

DI&C-ISG-05, Revision 1 Industry Comments

Computerized Procedures

1. General comment: Consider deleting the word “always” where it is unnecessary or unclear:
 - Page 2 of 24 Item 2.
 - Page 3 of 24 Item 3.
2. The industry does not agree with the requirements of Item 9. There is no logical difference between prompting and selection, and in specific cases the automation system should be able to select and display a procedure for the operator. For example, when the system receives an input that a reactor trip has occurred the system should be allowed to display the reactor trip response procedure without operator prompting. The operator’s “remaining in control” is adequately covered by Item 10, such that Item 9 could be deleted.
3. Item 12, “Procedure steps that call for the operator to make a decision.” Add: that requires judgment or expert knowledge that is not readily available in the computer.
4. Item 14 is too general. Consider restating as, “Soft controls are computer based interface elements that users can manipulate to perform actions that operate plant equipment”. Industry use of the term “soft controls” is analogous to hardware-based *component* controls. Selecting options and setting values are generic input elements of a graphical interface. Calling these generic input elements “controls” whether or not they operate plant equipment is confusing. Soft controls are input elements, but all input elements are not soft controls.
5. Item 15: To clarify and be consistent with the first sentence below Soft Control Review Criteria, consider replacing the first sentence of Item 15 with, “The function of a soft control should be obvious to the user”.
6. (deleted)
7. Item 19: Consider referring to “soft controls” instead of “computerized procedures”. The guidance applies to soft controls, with or without CPs, and so the means for error recovery are generally the same in both cases.
8. Item 25 remove the word “all”. This list includes many administrative procedures not used by control room staff such as Emergency Preparedness and severe action mitigation procedures. The list of procedures should be those needed in the control room for safe mitigation of an event. Consider rewriting the first sentence as follows: "Backup procedures should be maintained to ensure the ability to perform accident mitigation and safe shutdown."
9. Item 13: The underlying intent of the guidance is unclear. The bullets mainly identify monitoring and logical evaluation features. Aside from those already addressed by Item 12, these features may be more relevant to manual than to automated procedure execution. In addition, though desirable, such features are not necessary for a manual CP to fulfill the role of paper-based EOPs. Please clarify the type of CP system that is the object of these criteria.
10. Item 20: Consider changing the words “should include plant-specific standards”, to the words, “be compatible with plant-specific conventions”.
11. Item 22: Suggest replacing the word “change” with “modify”.

12. Item 26: Suggest replacing the words, “that is timely for their use”, with the words, “that permits timely use.”
13. Items 28, 29 and 30 under Backup Procedures Review Criteria: Consider combining these three items and rewriting to clarify that this guidance is related to ensuring that the operators can easily transition to backup procedures if the computer-based procedure system fails. For example, the following wording could be used:

"Measures should be taken to ensure that the operators can effectively transition from the primary computer-based procedures to backup procedures when necessary. For example:

- The presentations used on the two different media should be compatible, such that the operator can use either one effectively
 - A means should be provided to ensure that the content is consistent between the primary computer-based procedures and backup procedures
14. Bibliography Item 5: Purpose of this reference is no longer clear. Consider whether the “Java™ Look and Feel Design Guidelines” are still necessary in the ISG and appropriate to serve as SRP guidance.

