From:	VAUGHN, Stephen
To:	Morton, Wendell
Cc:	Govan, Tekia; Paige, Jason
Subject:	[External_Sender] NEI High-level comments on BTP 7-19
Date:	Thursday, March 21, 2019 4:36:08 PM
Attachments:	BTP 7-19 NEI High Level Comments - Rev 4.pdf

Wendell,

As promised...attached are some high-level comments that the NEI Digital I&C working group put together. Over the next two weeks (in preparation for the 4/4 public meeting) the industry team will be adding to these slides and adding more detail, etc.

Regards,

Steve

STEPHEN J. VAUGHN | *SENIOR PROJECT MANAGER, ENGINEERING AND RISK*

1201 F Street, NW, Suite 1100 | Washington, DC 20004

P: 202.739.8163 M: 202.256.5393

sjv@nei.org

Sent through www.intermedia.com

MP1D – BTP 7-19 Revision

NEI Proposed Changes

March 21, 2019

The Goal of MP 1D

- MP 1D Purpose: Revise BTP 7-19 to provide clear guidance to the staff on the appropriate scope and boundaries when evaluating CCF and associated defense-in-depth and diversity analyses.

- BTP 7-19 should be limited to the Reactor Protection System (RPS) logic and the regulatory guidance should be:

  - Risk-informed

  - Use a graded approach

Background

- Branch Technical Position (BTP) 7-19 provides the staff review guidance to implement Digital I&C guidance in SRM-SECY-93-087.
- There have been three revisions of BTP 7-19 from 1997 to 2012.
  - Revision 4 (1997) is 8 pages, Revision 5 (2007) is 9 pages, and Revision 6 (2012) is **28** pages
- Over that time period, the scope of BTP 7-19 was expanded to include auxiliary supporting features
- After Revision 4, validated operator actions were eliminated:
  - Credit of primary/secondary leak detection and pre-defined operating procedures, that together, can enable operators to take corrective actions before a large break (LBLOCA/MSLB)

NEI Proposed High Level Changes

- Title:
  - Move Diversity after Defense-in-Depth to de-emphasize diversity and emphasize Defense-in-Depth
    - Emphasizing Defense-in-Depth focuses on whether the digital protection system change affected other layers of defense (i.e., control system and monitoring/manual control)
    - Emphasizing Diversity detracts on the primary focus
  - Consider changing the title completely (e.g., "Evaluation of Digital Reliability")
- Background:
  - Refers generally to "digital protection systems" but should be limited to Reactor Protection System logic.

NEI Proposed High Level Changes

- BTP 7-19, Section 1.4, "Four-Point Position"

  - Include text to credit defensive measures and non-concurrent triggers
  - Existing coping analyses (e.g., Station Blackout) should be leveraged as appropriate to assess consequences
  - Move away from the premise that a CCF "could" disable a safety function and embrace risk-informed concepts of likelihood and consequence
  - Text should be revised to reflect risk-informed coping mechanisms for LBLOCA and MSLB

NEI Proposed High Level Changes

- Section 1.6, "D3 Assessment"

  - More flexibility should be added to use other beyond design basis strategies and methods (e.g., FLEX, B.5.b, etc.)

NEI Proposed High Level Changes

- Section 1.7, "The Diverse Means"
  - Control of equipment outside the main control room (MCR) should be acceptable for mitigation of CCF, which is a beyond design basis event

- Section 1.8, "Potential Effects of CCF: Failure to Actuate and Spurious Actuation"
  - Introduction of spurious actuation CCF modes has the real potential to lead to a seemingly endless "what if" analysis
  - Should be limited only to failures to actuate.

NEI Proposed High Level Changes

- Section 1.9, "Design Attributes to Eliminate Consideration of CCF"
  - Defensive measures must be considered:
    - Independent watchdog timers
    - Non-concurrent triggers
    - The use of very structured module software can be used to support likelihood of CCF decisions or be credited as a sufficient defensive measure (e.g., IEC-style function blocks are extensively tested with a large amount of OE)

NEI Proposed High Level Changes

- Section 3.1, "Specific Acceptance Criteria"
  - Point 9 demonstrates the added complexity which can force an I&C architecture to add a diverse actuation system (DAS)
    - Adding a DAS can increase the overall plant risk due to added complexity
- Section 3.7, "Effects of Spurious Actuation Caused by CCF"
  - See earlier discussion for Section 1.8
- Section 3.9, "System Testability"
  - See earlier discussion for Section 1.9

NEI Proposed High Level Perspective Changes

- Section 4.7, "Justification for Not Correcting Specific Vulnerabilities"
  - Later versions removed guidance that allowed a risk-informed, graded approach in performing a CCF coping analysis:

- Earlier versions suggested that a CCF unlikely conclusion was possible based on reasonable application of prevention and limitation measures

Conclusions

- BTP 7-19 guidance should:

  - Be risk-informed and use a graded approach
  - Be more general to restore flexibility and simplify the assessment of certain CCF modes
  - Include other industry-recognized defensive measures to preclude a CCF (e.g., independent watchdog timer, logic corruption detection, and other extensive diagnostics)