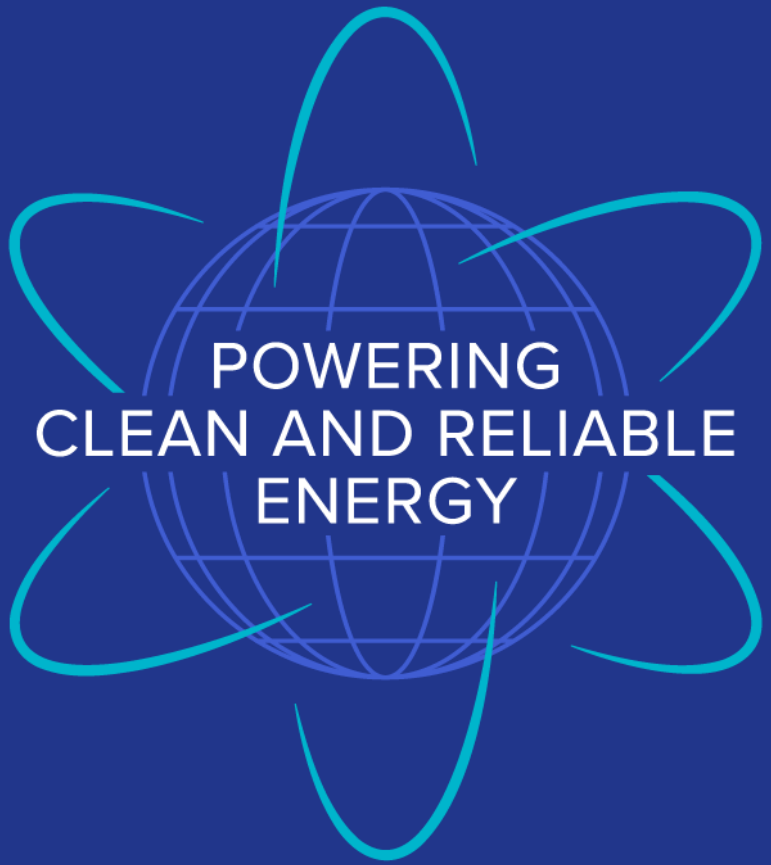
Digital I&C Workshop

ADVANCE Act and EO14300 Recommendations

NEI Digital I&C Working Group and Task Force

Alan Campbell
Technical Advisor

February 13, 2026



NUCLEAR ENERGY INSTITUTE

Common Cause Failure

The Issue

- No NRC-approved guidance exists for addressing the software CCF likelihood in redundant RPS and ESFAS equipment
- As a result, licensee are expected to assume a software CCF when upgrading redundant RPS/ESFAS equipment from analog to digital
- Assuming a software CCF in redundant RPS/ESFAS equipment will require a LAR to implement the change in most cases
- Industry is proposing development of guidance for addressing software CCF failure likelihood that can be used for RPS and ESFAS
- This presentation provides the proposed methodology and path forward for addressing software CCF likelihood for RPS and ESFAS equipment

Existing NEI 01-01 Guidance

- NEI 01-01 describes the use of an engineering analysis for addressing software CCF in redundant RPS/ESFAS digital upgrades (NEI 01-01 example provided on the next slide)
- However, NEI 01-01 does not provide specific details on the content to be included in an engineering analysis to address software CCF in redundant RPS/ESFAS equipment
- Because RIS 2002-22 Supplement 1 excludes RPS/ESFAS, there is no NRC-approved methods to address software CCF when implementing a digital upgrade to redundant RPS/ESFAS equipment

Example 4-8. Results of Malfunctions for a PLC Upgrade

The load sequencer in Example 4-6 monitors the 1E electrical distribution system voltage and sheds loads in response to an undervoltage condition, allowing the EDGs to come to rated speed and voltage. Loads are then sequenced back on line based on the ESF actuation signals provided to the sequencer from the ESFAS logic system. All ESF actuation signals are processed by the load sequencer so that if the sequencer fails, no ESF equipment will start.

A FMEA of the PLC system identified a limited number of possible single failures that are not detected by the system, but that can be detected by application-specific design features. In the design of the sequencer application, additional failure analysis was performed and results were used in the design to reduce the consequences of certain postulated failures.