Minimum Inventory

1. In items 1.a.iii and 1.b.ii of the Staff Position, delete “normal”. Minimum Inventory is only applicable to the “preferred safety” means.
2. Item 2.a indicates a description of the process that “will be used” to identify the minimum inventory should be provided as part of Tier 1 information in the DCD. Item 2.b indicates that a description of the process that “will be used” to verify the completeness of the minimum inventory should also be provided as part of Tier 1. Item 3 indicates that the minimum inventory of HSIs that “was developed” using the described process should be included in Tier 2* information in the DCD. Please clarify the Staff’s intent with respect to when the process of defining the detailed minimum inventory list is to be performed, and when the minimum inventory list is to be verified. In particular, Industry recommends this be a two-step process, developing an initial list at the DCD stage and later verifying it once the design is completed (e.g., as in Figure 3-4 of the Aug. 18 materials the industry provided to the Staff on the process for new plants)? Industry recommends the initial list be developed based on design data available at the time of the DCD. This would include an assessment of EOPs from previous plants based on the system descriptions, PRA, safety analysis and safe shutdown instrumentation documented in the DCD. EOPs for the subject plant should be used for ITAAC closure to verify the initial list.
3. Items 4 (verification of completeness) and 5 (checking as-built configuration) should be identified as ITAAC items.
4. Item 1.a.vi indicates that minimum inventory includes what’s needed to “implement the plant’s emergency operating procedures” – this seems to be a very broad statement – does the staff agree that only the specific functions/tasks identified in Table 4-1 of the industry white paper need to be supported by minimum inventory (and not the full set of EOPs)? This is limited to the preferred safety success paths.
5. The process description called for in 2.a is to include discussion of the technical requirements (qualification, independence, accessibility) applicable to the minimum inventory – however, are we correct in our understanding that minimum inventory is defined regardless of what accessibility requirements apply? In previous discussions, the staff indicated that decisions on accessibility requirements (e.g., spatial dedication) are secondary considerations, separate from the identification of what’s minimum inventory.
6. Item 2.a calls for discussion of **non-safety** as well as safety success paths in the EOPs (in 2.a.vi) – does the staff agree that only HSIs needed for preferred safety success paths are part of the minimum inventory?
7. Item 2.a.vii asks for discussion of D3 coping with respect to the minimum inventory – clarification is needed here, since the current definition of minimum inventory does not appear to include HSIs needed for D3 coping unless the non-safety HSI is adversely affected by the same CCF assumed for the RPS/ESFAS.
8. Item 2.a.viii asks for discussion of accessibility (e.g., spatial dedication) with respect to minimum inventory – yet as noted above, our understanding is that this is a separate design decision not part of identifying minimum inventory – clarification is needed here.
9. Is it the staff’s intent to make the ISG minimum inventory provisions consistent with the new definition and the upcoming revision of the SRP?
10. 1a states “always needs available”. Clarify what this means. Industry believes it means safety related (ie. qualified and meets the single failure criteria). If so, then:

- Delete item v. “analyze failure conditions of the normal human system interfaces, while maintaining the current plant operating condition and power level until the human system interfaces are restored in accordance with applicable regulatory requirements”, since only safe shutdown HSI is required to be safety related, not continued stable operation
 - Change item vi. to “implement the preferred manual safety success paths in the plant's emergency operating procedures”, since normal success paths and alternate safety success paths are not required to have safety related HSI.
 - Delete “carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment”, since risk important actions do not require safety related HSI unless those actions are credited in the safety analysis or credited for safe shutdown.
11. 1b states “always needs available”. Does this mean safety grade. Industry believes non-safety HSI is sufficient for the RSP.
 12. Item 1.a and 1.b: Consider deleting unnecessary/unclear use of “always”.
 13. Item 1.a.vii: “Bring the plant to a safe *shutdown* condition.”
 14. Item 1.b.ii: “Bring the plant to a safe *shutdown* condition.”

