U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-05

Task Working Group #5:
Highly-Integrated Control Rooms—Human Factors Issues
(HICR—HF)

Interim Staff Guidance

Revision1

November 3, 2008

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-05

Task Working Group #5:
Highly-Integrated Control Rooms—Human Factors Issues (HICR—HF)

Interim Staff Guidance
Revision1

OFFICE	DI&C/TWG5	DI&C/DD	OGC/NLO	NRO/DE	NSIR/DSP	RES/DFERR	NMSS/FCSS
NAME	MJunge*	SBailey	MSpencer	MMayfield	SMorris	MCase*	MBailey*
DATE	10/09/08	10/31/08	10/30/08	10/28/08	10/30/08	10/29 /08	10/28/08
OFFICE	NRR/ADES						
NAME	JGrobe						
DATE	11/2/08						

***CONCURRENCE VIA E-MAIL**

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-05

Task Working Group #5:
Highly-Integrated Control Room—Human Factors Issues (HICR—HF)

Interim Staff Guidance

Revision1

SUMMARY OF CHANGES

Revision 1 adds guidance on the process of crediting manual operator actions in a Diversity and Defense - in- depth (D3) analysis (see Section 3). Sections 1 and 2 of this ISG have not changed from the original revision

IMPLEMENTATION

Except in those cases in which a licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the NRC staff will use the methods described in this Interim Staff Guidance (ISG) to evaluate licensee compliance with NRC requirements as presented in submittals in connection with applications for standard plant design certifications and combined licenses.

This ISG provides acceptable methods for addressing HICR—HF in digital I&C system designs. This guidance is consistent with current Commission policy on digital I&C systems and is not intended to be a substitute for NRC regulations, but to clarify how a licensee or applicant may satisfy those regulations.

This ISG also clarifies the criteria the staff would use to evaluate whether an applicant/licensee digital system design is consistent with HICR—HF guidelines.

1. COMPUTER-BASED PROCEDURES

SCOPE

The purpose of this interim staff guidance is to provide additional review guidance for computer-based procedure systems and computer-based procedures for use by NRC Staff. This guidance is intended to complement existing guidance for procedure review that can be found in NUREG-0700 and NUREG-0899 (see Ref 1 and 2). This additional guidance should minimize any inconsistencies in the staff review of design-specific or plant-specific computer-based procedure systems and computer-based procedures.

This guidance may be generalized to any procedure type that is presented on a video display unit, including, but not limited to, emergency operating procedures and any procedure needed for accident mitigation, safe shutdown, emergency response, severe accident management, and the performance of other critical manual actions identified in the plant PRA.

STAFF POSITION

Applicants and licensees that plan to implement a computer-based procedure system should provide a description of the computer-based procedure system with the purpose of ensuring the review criteria below for computer-based procedure systems and computer-based procedures are met. The description should include:

1. Interaction between the operator and the computer-based procedure;
2. Interaction between the computer-based procedure system and the control and process systems;
3. The use of plant data, if any, in the computer-based procedure system;
4. The use of automation, if any, in the computer-based procedure system;
5. The use of operating controls, if any, in the computer-based procedure system;
6. Presentation of procedures on the computer-based procedure system, and
7. Implementation of a backup system to the computer-based procedure system.

Computer-Based Procedures Systems

General Review Criteria:

1. A computer-based procedure system that displays operating procedures should be designed as an integral part of the Main Control Room.

2. The procedure user (e.g., operators) should always be in control of the procedure system. That is, the system should accomplish a procedure step, including automated steps, only at the direction of the user. The computer-based procedure system should be designed to provide the user with sufficient information to know they are in control.

   The basis for ensuring the user is in control of a procedure system is rooted in the availability and suitability of information displays, controls and system processes. Human factors processes presented in NUREG-0711 (see Ref 3) can be used to define the information, control and process specifications.

Concepts such as system response time, system feedback, information representation, information format, information quality (validity), range of control options, as well as meeting user expectations and providing current information are all important in ensuring that the operator is in control. These and other guidelines can be found in NUREG-0700, especially Chapter 2, "User-interface Interaction and Management."

3. The computer-based procedure system should always present the most recently approved and issued version of a procedure.