In addressing Criterion 2, the quality, dependability, and enhanced capabilities of the digital system are evaluated in the context of the evaluation. The upgrade uses a pre-qualified PLC platform that has been shown to be a high quality, highly dependable system, as documented in an SER summarizing the review performed by the NRC. In a comparison to the equipment being replaced, it is shown that many hardware vulnerabilities have been eliminated, and self-test and diagnostic capabilities have been added. The qualitative assessment concludes that the net result is a decrease in the likelihood of failure of the system, so that the "minimal increase" threshold of Criterion 2 has not been challenged.

In addressing Criterion 6 in regard to potential software common cause failures, both the embedded software in the PLC and the application-specific or "configuration" software are considered. Evaluations performed during the pre-qualification efforts established assurance that the quality of the embedded software is such that the likelihood of failure is acceptably low. The application-specific software has been developed and tested under Appendix B QA processes, utilizing configuration tools that are designed specifically to minimize the likelihood of introducing errors. The conclusion of the qualitative assessment is that the likelihood of a software common cause failure is much less than that of other events considered in the UFSAR and therefore software common cause failure is not considered a possible malfunction with a different result (as discussed in NEI 96-07, Revision 1).

This example from NEI 01-01 illustrates a digital upgrade to ESFAS equipment where the same software is used in redundant divisions.

Based on use of a pre-qualified PLC and application software quality, it was concluded that the likelihood of software CCF is much less than that of other events considered in the UFSAR (i.e., sufficiently low).

As a result, software CCF was not considered a possible malfunction with a different result.

NEI 01-01 Section 4.4.6

Software Common Cause Failures: Engineering evaluations of the quality of the design processes determine if there is reasonable assurance that the likelihood of failure due to software is sufficiently low. In this evaluation, “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). Results of this evaluation are then used to determine whether failures due to software, including common cause failure, should be considered further in the 10 CFR 50.59 evaluation. If there is reasonable assurance that the likelihood of failure due to software is sufficiently low, then the upgrade would not require prior NRC review on the basis of common cause failure.

