From: VAUGHN, Stephen
To: Morton, Wendell; Govan, Tekia
Subject: [External_Sender] NEI Comments on BTP 7-19 Revision
Date: Wednesday, May 15, 2019 8:35:08 AM
Attachments: Industry Feedback on BTP 7-19-Rev 4.docx

Wendell and Tekia,

Please find the attached Word file that contains feedback on BTP 7-19 from the NEI Digital I&C working group based on discussions at the 1/31/19 and 4/4/19 public meetings.

We look forward to seeing the draft Revision 8 to BTP 7-19 in June and our next public interaction to provide more detailed feedback on the risk-informed and graded approach.

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

Industry Feedback on BTP 7-19

Section 1.5 “Manual Initiation of Automatically Initiated Protective Actions Subject to CCF”

- Concerns
  - Section 1.5 notes that Clauses 6.2 and 7.2 of IEEE 603-1991 state “a safety-related means shall be provided in the control room to implement manual initiation of the automatically initiated protective actions at the division level.” Industry, including members of the subcommittee responsible for the standard, note that Clauses 6.2 and 7.2 applies to design basis events, and does not address criteria for beyond design basis events (i.e., CCF)
- Recommendations
  - Clarify that outside the control room manual actions to initiate diverse protective actions to address CCF are permitted.

Section 1.8 “Potential Effect of CCF: Failure to Actuate and Spurious Actuations”

- Concerns
  - The scope of spurious actuations caused by a software CCF is not technically bounded
- Recommendations
  - Limit the scope of spurious actuations to be considered in the analysis using a reasonable set of criteria given that software CCF is a beyond design basis event

Section 1.9 “Design Attributes to Provide Reasonable Assurance that CCF Has Been Adequately Considered”

- Concerns
  - 100% Testing is not feasible for complex digital projects that involve software; therefore it is not feasible to use
  - Testability and diversity, as the only two options to adequately address CCF, are not effective
- Recommendations
  - Change the guidance for Testability and add an option for Defensive Measures:
  - Testability – [Based on IEEE 7-4.3.2-2016 technical guidance] In conjunction with the testing expected in NRC regulatory guides 1.152 and 1.168, a system or component can be extensively tested to provide reasonable assurance that the system or component is not susceptible to CCF. The following individual criteria would be used:
    - Throughout testing, allocated outputs are monitored for correctness (with respect to a reference of acceptable behavior) during testing for each of the test criteria objectives.
    - The separate test criteria applied are as follows:
      - Every possible combination of discrete inputs that are used by the logic (unused discrete inputs that are forced to a known state are excluded from this criteria)

                - The operational range of the analog inputs, with specific “at”, “below”, and “above” analog values that result in changes of logical state; as well as values “above” and “below” the operational range of the analog inputs (unused analog inputs that are forced to a known state are excluded from this criteria);
                - Every logic path (this includes non-sequential logic paths);
                - Every functional state transition for each state machine or logical group of state machines.
                - Any unreachable logic as a result of these tests will require further analysis to determine potential hazards
            - The applicant should demonstrate that unused inputs cannot cause transition, mode, or configuration changes in the system or component.
            - This testing should be conducted with test hardware representing the production hardware.
        - Defensive Measures –
            - Inherent design features
                - Independent watchdog timers
                - Isolation devices
                - Segmentation
                - Self-testing/self-diagnosing
            - Non-concurrent triggers
            - Structured module software and module testing
        - The three design attributes of Testability, Diversity, and Defensive Measures should be considered in the aggregate to make a reasonable technical determination that CCF has been adequately addressed and does not need to be considered any further (i.e., no need to provide additional external diversity.)

Section 3.1(8)b “Specific Acceptance Criteria”

- Concerns
    - States that the diverse means should be initiated from the control room, which would include operator actions
- Recommendations
    - State that the diverse means, which would include operator actions, could be initiated outside of the control room.