4. Measures should be taken to ensure that the computer-based procedure system will display the selected procedure. Measures should be taken to inform the operator, if the selected procedure is not or cannot be displayed.

5. The design of a computer-based procedure system should allow the operator to easily transition from one procedure to another procedure, at any time.

Plant Data Review Criteria:

The display of plant data may or may not be incorporated into the design of a computer-based procedure system.

6. Computer-based procedure systems that call for the user to enter data should provide a method for data entry.

7. Measures should be taken to ensure that plant data that is displayed in a computer-based procedure system is correct. The operator should be informed when the plant data presented has not been or cannot be validated or is invalid.

Automation Review Criteria:

The use of automation may or may not be incorporated into the design of a computer-based procedure system.

8. Automation of procedure steps should be predictable. The automation should be initiated by the operator. The operator should be able to easily interrupt the automated sequence and step, one-by-one, through each procedure step.

9. Automation should not select the procedure to be used. The user should be responsible for selecting the procedure. However, a computer-based system can recommend (e.g., via prompts) a procedure.

10. The computer-based procedure system should not initiate the execution of a procedure. The operator should direct the execution of the procedure, including its initiation.

11. The computer-based procedure system should not automatically initiate control actions without first receiving a command from the operator to do so. The

computer-based system can prompt the operator to take a specific manual action if an automatic control function fails.

12. Hold points should be established to allow operators to effectively monitor automation progress, maintain adequate situation awareness, and evaluate decisions at critical points in the procedure. Examples of hold points include:

    - A Caution or Warning is present at the procedure step ready to be executed.
    - Procedure steps that call for the operator to make a decision.
    - Any procedure step that calls for operator input.
    - Upcoming decisions or actions could involve a risk to plant safety, personnel safety or investment protection, and operator involvement in deciding whether to move forward would be expected to significantly reduce the risk.
    - When a manual operator action or verification is needed, e.g., where the computer-based procedure does not have access to the needed information or significant judgment or cross-checking is called for to make an informed decision.
    - When the next step needs a peer check.
    - When actions taken at the next step could impact compliance with plant Technical Specifications.

13. If emergency operating procedures or any procedure needed for accident mitigation, safe shutdown, emergency response, severe accident management, or the performance of other critical manual actions identified in the plant PRA are designed to include automation, the following guidance is appropriate. The computer-based procedure should:

    - Inform the operator when presenting concurrent steps, such as steps in two different legs of a flowchart emergency operating procedure.
    - Inform the user of "Result Not Obtained" and present contingency actions.
    - Monitor procedure entry conditions, cautions, warnings, branches, and exits.
    - Be integrated with alarms, system status, and critical safety functions.
    - Identify continuously applicable steps to the operator.
    - Address concurrent use of multiple procedures.

Soft Control Review Criteria:

The use of soft controls may or may not be incorporated into the design of a computer-based procedure system.

14. Soft controls are interface elements that users can manipulate to perform an action, select an option, or set a value.

15. A computer-based procedure system should contain a concise set of soft controls whose meaning should be obvious to the user. Soft controls have a single, unambiguous control function. A control function can be defined as comprising one or many control actions.

16. Soft controls should provide needed feedback to the user regarding the state of the control.

17. The control of plant equipment by an operator should take at least two discrete actions.

18. Soft control display properties should not violate stereotypes of hard or soft controls already in place in a Main Control Room.

19. A computer-based procedure system should provide a simple method to allow the operator to recover from an error of commission.

Modernization Review Criteria:

20. When implementing a computer-based procedure system into a Main Control Room via a modernization project, the human system interface conventions should include plant-specific standards that are in place at the site where the computer-based procedure system will be implemented. Failure to understand local conventions can result in conflicting sets of mental models and lead to an operational error.

Computer-Based Procedures

General Review Criteria:

21. Computer-based procedures should be written and formatted to be readable and usable on the display device of choice. If the procedure is presented on more than one "page" then continuous up/down scrolling should be implemented. The computer-based procedure system should avoid left/right scrolling. If left/right scrolling is unavoidable, the presence of information to the left or right of the viewable window should be obvious to the user.

22. The computer-based procedure system should not change the approved procedure.

23. Computer-based procedures should provide the user with a minimum set of information to allow the user to know the state of the procedure system and the plant as appropriate to the procedure. As an example, the minimum set of information should include a procedure title that is continually displayed on the screen.