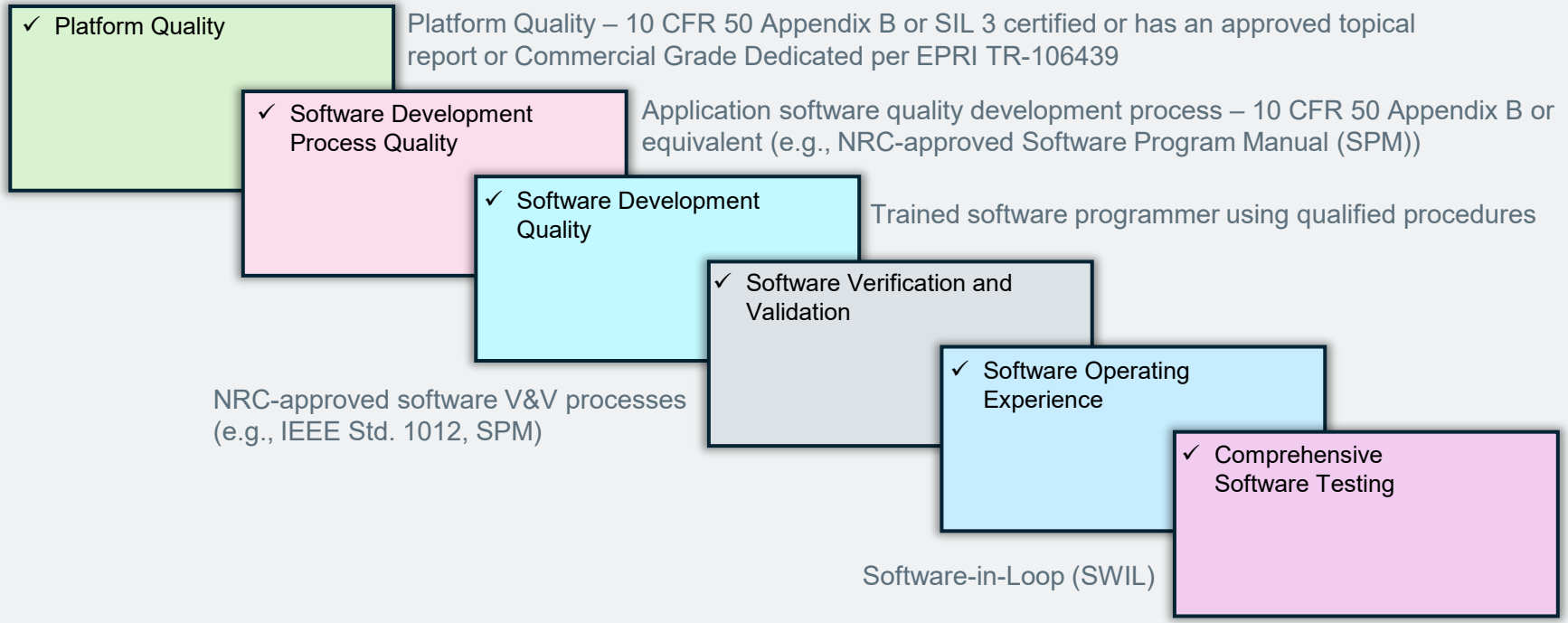
Based on the Guidance in NEI 01-01…

- An engineering analysis can be used to address software CCF in redundant RPS/ESFAS equipment
- If the engineering analysis concludes that the likelihood of a software CCF is comparable to other CCFs not considered in the UFSAR (design flaws, maintenance errors, calibration errors), then the upgrade would not require prior NRC review because of common cause failure
- In other words, a software CCF would no longer need to be assumed in the 10 CFR 50.59 review process

Proposed Engineering Analysis Characteristics

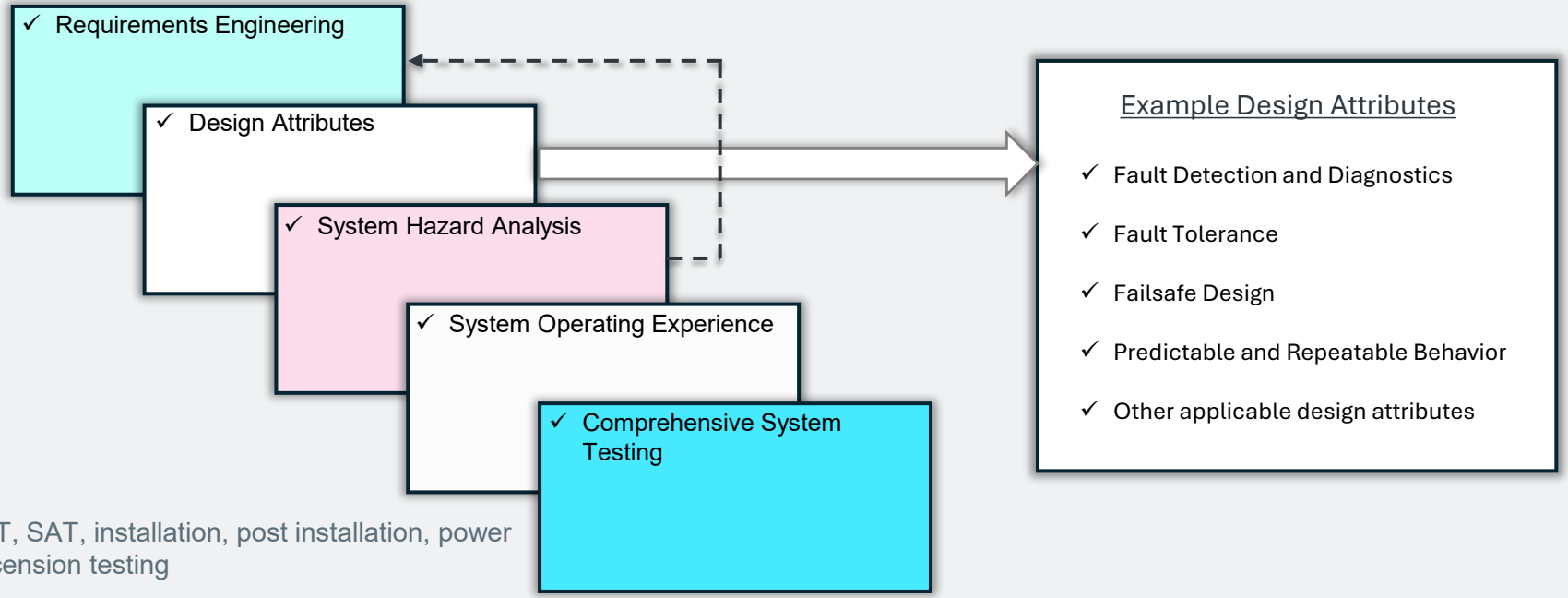
- The core elements for addressing software CCF in RPS/ESFAS are:
  - ✓ ***Quality*** of the platform and application software development
  - ✓ ***Functional Safety*** of the integrated system
- The proposed elements of an engineering analysis to assess platform and application software ***quality*** and ***functional safety*** of the integrated system are presented in the following slides

