U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Guidance for Performing 10 CFR 50.59 Evaluations for Digital Instrumentation and Controls Modifications

Presented By: Philip McKenna
Senior Reactor Systems Engineer
NRR/DIRS/ROP Support and Generic Communications Branch
February 27, 2019

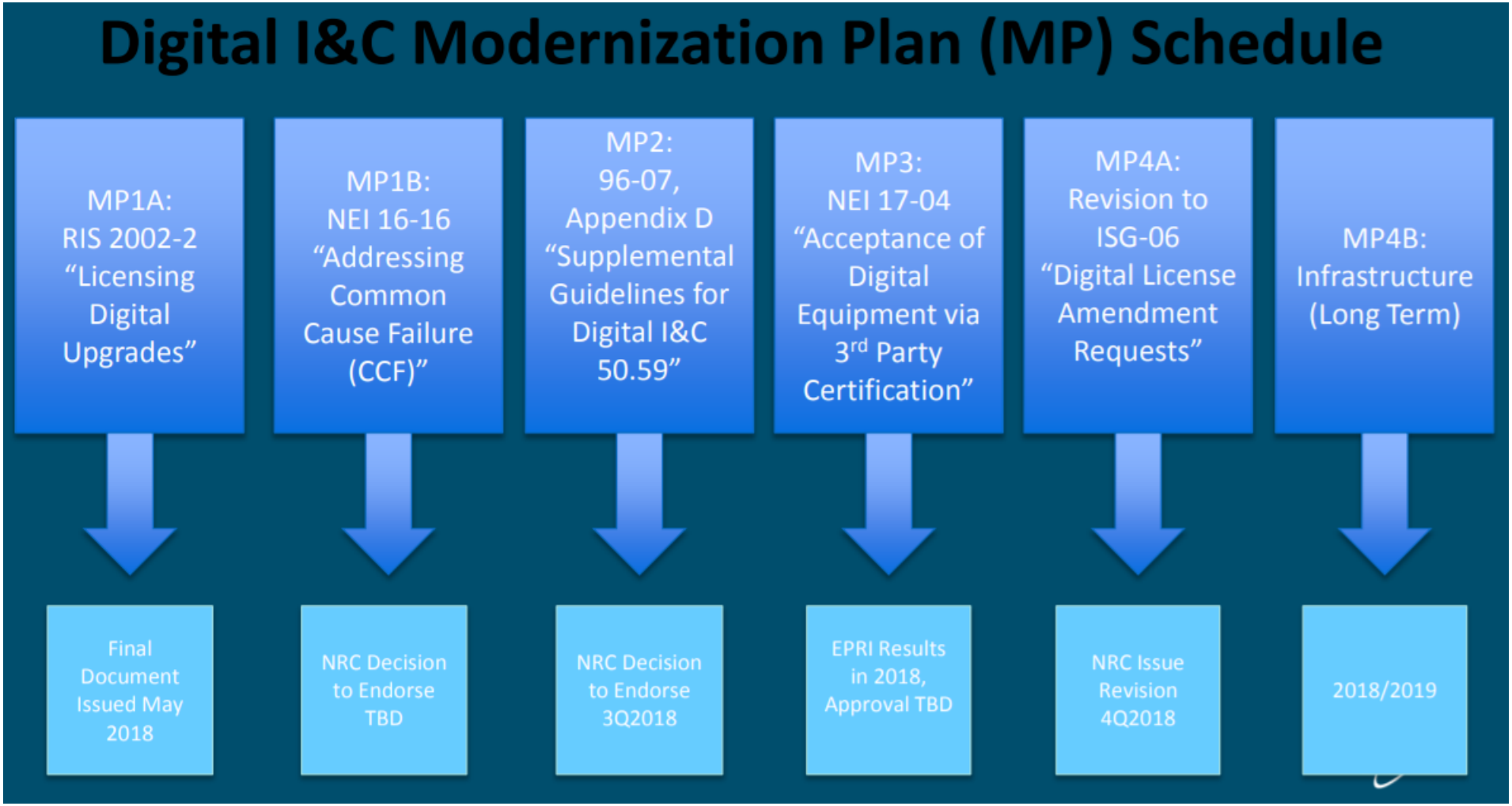
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Purpose