Section 3.1(9) “Specific Acceptance Criteria”

- Concerns
    - The scope of spurious actuations caused by a software CCF is not technically bounded
- Recommendations
    - Limit the scope of spurious actuations to be considered in the analysis using a reasonable set of criteria given that software CCF is a beyond design basis event

Section 3.5 “Use of Manual Action as a Diverse Means of Accomplishing Safety Functions”

- Concerns

    - The paragraphs in Section 3.5 are disconnected and do not clearly describe the expectations in using manual actions as a diverse means to accomplish safety functions.
- Recommendations
    - Change the language in Section 3.5 to read:

      "If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, a suitable HFE analysis should be performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postulated accident. When manual actions are credited and are required in less than thirty minutes, the applicant must justify that the time available and time required for the operator action to maintain the recommended acceptance criteria for the particular AOO or postulated accident is feasible and reliable. The acceptability of such actions is to be reviewed by the NRC staff taking into account the applicant's existing operating and emergency procedures already in place that would be invoked to respond to such a beyond design basis event.

      The applicant must demonstrate that these manual actions are independent of the automatic actuation system with the postulated CCF. SRP Chapter 18, Revision 3, Attachment A, "Guidance for Evaluating Crediting Manual Operator Actions," provides various methods available to the applicant to justify the feasibility and reliability of credited operator actions including diverse manual operator actions to cope with CCF. Attachment A does not limit these manual actions to the control room. Similar to FLEX strategies for beyond design basis events, the applicant may make the justification that there is sufficient time to use manual operator action reliably outside of the control room to maintain plant conditions within the recommended acceptance criteria for the particular AOO or postulated accident."

Section 3.7 "Effects of Spurious Actuation Caused by CCF"

- Concerns
    - The scope of spurious actuations caused by a software CCF is not technically bounded
- Recommendations
    - Limit the scope of spurious actuations to be considered in the analysis using a reasonable set of criteria given that software CCF is a beyond design basis event

Section 4.7 "Justification for Not Correcting Specific Vulnerabilities"

- Concerns
    - Revision 4 to BTP 7-19 had guidance regarding LBLOCA and MSLB and Revision 7 does not.
- Recommendations
    - Use the language below for Section 4.7 "If any identified vulnerabilities are not addressed by provision of alternate trip, initiation, or mitigation capability, justification should be provided. Justification may be based upon the availability of systems outside of the scope of the analysis that act to prevent or mitigate the event of concern. For example, I&C system vulnerability to CCF affecting the response to large-break loss-of-coolant accidents and main steam line breaks can credit existing primary and secondary

coolant system leak detection, including pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs."

Graded Approach

- Concerns
  - The A1 definition (part (2)) can have a wide scope because it does not clearly define a "support" system
  - Under A2 and B1 of the graded approach the CCF evaluation is a Defense-in-Depth/Qualitative Assessment. Is the Defense-in-Depth analysis limited to the Defense-in-Depth discussion in RIS 2002-22, Supplement 1 (End of Section 4.2 "Failure Analysis" on page 12 of 16)? If it is something beyond that, what defines a Defense-in-Depth analysis?
- Recommendations
  - Replace the existing NRC definition with the "Industry revised definition" below:

  A1: Safety-related system (1) that plays a principal role in the achievement or maintenance of nuclear power plant safety to prevent a DBE from leading to unacceptable consequences. ; or (2) whose failure could directly lead to accident conditions which may cause unacceptable consequences if not mitigated by other A1 systems. [adapted from IEC 61226 Ed. 3]
  - Clarify what is expected for a Defense-in-Depth analysis for A2 and B1 categories.

General

- Concerns
  - Some topics have guidance dispersed throughout the document in multiple sections, which makes the concepts difficult to understand. For example, manual operator actions are discussed in Section 1.5, Section 1.7, Section 3.1(8), and Section 3.5.
- Recommendations
  - Where appropriate, consolidate concepts to a limited number of sections for simplicity and overall clarity.