT 1 CONCEPT

- 10 CFR 50.59 Criterion 1 addresses accident frequency:
  - The frequency of occurrence of an accident is directly related to the likelihood of failure of equipment that can initiate the accident
  - Thus, an increase in the likelihood of failure of the modified equipment would result in an increase in the frequency of the accident
  - Therefore, if the qualitative assessment outcome is “sufficiently low,” there will be no more than a minimal increase in the frequency of occurrence of an accident previously evaluated in the UFSAR

RIS 2002-22, SUPPLEMENT 1 CONCEPT

- 10 CFR 50.59 Criterion 2 addresses malfunction likelihood:
  - The likelihood of occurrence of a malfunction of an SSC important to safety is directly related to the likelihood of failure of equipment that causes a failure of SSCs to perform their intended design functions
  - Thus, the likelihood of failure of modified equipment that causes the failure of SSCs to perform their intended design functions is directly related to the likelihood of the occurrence of a malfunction of an SSC important to safety
  - Therefore, if the qualitative assessment outcome is “sufficiently low,” the activity will not result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR

RIS 2002-22, SUPPLEMENT 1 CONCEPT

- 10 CFR 50.59 Evaluation Criterion 5 addresses accidents of a different type:
  - Accidents of a different type are caused by failures of equipment that can initiate an accident of a different type
  - If the outcome of the qualitative assessment concludes that the likelihood of failure associated with the proposed activity is sufficiently low, the activity will not introduce any failures that are **as likely to happen** as those in the UFSAR that can initiate an accident of a different type
  - Therefore, if the qualitative assessment outcome is “sufficiently low,” the activity cannot create a possibility for an accident of a different type than previously evaluated in the UFSAR

RIS 2002-22, SUPPLEMENT 1 CONCEPT

- 10 CFR 50.59 Evaluation Criterion 6 addresses malfunctions with a different result:
  - A malfunction of an SSC important to safety is an equipment failure that causes the failure of SSCs to perform their intended design functions
  - If the outcome of the qualitative assessment concludes the likelihood of failure associated with a proposed activity is sufficiently low, the activity will not introduce any failures that are **as likely to happen** as those in the UFSAR
  - Therefore, if the qualitative assessment outcome is “sufficiently low,” the activity cannot create a possibility for a malfunction of an SSC important to safety with a different result from any other previously evaluated in the UFSAR

RIS 2002-22, SUPPLEMENT 1 CONCEPT

What about the other 10 CFR 50.59 Evaluation Questions?

- 10 CFR 50.59 Evaluation Criteria 3 and 4 address accident and malfunction consequences (dose), respectively
- 10 CFR 50.59 Evaluation Criterion 7 addresses fission product barriers
- 10 CFR 50.59 Criterion 8 addresses methods of evaluation
- Criteria 3, 4, 7, and 8 do not have aspects unique to digital and can be addressed using existing guidance provided in NEI 96-07

RIS 2002-22, SUPPLEMENT 1 CONCEPT

To summarize:

- RIS 2002-22 Supplement 1 provides a framework for development of a qualitative assessment that can be used to assess digital equipment failure likelihood
- If the likelihood of failure is sufficiently low, the likelihood of CCF (including software CCF) is considered sufficiently low
- If a qualitative assessment determines that a potential failure has a sufficiently low likelihood, the associated 10 CFR 50.59 Evaluation does not need to consider the effects of the failure
- Note that the information required to develop an acceptable qualitative assessment is information needed to develop a quality 10 CFR 50.59 Evaluation
- A well-developed and well-documented qualitative assessment will help an inspector understand the considerations taken by a licensee in the development of a digital 10 CFR 50.59 Evaluation

QUALITATIVE ASSESSMENT CATEGORIES

- The RIS Supplement defines three qualitative assessment categories:
  - Design Attributes
  - Quality of the Design Process
  - Operating Experience
- Design Attributes and Quality of the Design Process will always be essential elements of a qualitative assessment
- Operating experience, if available, may serve to compensate for weakness in the other two categories
- Qualitatively assessing and documenting these factors separately, and in the aggregate, will enable licensees to document qualitative assessments “in sufficient detail that an independent third party can verify the judgements”
- A discussion for each category follows

DESIGN ATTRIBUTES

- Design attributes are design measures implemented to prevent or limit failures from occurring
- Design attributes focus primarily on built-in features such as fault detection and failure management schemes, internal redundancy, and diagnostics
- Design features external to the proposed modification (e.g., mechanical stops on valves or pump speed limiters) may also be considered
- Table 1 of the RIS Supplement provides some sample design attributes for consideration
- A comprehensive list of design attributes can be found in Appendix A, “Defensive Measures,” of EPRI Technical Report 3002005326, “Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems”