Manual Operator Actions

1. Title of Section 3 is *Crediting Manual Operator Actions for Diverse Actuation of Safety Systems*. Industry believes that a title such as *Crediting Manual Operator Actions for Coping with Software Common Cause Failures* would be more appropriate since BTP 7-19 allows crediting non-safety systems also.
2. Staff Position, page 14 of 24, 1st paragraph: Industry recommends that Staff consider reworking this paragraph to include crediting Manual Operator Actions outside of the Control Room @ T>30 minutes.
3. Staff Position, page 14 of 24, 2nd paragraph: Industry recommends that “performance monitoring” be changed to “human performance monitoring”. (Note: Industry also recommends that the title of Phase 4 also be changed to “Human Performance Monitoring – ...”)
4. Staff Position, page 14 of 24, 3rd paragraph: Industry requests that Staff add discussion of docketing/implementation requirements for manual operator actions relative to Tier 1/Tier 2.
5. Phase 1: Analysis, 1.A. Method, page 14 of 24, 1st paragraph: An I&C timing analysis is not needed to determine the acceptability of manual operator actions, since these actions are measured in minutes and digital I&C timing is typically less than a few seconds. Industry believes that time available is determined by plant response analysis, including thermal hydraulic analysis, RCS and containment integrity analysis, and offsite radiation release analysis.
6. Phase 1: Analysis, 1.A. Method, page 15 of 24, 1st paragraph: Industry recommends that Staff add discussion of diagnostic interval. DI&C-ISG-02 provides guidance for a 30 minute diagnostic interval. Industry believes that an acceptable method to reduce the diagnostic interval should be provided by DI&C-ISG-05, as explained in the industry white paper (eg. unique prompting alarms).
7. Phase 1: Analysis, 1.A. Method, page 15 of 24, 2nd paragraph (bulleted items); Industry requests that Staff clarify that only one method of analysis is required and that multiple analyses are not required (Note: Chapter 15 events do not require multiple analyses)
8. Phase 1: Analysis, 1.A. Method, page 15 of 24, 4th paragraph: Industry requests that “measured time(s)” be changes to “analyzed times”, since the only time developed at this stage of the process is by analysis, not test.
9. Phase 1: Analysis, 1.A. Method, page 15 of 24, 4th paragraph: Industry believes that including a margin for *any* single credible operator error, including error detection and recovery will yield excessive margin for simple actions and insufficient margin for complex actions.). More generally, imposing margin on an unspecified method is premature, since the selected method may already embody conservatism. ANSI/ANS 58.8, for example, embodies conservative assumptions to produce high confidence estimates.
10. Phase 1: Analysis, 1.A. Method, page 15 of 24, 1st paragraph: It is not correct that, “time intervals described in ANSI/ANS 58.8 were *developed* using analog controls and, therefore, may not be appropriate.” Rather, the time intervals were *validated* using analog controls. The role of validation versus analysis is similar with digital controls, and for any of the analytic methods proposed. Thus, it is unclear why the objective methodology of the Standard, with a pedigree of successful industry use, should be excluded from the list of

acceptable analysis methods. Industry requests that ANSI/ANS 58.8 be added to the list of acceptable methods.

11. Phase 1: Analysis, 1.B. Review Criteria, page 16 of 24, 3rd bullet: Industry requests information as to why this criterion is included (see comment 14). Industry recommends I&C timing analysis be deleted as discussed above.
12. Phase 1: Analysis, 1.B. Review Criteria, page 16 of 24, 5th bullet: Industry recommends that Staff consider reworking this paragraph to include use of local controls if T>30 minutes (see also comment 11).
13. Phase 1: Analysis, 1.B. Review Criteria, page 16 of 24, 6th bullet: Industry notes that this bullet seems to provide for reducing the diagnostic interval through the use of a unique prompting alarm. Industry concurs. The Staff should clarify this point.
14. Phase 1: Analysis, 1.B. Review Criteria, page 16 of 24, 7th bullet: Industry believes that demonstrating sufficient TIME AVAILABLE for a symptom/function based recovery as a mandatory back-up to an optimal recovery will require unnecessary multiple analyses and recovery methods. The symptom/function based recovery analysis in addition to the optimal recovery analysis is considered too conservative for this BTP 7-19 event. Industry recommends this requirement be limited to demonstrating the HSI inventory is sufficient for symptom based recovery (ie. there should be no timing analysis). This would be consistent with BTP-19 Position 4.
15. Phase 1: Analysis, 1.B. Review Criteria, page 16 of 24, 8th and 10th bullets: Industry notes that crew size for analysis may be beyond minimum technical specification requirements if justification is provided within the analysis. Industry believes that this is a reasonable approach.
16. Phase 1: Analysis, 1.B. Review Criteria, page 17 of 24, 1st bullet: Industry notes that recovery from a single error is not considered in Ch.15 analysis, and that other bases for conservatism might be more realistic (e.g., time distributions). In addition, Industry reasons that recovery from a single error in a large sequence of operator actions will result in very little margin being added to an analysis. Conversely, recovery from a single error in a small sequence of operator actions will result in a large margin being added to the analysis. Margin, or other conservatism, should be proportional to the sequence of actions required.
17. Phase 2: Preliminary Validation, page 17 of 24: Industry requests that the Staff consider titling Phase 2 as Verification. Industry believes that validation implies testing and testing is not required in Phase 2.
18. Phase 2: Preliminary Validation, 2.A. Method, page 17 of 24: Industry believes that use of several diverse methods for verification are unnecessary for this BTP 7-19 “beyond design basis” event and requests that only “a method”, not diverse methods, be invoked (see also 1st bullet of page 19 of 24, citing diverse methods). In the present process, diversity exists between the stages of analysis, verification, and validation. Further diversity offers not added value, but diminishing returns, and is entirely out of proportion to the associated plant risk. In comparison, Industry notes that diverse methods for verification are not required for Chapter 15 safety analysis.
19. Phase 2: Preliminary Validation, 2.A. Method, page 17 of 24, 3rd paragraph: Since time response is an objective result, Industry believes the independence requirements are excessive. It would be sufficient to exclude individuals who performed the analysis from