- Update Licensees and the Public on the process for evaluating and documenting digital I&C modifications using the 10 CFR 50.59 Rule
  - Discuss the structure of RIS 2002-22, Supplement 1, "Clarification on Endorsement of NEI Guidance in Designing Digital Upgrades in Instrumentation and Control Systems" (Issued on 05/31/18).
  - NEI conducted workshops for licensees on RIS 2002-22, Supplement 1 from September through November 2018.
  - Discuss an example of a Qualitative Assessment.
  - Briefly discuss NEI 96-07, Appendix D.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital I&C Integrated Action Plan



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

History of the 10 CFR 50.59 Rule

- First promulgated in 1962 and modified in 1968.
- Allows Licenses to make changes to the facility without prior NRC staff approval.
  - Must maintain acceptable levels of safety as documented in the FSAR.
- Rule was reviewed in 1995; issued in 1999 which increased flexibility for licensees:
  - Now allows changes that only minimally increase the probability or consequences of accidents
  - Nov 2000: NRC issues RG 1.187
    - Endorses NEI 96-07, Rev.1, “Guidelines for 10 CFR 50.59 Implementation”

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI 96-07 and RG 1.187

- NEI 96-07 was originally NSAC-125, but not endorsed by NRC.
- NEI 96-07
  - Applicability
  - Screening
  - Evaluation Process
- Regulatory Guide 1.187
  - Endorses NEI 96-07 – "Provides methods that are acceptable to the NRC staff for complying with the provisions of 10 CFR 50.59"