DESIGN ATTRIBUTES

- An adequate qualitative assessment of the likelihood of failure of a proposed modification will describe potential failures the proposed modification could introduce and the specific design attributes incorporated to resolve the identified potential failures
- How the chosen design attributes and features resolve the identified potential failures should also be discussed in the qualitative assessment
- Diversity is one example of a design attribute that licensees can use to demonstrate that an SSC modified with digital technology is protected from a loss of design function caused by a potential CCF
- In some cases, a plant's design basis may specify diversity as part of the design – in other cases, licensees do not need to consider the use of diversity in evaluating a proposed modification

DESIGN ATTRIBUTES

- Typical Design Attributes
  - Watchdog timers that function independent of software
  - Self-testing and diagnostics capabilities
  - Use of highly testable devices (e.g., breakers, relays)
  - Elimination of concurrent triggers
  - Segmentation
  - Redundant networks
  - Unidirectional communications
  - Network switches with traffic modulation
  - Use of redundant controllers, I/O, power sources, etc.
  - Internal or external diversity
  - Use of isolation devices
  - Extensive testing

QUALITY OF THE DESIGN PROCESS

- Quality of the design process is a key element in determining the dependability of proposed modifications
- Digital equipment designed and implemented as safety related from an Appendix B supplier should have the necessary documentation to satisfy the quality of design process category
- Digital equipment qualified through the commercial grade dedication process (e.g., EPRI TR-106439) will not likely have the same level of documentation needed to satisfy the high quality design process category as Appendix B processes.
- However, utilities following their NRC-approved commercial grade dedication processes provide additional assurance of design quality needed to demonstrate an equivalent level of assurance as Appendix B.
- Use of applicable industry standards contributes to a quality design process and provides a previously established acceptable approach

QUALITY OF THE DESIGN PROCESS

- Documented capability through qualification testing or analysis to withstand environmental conditions within which the SSC is credited to perform its design function (e.g., EMI/RFI, temperature, humidity, radiation, seismic activity) is important
- Typical characteristics of a quality design process for safety related equipment consists of use of well-defined processes for:
  - Project management
  - Software design and development
  - Implementation
  - Software verification and validation
  - Software safety analysis
  - Change control
  - Configuration control

QUALITY OF THE DESIGN PROCESS

- For safety related SSCs, quality standards should be documents that are established by consensus and approved by an accredited standards development organization (e.g., IEEE)
- Quality standards used to ensure that a quality design process was used to develop the proposed change need not be limited to those endorsed by the NRC staff (e.g., IEC 60880)
- In some cases, other nuclear or non-nuclear standards can provide technically justifiable approaches for use if they apply to the specific application
- For non-safety related SSCs, adherence to generally accepted commercial standards is generally sufficient
- For non-safety related SSCs, procurement or manufacturer documentation showing that design specifications are met or exceeded with respect to the equipment being replaced is adequate

OPERATING EXPERIENCE

- NEI 01-01 states, “Substantial applicable operating history reduces uncertainty in demonstrating adequate dependability”
- Although a qualitative assessment can be completed without consideration of operating experience, a qualitative assessment cannot be based solely on operating experience
- Operating experience can be used to support a low likelihood of failure conclusion in instances where quality of the design process or design attributes are lacking
- Operating experience is also applicable to software tools and the hardware used to implement the device, as well as the complete device
- The design conditions and modes of operation of the equipment whose operating experience is being referenced should be similar to that of the proposed digital I&C modification

OPERATING EXPERIENCE

- The architecture of the OE-referenced equipment and software should be similar to that of the proposed system
- Design features that serve to prevent or limit possible CCFs in a design that is referenced as relevant OE should be documented and considered for inclusion in the proposed design
- When collecting operating experience, obtaining specific design information from the OE source, although not required, can help justify the qualitative assessment conclusions

FAILURE LIKELIHOOD DETERMINATION

- A qualitative assessment will typically conclude a sufficiently low likelihood of failure in the presence of the following:
  - Documented evidence of design attributes used and design measures implemented that can prevent or limit failures from occurring
  - Documented evidence that a quality process was used in the development of the equipment and an acceptable design process was followed
  - Relevant operating experience was captured on the equipment used in the design
- Remember, more safety significant SSCs will require more qualitative assessment justification and documentation to support a sufficiently low likelihood of failure conclusion
- Documentation is *CRITICAL!*

THE ROLE OF FAILURE ANALYSES

- The RIS Supplement uses the term “failure analysis” in the plain English context and does not necessarily mean a formal analysis – depending on the project scope and complexity, a failure analysis could simply consist of a short statement in the qualitative assessment
- The RIS Supplement does not provide guidance on how to develop failure analyses – licensees are expected to develop various failure analyses for a given activity based on their approved administrative design procedures
- A failure analysis can provide valuable input when constructing a qualitative assessment
- The RIS Supplement emphasizes key areas of consideration for identifying CCF vulnerabilities that should be addressed and documented in the final design and to support a qualitative assessment