serving as Validation test subjects. Consider adding “as test subjects” to the end of the first sentence.

20. Phase 3: Integrated System Validation, 3.B. Review Criteria, Performance Times, page 21 of 24, 2nd bullet under Performance Times: Industry believes that this implies validation of the analysis instead of validation of the HSI system and requests that this bullet be deleted. Industry believes that validation is only required to conclude that the operators perform the required actions within the Time Available, with reasonable margin as discussed below.
21. Phase 3: Integrated System Validation, 3.B. Review Criteria, Performance Times, page 21 of 24, 3rd bullet under Performance Times: Industry believes that the intent of this statement is conservative, but acceptable. However, for clarity reword as follows: the performance time of each crew, plus the margin determined in the time required analysis, is less than the analyzed time available.
22. Phase 3: Integrated System Validation, 3.B. Review Criteria, Performance Times, page 21 of 24, 4th bullet under Performance Times: Industry believes that digital system timing analysis is not needed, as discussed above. Industry requests that this criterion be deleted.
23. Phase 3: Integrated System Validation, 3.B. Review Criteria, Performance Times, page 21 of 24, 1st bullet under Performance Times: Industry believes that performance times (i.e., validation results) confirm, not “the integrity of the analytical process”, but rather, “that necessary operator actions can be reasonably performed within the time available.”
24. Phase 3: Integrated System Validation, 3.B. Review Criteria, Performance Times, page 21 of 24, 2nd bullet under Performance Times: The performance time of each crew cannot be expected to be less than or equal to the estimated time required, unless the estimate is excessively conservative. Industry proposes that, “the average performance time of all crews” be less than or equal to the estimated time required.
25. Phase 4: Page 21 and 22, what is the purpose of the qualifier “long-term” attached to the performance monitoring of operator abilities? Recommend removal.
26. Page 22 second paragraph delete “for the credited sequence of operator actions”. The credited sequence of operator actions is used only during the analysis phase.
27. Phase 4: Page 22, first paragraph last sentence is out of place. Design engineering training need not require classroom or simulator.
28. Phase 4: Page 22, replace “documented sequence of operator actions” with “EOPs”. The documented sequence of operator actions is used only during the analysis phase (ie. to determine the time required).
29. Phase 4: Performance Monitoring, 4.B., Review Criteria, 2nd bullet: Industry suggests restating as, “The program is structured such that corrective actions will be accomplished in a formal, effective, and timely manner.”
30. Responsibilities, page 23 of 24: Industry notes that the responsibilities statement is exceptional for an ISG and requests information as to the basis for I&C Branch leadership [Are we sure of this Branch name; I am not.]. Industry believes organizations with lead responsibility for the review of accident analysis have the technical skills needed to review the most significant portion of this analysis, which is the required operator actions and the time available for those actions.