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

50.59 Process Chart

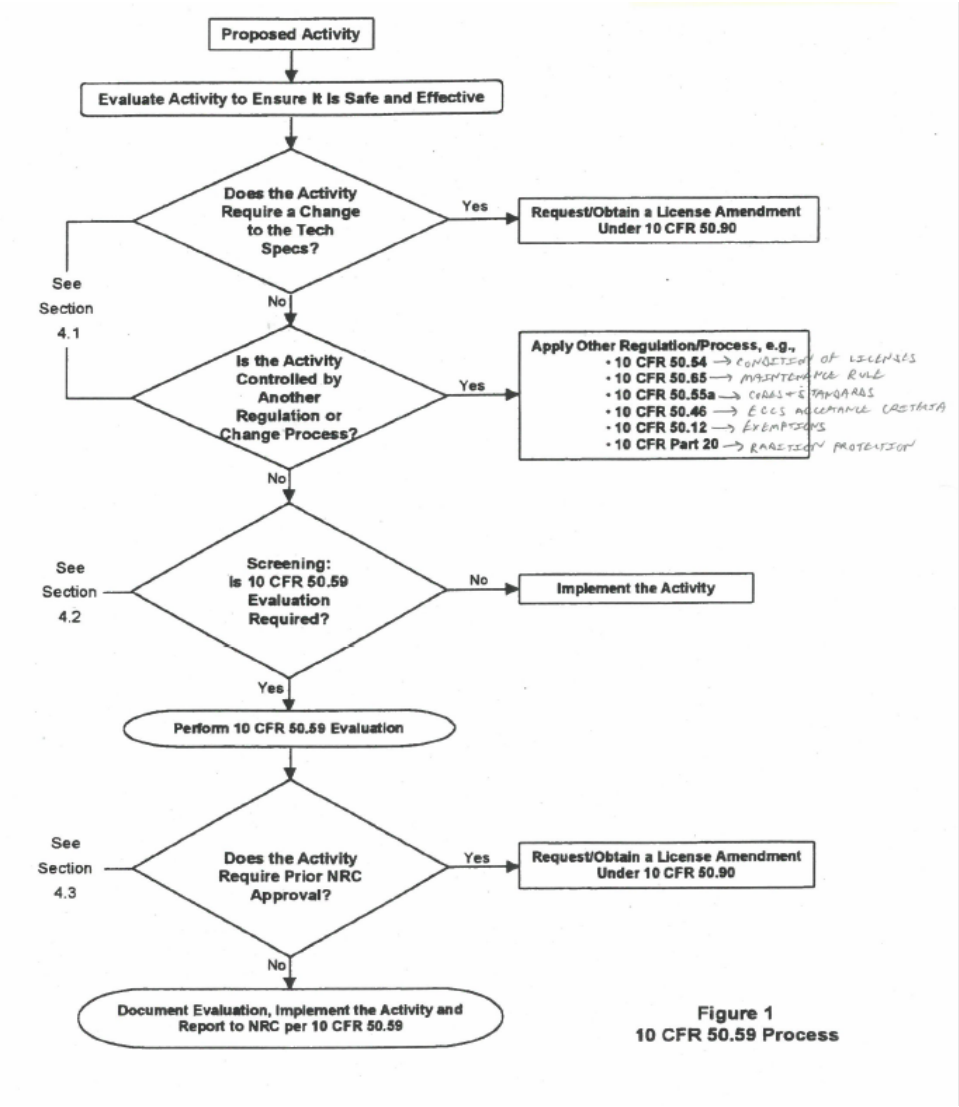


Figure 1
10 CFR 50.59 Process

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital I&C 10 CFR 50.59 Guidance

- EPRI TR-102348
  - Issued in 1993 to establish guidelines for digital upgrades in the context of 10 CFR 50.59.
  - Endorsed by NRC GL 95-02
    - "Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades,' in Determining the Acceptability of Performing Analog-to-Digital Replacements under 10 CFR 50.59"
- EPRI TR-102348, Revision 1 issued to address revised 10 CFR 50.59 rule in 1999
  - Issued as NEI 01-01
  - Endorsed by NRC RIS 2002-22

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI 01-01

- Industry inconsistently applying guidance in NEI 01-01 in digital upgrades
  - Lack of industry guidance on the technical evaluation of common cause failures
  - NRC IN 2010-10: "Implementation of a Digital Control System Under 10 CFR 50.59"
  - Harris 2013 violation: SSPS control circuit boards replaced with digital complex programmable logic device (CPLD)-based boards
  - NRC Letter to NEI: "Summary of Concerns with NEI 01-01," dated 11/05/13 (ADAMS Accession No. ML13298A787)
- NRC issues RIS 2002-22, Supplement 1 in May 2018 to clarify RIS 2002-22
  - NRC continues to endorse NEI 01-01

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital I&C Modifications

- What make these different?
  - Common Cause Failure (CCF)
    - Due to combined functions, shared communications, shared resources, and software error in redundant channels
- Safety Model of nuclear plant
  - Defense in depth and redundant equipment
  - Hardware: Likelihood of CCF acceptably low
    - High quality standards in development and manufacture
    - Physical separation of redundant equipment
    - Degradation methods slow to develop (i.e. corrosion)
  - Software: Special cause of single failure vulnerability
    - Software resides in redundant channels of the system
    - Single undetected design error in software could lead to CCF in all redundant channels

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RIS 2002-22, Supplement 1

- RIS 2002-22, Supplement 1, clarifies guidance for preparing and documenting "Qualitative Assessments"

- Not for Replacement of:
  - Reactor Protection System (wholesale)
  - Engineered Safety Features Actuation System (wholesale)
  - Modification/Replacement of the Internal Logic Portions of These Systems

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment

- Originally discussed in NEI 01-01, Sections 4 and 5 and Appendices A and B, but limited guidance on how to accomplish.
- RIS 2002-22, Supplement 1
  - Evaluate the likelihood of failure of a proposed digital mod to accomplish designated safety function
  - Evaluate the likelihood of common cause failure
- Used to support a conclusion that a proposed digital I&C modifications will not result in more than a minimal increase in:
  - The frequency of occurrence of accidents (50.59(c)(2)(i)
  - The likelihood of occurrence of malfunctions (50.59(c)(2)(ii)
  - Create the possibility of an accident of a different type (50.59(c)(2)(v)
  - Create the possibility for a malfunction of an SSC with a different result (50.59(c)(2)(vi)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

- Design Attributes
  - Can prevent or limit failures from occurring.
  - Focus primarily on built-in features
    - Fault detection
    - Failure management schemes
    - Internal redundancy
    - Diagnostics within the integrated software and hardware architecture
  - Can be external
    - For example: Mechanical stops or speed limiters