24. The computer-based procedure should provide a means to access relevant meta-data (e.g., author, plant name, Unit, procedure type, etc.). However, the meta-data does not need to be presented to the operator.

Backup Procedures Review Criteria:

25. Back-up procedures should be maintained to ensure the ability to perform all emergency operating procedures and any procedure needed for accident mitigation, safe shutdown, emergency response, severe accident management, or the performance of other critical manual actions identified in the plant PRA. The backup procedures can be either paper-based or a safety-related,computer-based procedure system.

26. Backup procedures should be available to those who need them in a manner and location that is timely for their use.

27. Backup procedure systems should be subject to the same procedural controls as the primary computer-based procedure system.

28. A means should be provided to ensure that operators can quickly, easily and effectively transition to backup procedures when necessary.

29. Procedures presented on different media should be compatible, such that the operator can use them equally effectively.

30. The content of the backup procedure should be the same as the content of the primary procedure.

RATIONALE

The staff review of an applicant's or licensee's computer-based procedure system will be multi-disciplinary, and will consist of inputs from human factors engineering, instrumentation and controls, and electrical engineering.

In the past, procedures were typically written documents (including both text and graphic formats) that presented a series of decision and action steps to be performed by plant personnel (e.g., operators and technicians) to accomplish goals safely and efficiently. Procedures are used for a wide variety of tasks from administration to testing and plant operation. Computer-based procedure systems are being developed as an alternate to paper-based procedures to assist personnel in performing their tasks to increase the likelihood that the goals of the tasks would be safely and efficiently achieved.

The content and development of paper-based and computer-based procedures can be essentially the same. Both should be easy to use. However, there can be significant differences in how the procedures are presented, the method for providing information to operators, and how operators interact with the procedure. The possible differences between paper-based and computer-based procedure systems, and among computer-based systems, e.g., such as those related to automation, should not limit the control or situational awareness of licensed operators, to have full knowledge of the plant.

REFERENCES

1. NRC (2002). *Human-System Interface Design Review Guidelines* (NUREG-0700, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.

2. NRC (1982). *Guidelines for the Preparation of Emergency Operating Procedure* (NUREG-0899). Washington, D.C.: U.S. Nuclear Regulatory Commission.

3. NRC (2004). *Human Factors Engineering Program Review Model* (NUREG-0711). Washington, D.C.: U.S. Nuclear Regulatory Commission.

BIBLIOGRAPHY

1. NRC (1981). Functional Criteria for Emergency Response Facilities (NUREG-0696). Washington, D.C.: U.S. Nuclear Regulatory Commission.

2. NRC (2007). Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (NUREG-0800). Washington, D.C.: U.S. Nuclear Regulatory Commission.

3. NRC (1981). Human Factors Acceptance Criteria for the Safety Parameter Display System (NUREG-0835). Washington, D.C.: U.S. Nuclear Regulatory Commission.

4. NRC (1973). Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Regulatory Guide 1.47). Washington, D.C.: U.S. Nuclear Regulatory Commission.

5. Sun Microsystems (2001). JavaTM Look and Feel Design Guidelines, Second Edition. Palo Alto, CA. Sun Microsystems, Inc.

2. MINIMUM INVENTORY

SCOPE

The purpose of this interim staff guidance is to better describe the minimum inventory of human system interfaces (i.e., alarms, controls, and displays) needed to implement the plant's emergency operating procedures, bring the plant to a safe condition, and to carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment. The improved description and associated review criteria should minimize any inconsistencies in the staff review of a design-specific minimum inventory of human system interfaces.

STAFF POSITION

1. The minimum inventory of human system interfaces should be developed for the Main Control Room and for the Remote Shutdown Facility.

    a. The Main Control Room minimum inventory includes the human system interfaces that the operator always needs available to:

        i. monitor the status of fission product barriers,
        ii. perform and confirm a reactor trip,
        iii. perform and confirm a controlled shutdown of the reactor using the normal or preferred safety means,
        iv. actuate safety related systems that have the critical safety function of protecting the fission product barriers,
        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,
        vi. implement the plant's emergency operating procedures,
        vii. bring the plant to a safe condition,
        viii. carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment.

    b. The minimum inventory at the Remote Shutdown Facility should include the human system interfaces that the operator always needs available to:

        i. perform and confirm a reactor trip, and
        ii. place and maintain the reactor in a safe condition using the normal or preferred safety means.

    c. The minimum inventory of human system interfaces in the Main Control Room and at the Remote Shutdown Facility should be readily accessible to the operator.