THE ROLE OF FAILURE ANALYSES

Key areas to consider in a failure analysis:

- Potential sources of CCF
  - Sources of CCF that could affect more than one SSC need to be closely reviewed for adverse impacts on the design function(s)
- Combination of design functions into a single digital device
  - A failure analysis should consider whether single failures that could previously have affected only individual design functions can now affect multiple design functions
- Digital communications
  - The effect of digital communications on SSC independence should be considered within a failure analysis as digital communications may introduce interactions resulting in new types of failure modes

THE ROLE OF FAILURE ANALYSES

Key areas to consider in a failure analysis (cont.):

- Creating new interactions with other SSCs
  - The interface of modified SSCs with other SSCs that use identical hardware and software, power supplies, or human-machine interfaces needs to be closely reviewed to ensure that possible common triggers have been addressed
- Interconnectivity across channels, systems, and divisions
  - Ensure appropriate design attributes are incorporated to ensure redundancy, diversity, separation, and independence, as required by the plant's licensing basis, have not been reduced
- Changing response times
  - In some cases, digital equipment may change response times due to processing time – the failure analysis should consider the effect of response time

DEFENSE IN DEPTH ANALYSIS

- NEI 01-01 describes the need for a defense-in-depth analysis as limited to substantial replacements of RPS and ESFAS
- However, a defense-in-depth analysis is a powerful tool that can be used to support arguments made in a 50.59 Evaluation
- A defense-in-depth analysis can reveal the impact of potential CCFs caused by the introduction of:
  - Shared resources
  - Common hardware and software
  - Combination of design functions that were previously considered independent from one another
- The results of a defense-in-depth analysis also informs the process for identifying applicable design attributes
- The analysis may also demonstrate that existing SSCs or procedures could serve to mitigate effects of possible CCFs

SPECIFIC AREAS OF CONCERN

The NRC staff expressed the following specific areas of concern that require special attention and merit careful review:

- Use of the same software/hardware in multiple safety related channels/trains
- Combination of previously separate UFSAR-described design functions (safety or non-safety) previously analyzed as independent
- Application of digital communications across safety related channels or equipment
- Interconnectivity across channels, systems, or divisions in safety related SSCs
- Use of shared resources (e.g., power supplies, networks)
- Networking
- Bidirectional digital communications
- Multifunction displays and control stations
- Use of common controllers

QUALITATIVE ASSESSMENT STRUCTURE

The following structure is suggested when documenting a qualitative assessment:

- Activity Description
- Identification of Affected Design Functions
- Failure Mode Comparison
- Failure Results
- Assertions
  - Design Attributes
  - Quality of Design Process
  - Operating Experience
- Documentation of Evidence
- Conclusion (sufficiently low/not sufficiently low)
- References Consulted

QUALITATIVE ASSESSMENT RETENTION

- There are no specific retention requirements for the qualitative assessment specified by the RIS Supplement
- The qualitative assessment provides the materials needed by the 10 CFR 50.59 reviewer and approver, and should be part of their 50.59 review
- The qualitative assessment should be easily retrievable
- If not easily retrievable, consider attaching the qualitative assessment to the related 10 CFR 50.59 Evaluation
- The qualitative assessment should be retained based on the licensee's specific QA plan

QUALITATIVE ASSESSMENT EXAMPLE

- Replacement of motor operated potentiometer on EDG voltage regulator with a digital reference adjuster
  - Concern is a software CCF simultaneously affecting operability of both EDG trains – a condition that did not previously exist
  - Workshop exercise – step through and discuss the qualitative assessment developed for this activity

INDUSTRY PART

- We must do a better job properly addressing the 10 CFR 50.59 Screen and Evaluation questions associated with digital plant changes
- We need to adequately document and explain why our designs have a low likelihood of failure
- Documentation is the issue – industry has fallen short of adequate documentation and justification when developing our 10 CFR 50.59 Screens and Evaluations for digital plant modifications
- Industry must work together and share information regarding digital project designs and associated 10 CFR 50.59 reviews
- Implementation of an industry SharePoint where good examples of digital equipment qualitative assessments and digital-based 10 CFR 50.59 reviews can be easily accessed for industry use

UPCOMING DI&C GUIDANCE

- Appendix D to NEI 96-07, Supplemental 10 CFR 50.59 Guidance for Digital Activities
  - Provides supplemental 10 CFR 50.59 Screen and Evaluation guidance for digital activities
  - Now in the endorsement process – expected to be endorsed by June 2019
- Guidance for Addressing Digital CCF (Long Term)
  - Work continues on this item
- NEI 17-06 – Digital Equipment Commercial Grade Dedication Process
  - Investigating the use of SIL certification for software assessment
  - Expect NRC endorsement by mid-to-late 2019
- ISG-06, Revision 2, DI&C LAR Process
  - Approved December 2018

QUESTIONS?