Elements of the Software Development Quality Part of the Analysis for RPS/ESFAS



✓ *The engineering analysis will document the pertinent information for each phase of the software development process used to justify the software quality conclusions*

Elements of the Functional Safety Part of the Analysis for RPS/ESFAS



✓ *The engineering analysis will document the applicable artifacts for each phase of the integrated system design and testing used to justify the functional safety conclusions*

Proposed Resolution

- Industry will define the engineering analysis content and criteria necessary to assess quality and functional safety when implementing digital upgrades to redundant RPS/ESFAS equipment
- The engineering analysis will be used to determine if the software development quality and functional safety of the integrated system are sufficient to conclude the likelihood of software CCF is comparable to the likelihood of other CCFs not considered in the UFSAR (design flaws, maintenance errors, calibration errors)
- If the engineering analysis concludes the RPS/ESFAS quality of the software development meets the defined software quality thresholds and functional safety meets the defined functional safety thresholds, then software CCF need not be further considered in the 10 CFR 50.59 review

Recommended Actions

Industry

1. Repurpose NEI 20-07 to provide specific guidance on development of an engineering analysis for addressing software quality and functional safety in redundant digital RPS/ESFAS equipment
2. Move the guidance in RIS 2002-22 Supplement 1 into NEI 96-07 Appendix D

NRC

1. Use RG 1.187 to endorse Appendix D with the RIS guidance included and to endorse NEI 20-07 for use as an engineering analysis to address software CCF for RPS/ESFAS
2. Retire the existing CCF policy (SRM SECY 93-087 and SRM SECY 22-0076) and BTP 7-19