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

- Quality of the Design Process
  - Software development
  - Hardware and software integration processes
  - System design
  - Validation and testing processes
- For Safety Related:
  - Development process is documented and available for referencing in the Qualitative Assessment
- Commercial grade:
  - Documentation may not be extensive
  - Qualitative Assessment may place greater emphasis on Design Attributes and OE

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

- Operating Experience (OE)
  - Relevant OE: can be used to show that integrated software and hardware in a mod has adequate dependability
  - OE from nuclear industry
  - Supplier uses quality processes
    - Continual process improvement
    - Incorporation of lessons learned

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Failure Analysis

- Can be used to identify possible CCF vulnerabilities and assess the need to further modify the design.
- It can provide a valuable input into the Qualitative Assessment
- Key Areas to Consider:
  - Potential sources of CCF
  - Combination of design functions into a single digital device
  - Digital Communications
  - Creating new interactions with other SSCs
  - Interconnectivity across channels, systems, and divisions
  - Changing response times

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

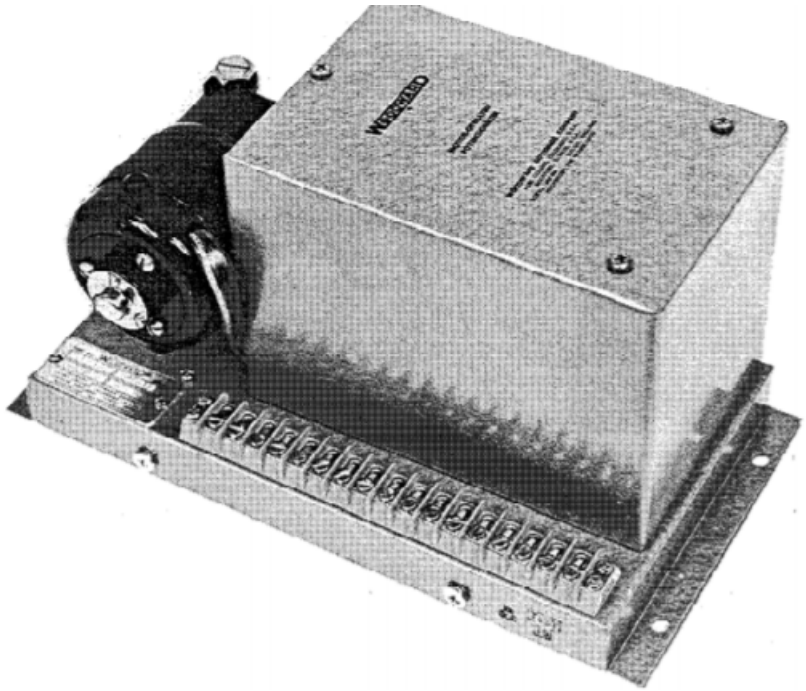
Digital Modification Examples

- Examples of digital modifications that can be done without prior NRC approval using a qualitative assessment:
  - Replacement of analog relays (including timing relays) with digital relays
  - Replacement of analog controls for safety-related support systems (i.e. main control room chillers)
  - Replacement of analog controls for emergency diesel generator supporting systems and auxiliary systems such as voltage regulation
  - Installation of circuit breakers that contain embedded digital devices
  - Replacement of analog recorders and indicators w/ digital
  - Digital upgrades to non-safety related control systems

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Example

Replacement of the Existing Electric Diesel Generator (EDG) Voltage Regulator Analog Motor-Operated Potentiometer (MOP) with a Digital Reference Adjuster (DRA)



Motor Operated Potentiometer

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Example

Replacement of the Existing EDG Voltage Regulator Analog Motor-Operated Potentiometer (MOP) with a Digital Reference Adjuster (DRA)

