Handout to Discuss Proposed Regulatory Use of NEI 16-16

This is a draft document to facilitate discussions between NEI and the NRC to:

- Reach alignment between NEI and NRC on the regulatory purpose/intent of NEI 16-16.
- Reach alignment between NEI and NRC on the regulatory requirements that NEI must meet for endorsement of NEI 16-16.
- Clarify the path-forward for NEI 16-16 endorsement review.

Discussion Questions and Comments

1. What is the scope and intended use by NRC licensees for NEI 16-16 in the near-term and long-term?
   - Support the licensing basis of future license amendment requests?
   - Address the technical analysis to support the 50.59 conclusion of "CCF Sufficiently Low" in draft NEI 96-07, Appendix D?
   - Address the appropriate design attributes, quality design process, and operating experience for qualitative assessments described in the draft RIS supplement to RIS 2002-22?
   - Eliminate or modify the need for a D3 analysis for specific types of DI&C components and systems (e.g. as described in Section 3 of BTP 7-19)? Which components and systems?

2. What are the applicable requirements that NEI 16-16 is intended to address? The regulatory requirements listed on page 2 of this document may provide some insight.

3. Is NEI proposing that an existing regulatory guide be updated or that a new regulatory guide be created?
   - Update Regulatory Guide 1.152 "Criteria for Digital Computers in Safety Systems in Nuclear Power Plants" or another Regulatory Guide to include guidance contained in NEI 16-16?
   - Create of new regulatory guide that provides one way of addressing regulations that include those listed in "Regulations pertinent to D3 and Diversity" on page 2 of this handout?

4. Is NEI claiming that NEI 16-16 is consistent with SRM 93-087 and BTP 7-19?
   - NEI 16-16 states: "This document provides technical guidance for addressing CCF for compliance to deterministic licensing criteria and NRC policies and positions such as "SRM-SECY-93-087 and BTP 7-19. See NEI 16-16, Draft 2, page 1.
   - NRC has received industry comments for updating BTP 7-19? The staff is reviewing these comments. The MP1C team is developing a SECY with recommendations for updating NRC's policy on protection of DI&C components and systems.
   - It seems that BTP 7-19 would need to be revised if NEI 16-16 is endorsed? See section 1.9 of BTP 7-19?

5. Is NEI proposing a method to eliminate the need for a D3 analysis for specific types of DI&C components and systems? If so, which components and systems?

Regulations pertinent to D3 and Diversity

NRC's regulatory basis for defense-in-depth and diversity are embodied in these regulatory requirements. These regulations are cited in Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" or BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems Review Responsibilities. Regulations below, among others[1], capture the primary regulations that the staff is considering in the review of NEI 16-16.

- 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," requires in part various diverse methods of responding to ATWS.
- GDC 21, "Protection system reliability and testability."
- GDC 22, "Protection System Independence,"
- GDC 24, "Separation of Protection and Control Systems,"
- GDC 29, "Protection against Anticipated Operational Occurrences,"
- 10 CFR 50.55(a)(h) incorporated by reference …
    - IEEE Std 603-1991, Clause 5.1, requires in part that "safety systems shall perform all safety functions required for a design-basis event (DBE) in the presence of any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures."
    - IEEE Std 603-1991, Clause 6.2, "Manual Control," requires in part that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions.
    - IEEE Std 279-1971, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."
    - IEEE Std 279-1971, Clause 4.17, "Manual Initiation," requires in part that the protection system shall include means for manual initiation of each protective action at the system level.

There are no regulations that explicitly articulate the requirement for protection against digital CCF. Criteria for addressing common cause failure (for safety functions) for satisfying the above regulatory requirements, is primarily described in BTP 7-19 for licensing actions, and derived from the policy established by the commission in SRM-SECY 93-087 [ML003708056]

Common cause failure acceptance criteria (BTP 7-19)

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have adequately been addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different

[1] This document is not intended to capture or fully articulate all regulations pertinent to D3 and Diversity nor to articulate all regulations that implicitly require protection of DI&C components and systems against CCF concerns. There are other pertinent regulations that address protection against CCF concerns in DI&C components and systems.

function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

   Inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis.

   In addition, *BTP 7-19 identifies two means* to eliminate consideration of CCF from further consideration without the need for a D3.

   - Sufficient Internal Diversity
   - 100 % Testability
   - *Is NEI proposing an additional means beyond Sufficient Internal Diversity and 100% testability listed in BTP 7-19, Revision 7?*
   - *Can specific means proposed by NEI be listed in this portion of the document?*

   These means are evaluated on a case-by-case basis and there are no specific criteria for sufficient internal diversity.

Note:
Regulatory Guide 1.152, Revision 3 endorses IEEE Std. 7-4.3.2-2003 to satisfy NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. Other means exist (e.g., manual actions, external diversity, etc.).