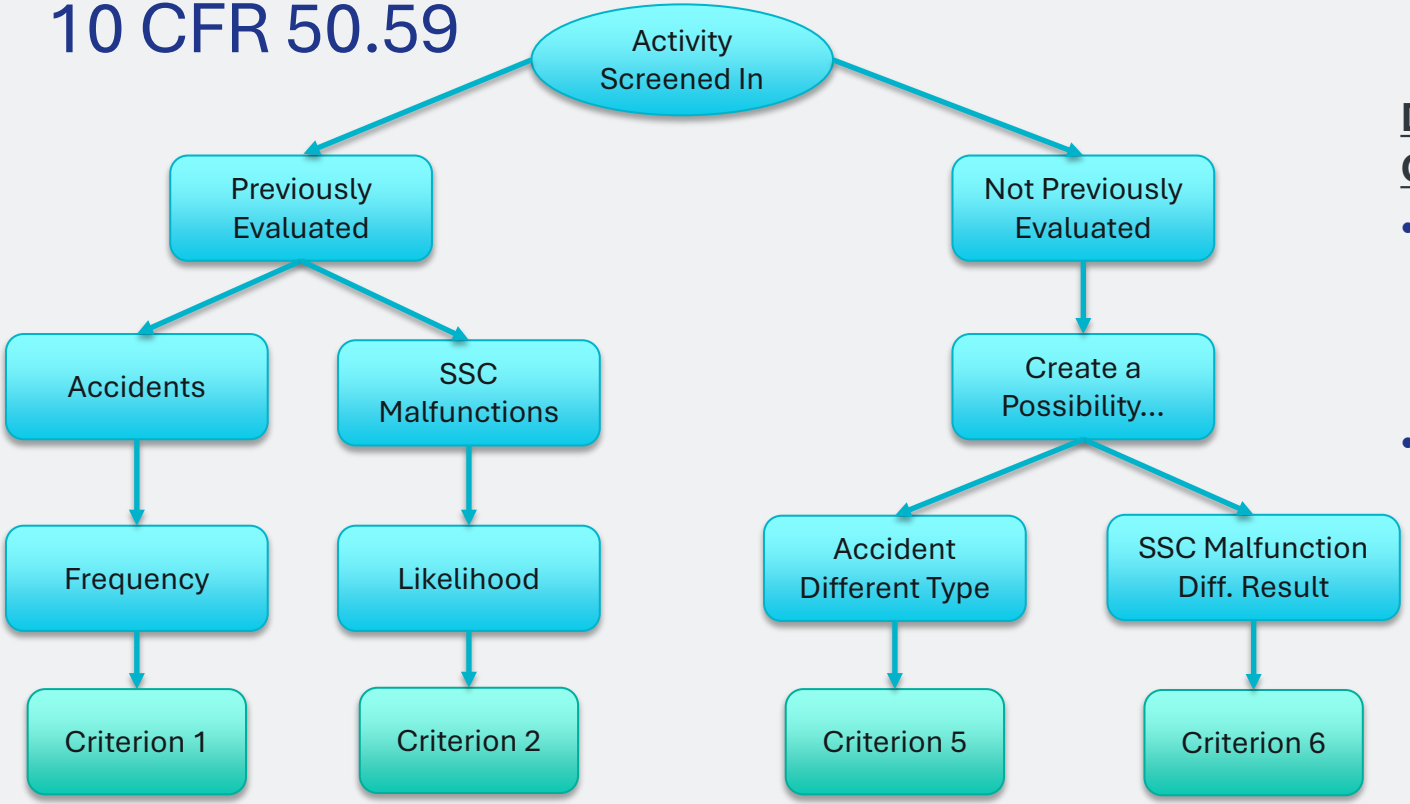
Focused License Amendment Reviews

Focused LAR Reviews

Drivers

- LAR reviews must be able to be accomplished within NEIMA schedule requirements
  - No more than 12 months
- Need to be able to support multiple concurrent reviews
- Previously discussed, CCF should not drive need for a LAR
  - Use engineering analysis to demonstrate sufficiently low likelihood
  - 10 CFR 50.59 excludes Beyond Design Basis Events
- What should drive the need for a License Amendment Request for a digital modification?
  - 10 CFR 50.59 evaluation criteria

10 CFR 50.59



Digital Specific Criteria

- Criterion 1 and 5 - Accidents (Frequency and Type)
- Criterion 2 and 6 - SSC Malfunctions (Likelihood and Diff. Result)

Focused LAR Reviews

Digital I&C and HFE Considerations

- What should drive the need for a License Amendment Request for a digital mod?
- Examples:
  - Reductions beyond the level credited in the UFSAR in:
    - Separation
    - Independence
    - Redundancy
    - Diversity
  - Changing an automatic action to a manual action
  - Adverse impact to safety analysis response time assumptions
    - Based on equipment response OR operator response

Focused LAR Reviews

Content Impacts

- License Amendment Request contents should focus on the safety significant aspects of the design
  - Focus on the element(s) that cannot be addressed under 10 CFR 50.59 (or similar licensing processes)
- Technical issues that can be addressed through normal plant processes should not require LAR submittal. Examples:
  - Equipment Qualification
  - Human Factors Engineering
  - Calculations
  - Vendor Quality Oversight
  - Cyber Security

Focused LAR Reviews

Next Steps

- NEI suggests future public meetings in 1Q26 and 2Q26 to discuss revision to digital LAR guidance (currently in DI&C-ISG-06)
- Objectives:
  - Revise guidance to allow flexibility for licensees to only provide the information necessary based 10 CFR 50.59 evaluation (or similar licensing guidance)
    - Focus on safety outcomes
  - Move guidance out of interim staff guidance and into more durable staff guidance document

Codes and Standards

Codes and Standards

IEEE 603 Rulemaking

- NEI Recommendation
  - Eliminate 10 CFR 50.55a(h)
  - Regulatory basis becomes the GDCs
  - Revise RG 1.153 to endorse the safety criteria standards (IEEE 279, IEEE 603)
    - Exclude CCF – IEEE 279 and 603 are technology neutral standards, NRC CCF policies are specific to digital

Codes and Standards

Basis for eliminating 10 CFR 50.55a(h)

- Remove unnecessary duplication of regulatory requirements
  - GDCs use IEEE safety criteria standards as acceptance criteria
- Consistency with all other IEEE standards
  - Every other IEEE standard (including the power system safety criteria) is endorsed via Regulatory Guide.
- SRM-SECY-98-0144
  - Commission directed the transition to risk-informed, performance-based regulation
- Ease of maintenance
  - Does not require rulemaking once removed

Codes and Standards

Unnecessary Duplication

Example from NUREG-0800, Chapter 7, Appendix 7.1-A

(i) GDC 20, "Protection System Functions"

"The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to ensure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety."

Applicability - The protection systems, RTS, and ESFAS.