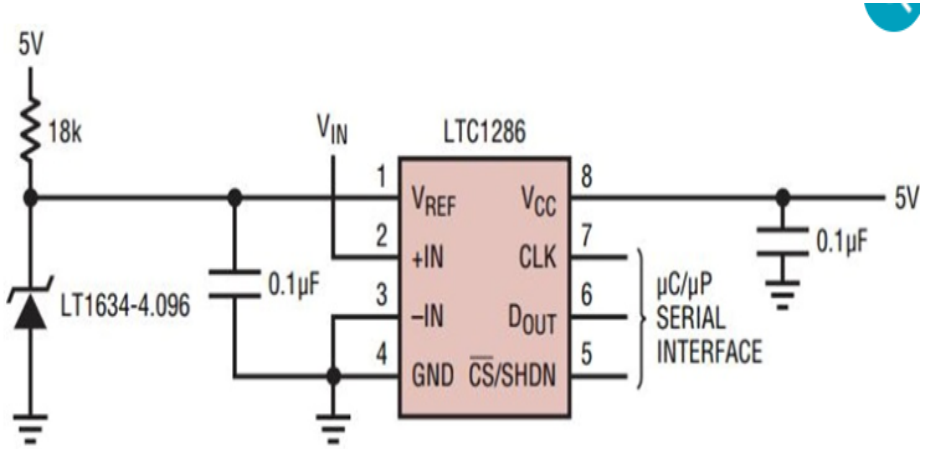


Figure 1. Typical use of a voltage reference for an ADC

Digital Reference Adjuster

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Example

Replacement of the Existing EDG Voltage Regulator Analog Motor-Operated Potentiometer (MOP) with a Digital Reference Adjuster (DRA)

- DRA will perform the exact same function as the MOP
- Failure modes are the same
    - Failure due to an internal defect
    - Failure due to a loss of power
    - Failure resulting from environmental factors
- Failure results in inoperability of the EDG

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Example

Design Attributes: The following design attributes were employed as part of the proposed design change to minimize failure likelihood:

- Use of a highly testable device
    - No Microprocessor
    - Two discrete outputs
    - Single input
    - Performs a single function w/ limited configurability
    - testable before and after installation using simple test methods
- Application of watchdog timers that function independent of the software
- Diverse indication of failure
- Use of the following barriers to prevent CCF:
    - environmental qualification
    - physical separation of equipment
    - absence of concurrent triggers
    - simple architecture
    - software quality and testability

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Example

Quality of the Design Process

- Commercial grade dedicated for use in safety-related applications using the guidance provided in EPRI TR-106439 (for digital) and EPTI 3002002982 (for commercial grade dedication)

- Qualified for temperature, humidity, and seismic stressors using EPRI TR-107330 (endorsed by RG 1.209)

- Qualified for electromagnetic compatibility IAW RG 1.180

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Example

Operating Experience

- Limited users of the DRA for EDG, but those users had many operating-years of experience with the DRA

- DRA is a quality product consistent with quality equal to or exceeding other non-digital setpoint adjustment devices (MOP)

- DRA eliminates the existing hardware common cause failure vulnerabilities of variable resistor wear and wiper to resistor corrosion of the MOPs

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI 96-07, Appendix D, "Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications"

- Submitted to NRC for endorsement in January 2019
- Gives greater detail to industry on how to conduct 50.59 screenings and evaluations for digital modifications.
- Provides examples.
- Complements NEI 96-07 guidance
- Will be endorsed by RG 1.187 revision
  - Possible exceptions in the endorsement

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Questions

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Back-Up Slides

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

50.59 Revised Rule

- Meaning of old rule language not clear/staff and industry differing interpretations
  - Established clear definitions to promote common understanding of the rule's requirements.
  - Clarified the criteria for determining when changes, test, experiments require prior NRC approval.
  - Provide greater flexibility to licensees, primarily by allowing changes that have minimal safety impact.
  - Clarified the threshold for "screening out" changes that do not require a full evaluation under 10 CFR 50.59

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

Design Attributes	• Defense-in-depth, diversity, independence, and redundancy (if applicable) • Inherent design features for integrated software and hardware or architectural/network (e.g., watchdog timers that operate independent of software, isolation devices, segmentation of distributed networks, self-testing, and self-diagnostic features) • Nonconcurrent triggers • Sufficiently simple (see NEI 01-01, Section 5.3.1) • Testability (e.g., highly testable) • Resolution of the possible failures identified in the failure analysis

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

Quality of the Design Process	Safety-Related Equipment: • Use of industry consensus standards shown to be applicable • Use of other standards shown to be applicable • Use of Appendix B vendors If an Appendix B vendor is not used, the analysis can state which generally accepted industrial quality program was applied. • Use of commercial-grade dedication processes in accordance with the guidance in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications," dated October 1, 1996. • Use of commercial-grade dedication processes in accordance with the guidance in Annex D to IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," and with the examples in EPRI TR-107330, " Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants" • Documented capability through qualification testing or analysis, or both, to withstand environmental conditions within which the SSC is credited to perform its design function (e.g., electromagnetic interference, radio-frequency interference, seismic activity) • Demonstrated dependability of custom software code for application software through extensive evaluation or testing

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

Non-safety Related Equipment:

- Adherence to generally accepted applicable commercial standards
- Procurement or manufacturer documentation, or both, showing that design specifications are met or exceeded for equipment being replaced

RIS 2002-22, Supplement 1, Attachment
Page 10 of 16

- Verification of design requirements and specifications

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Qualitative Assessment Factors

Operating Experience	• Operating experience in similar applications, operating environments, duty cycles, loading, and comparable configurations to that of the proposed modification • History of lessons learned from field experience addressed in the design • Referenced relevant operating experience should be equipment similar to that being proposed in the digital I&C modification. – Architecture of the referenced equipment and software (operating system and application) – Design conditions and modes of operation – Widely used high-quality commercial products with relevant operating experience used in other applications For software, limited use, custom, or user-configurable software applications can be challenging. – Experience with software development tools used to create configuration files

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Failure Analysis Resolution and Documentation

Table 2 Example: Failure Analysis Resolution and Documentation	
Topical Area	**Description**
Step 1— Identification	• Describe the scope and boundaries of the proposed activity, including interconnections and commonalities with other SSCs. • List the UFSAR-described design function(s) affected by the proposed change. • Describe any new design functions performed by the modified design that were not part of the original design. • Describe any design functions eliminated from the modified design that were part of the original design. • Describe any previously separate design functions that were combined as part of the activity. • Describe any automatic actions to be transferred to manual control. • Describe any manual actions that are to be transferred to automatic control. • Describe the expected modes of operation and transitions from one mode of operation to another.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Failure Analysis Resolution and Documentation

Step 2—Failure Mode Comparison	• Provide a comparison between the failure modes of the new digital equipment and the failure modes of the equipment being replaced. • If the failure modes are different, describe the resulting effect of equipment failure on the affected UFSAR-described design function(s). Consider the possibility that the proposed modification may have introduced potential failures: – Describe the effects of identified potential failure modes or undesirable behaviors, including, but not limited to, failure modes associated with hardware, software, combining functions, use of shared resources, software tools, programmable logic devices, or common hardware/software. – Describe the potential sources of CCFs being introduced that are also subject to common triggering mechanisms with those of other SSCs that are not being modified. • Explain how identified potential failures are being resolved (see NEI 01-01, Section 5.1.4.).
Step 3—Determination of Equipment Dependability and CCF Likelihood	Based on the qualitative assessment factors provided in Table 1, is the new digital equipment at least as reliable as the equipment being replaced?

Failure Analysis Resolution and Documentation

Step 4—Assessment of Equipment Dependability and CCF Likelihood Results	**IF** the results of Step 3 indicate that the new digital equipment is at least as dependable as the equipment being replaced or that the level of dependability is determined acceptable: • Document the bases for the conclusion. • Continue to Step 5. **IF** not, consider modifying the design or rely on existing design function backup capabilities.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Failure Analysis Resolution and Documentation

Step 5—Documentation	Summarize the results and overall conclusions reached. Discuss the effect of the proposed activity, if any, on applicable UFSAR-described design functions. Discuss the differences in equipment failure modes and the associated effects of different failure modes on applicable UFSAR-described design functions. Describe the incorporation of design attributes to resolve potential CCF vulnerabilities. Examples of supporting documents include the following: • Applicable codes and standards applied in the design • Equipment environmental conditions (e.g., ambient temperature, electromagnetic interference, radio-frequency interference, seismic activity) • Quality design processes used (e.g., Subpart 2.7 of Part II of American National Standards Institute/American Society of Mechanical Engineers NQA-1, "Quality Assurance Program Requirements for Nuclear Power Plants") • Commercial-grade dedication documentation, such as described in EPRI TR-106439 (if applicable) • Failure modes and effects analysis (if applicable) • Software hazard analysis (if applicable)