Review Methods – The review of compliance with GDC 20 should address the characteristics listed in the table below. These characteristics are described in IEEE Std 279-1971 and IEEE Std 603-1991, and methods for reviewing them are discussed in SRP Appendix 7.1-B and SRP Appendix 7.1-C (see table below for sections).

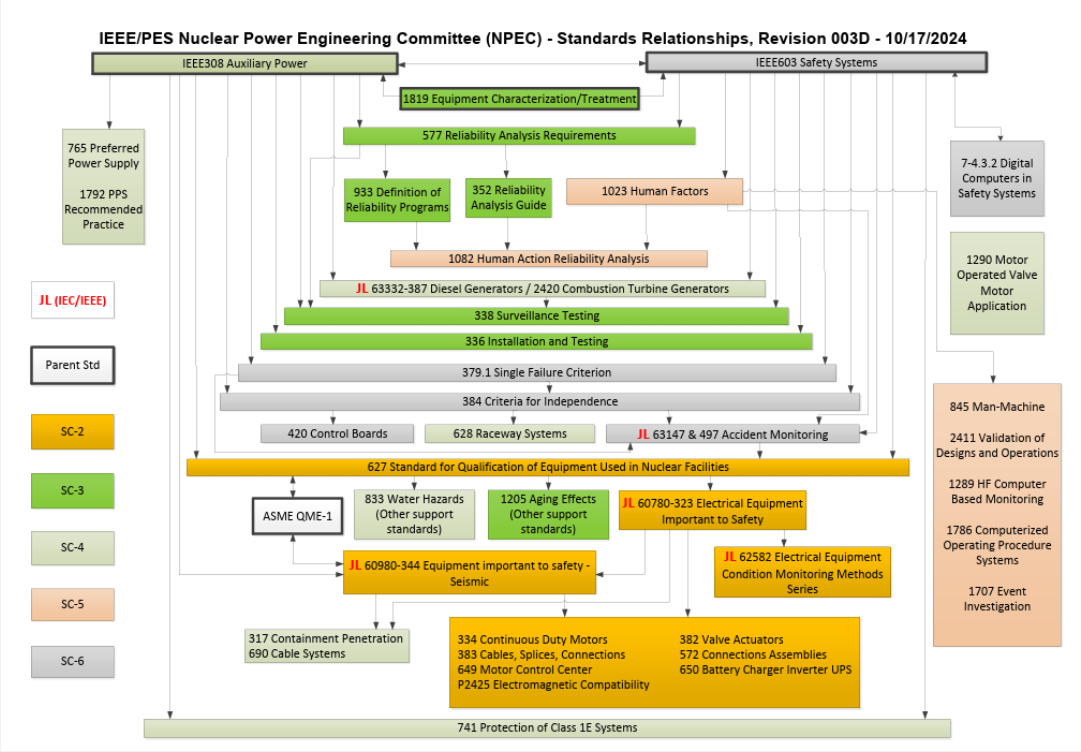
Characteristic	Review Guidance	
	SRP Appendix 7.1-B	SRP Appendix 7.1-C
Design basis requirements	Section 3	Section 4
General functional requirements	Subsection 4.1	Subsections 5, 6.1, and 7.1
System integrity	Subsection 4.5	Subsection 5.5
Setpoints	Subsections 3 and 4.15	Subsection 6.8

The evaluation of conformance to this requirement should be addressed in the review of Sections 7.2 and 7.3 of the SAR.

Codes and Standards

Consistency with IEEE Standards

- Example of “sister standard” to IEEE603
  - IEEE 308-2020 is endorsed via RG 1.32
- Publicly available graphic (https://site.ieee.org/pes-npec/npec-standards/)



Codes and Standards

Recommended Actions

- NRC - EO14300 rulemaking to eliminate 10 CFR 50.55a(h)
- NRC - Update RG 1.153 to endorse as acceptable standards to meet GDCs
  - IEEE 279-1968
  - IEEE 279-1971
  - IEEE 603-1991
  - IEEE 603-2018
- NRC – In future updates to other referenced RGs, update regulatory basis to remove 10 CFR 50.55a(h).

Back-Up Slides

Functional Safety Definition

The term "*Functional Safety*" is used in industry standards and within the EPRI systems engineering framework for digital design guidance (e.g., DEG, HAZCADS, DRAM)

From IEC 61508-2010:

Functional safety – Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.

EUC = Equipment Under Control
E/E/PE = Electrical/Electronic/Programmable Electronic Systems