2. Applications should include with the Tier 1 information of the design control document:

    a. A description of the process that will be used to identify the minimum inventory in the Main Control Room and at the Remote Shutdown Facility. The description of

the identification process should include a description of:

i. the selection criteria,
ii. how the functions and tasks that need to be supported by the minimum inventory of human system interfaces will be identified,
iii. the technical requirements that apply to the design of the human system interfaces including those imposed by regulatory requirements, and particularly addressing requirements related to qualification, independence, and accessibility,
iv. how the plant-specific probabilistic risk assessment will be used to identify operator actions or tasks that are risk important,
v. how the guidance provided in Regulatory Guide 1.97, Rev. 4 will be addressed,
vi. the operator actions credited in the safety analysis or plant-specific emergency operating procedures for safety and non-safety success paths,
vii. how the diversity and defense-in-depth evaluation will be used to identify any specific operator actions credited for coping with common cause failures of digital protection systems, and
viii. the criteria that will be used to determine which human system interfaces need to be spatially dedicated, continuously visible, continuously available, or accessible by taking only one action.

b. A description of the process that will be used to verify the completeness of the minimum inventory in the Main Control Room and at the Remote Shutdown Facility. The description of the verification process should include discussion of:

i. the use of generic technical guidelines or design-specific guidelines for developing emergency operating procedures,
ii. the task analysis (or surrogate based on either an applicable predecessor plant design or an abbreviated, high-level, design-specific task analysis) that describes the operator actions necessary to bring the reactor to a safe shutdown under conditions when the primary instrumentation is available and when it is unavailable,
iii. the risk-important operator actions identified through the plant-specific probabilistic risk assessment or plant-specific human reliability analysis,
iv. the critical operator actions credited for diversity and defense-in-depth (including those for coping with common cause failures), and
v. the use of a full-scope simulator that meets the guidance in ANSI/ANS 3.5.

c. A description of the information that will be available to implement Inspections, Tests, Analysis, and Acceptance Criteria (ITAAC) and which will be used to verify that:

i. the process for developing the minimum inventory was implemented,
ii. the selection criteria for determining the minimum inventory were applied,
iii. the Main Control Room and Remote Shutdown Facility minimum inventories are complete, and
iv. the Main Control Room and Remote Shutdown Facility contain the minimum inventory.

3. Applicants seeking approval of a Main Control Room or Remote Shutdown Facility design should include with the Tier 2* information of the design control document the minimum inventory of human system interfaces that was developed using the process described in the design control document.

4. The completeness of the minimum inventory should be verified once the control room design has been implemented (e.g., construction or modification of full-scope simulator).

5. The as-built Main Control Room and Remote Shutdown Facility should be evaluated to assure that both contain the minimum inventory determined from the development process and selection criteria.

RATIONALE

The staff review of an applicant's minimum inventory will be multi-disciplinary and will consist of inputs from human factors engineering; instrumentation and controls; risk assessment; plant systems, reactor systems, and electrical engineering.

The staff identified control room design and advanced instrumentation and controls as areas where detailed design information may not be available for NRC staff review during a design certification. Therefore, the NRC staff developed a two-part approach for the review of the human factor aspects of the control room design. The first part involves a review of both the detailed process that was used to establish the minimum inventory, as well as, the actual list of human system interfaces necessary for the operators to implement the emergency operating procedures, bring the plant to a safe condition, and carry out those human actions shown to be risk important by the applicant's PRA. The second part of the staff's review uses design acceptance criteria to ensure the implementation of the systematic process to the incorporation of human factors principles in completing the design of the control room, such as designing alarms, controls, and displays.

BIBLIOGRAPHY

1. American National Standards Institute (1998). Nuclear Power Plant Simulators for Use in Operator Training and Examination (ANSI/ANS-3.5-1998). La Grange Park, IL: American National Standards Institute.

2. Institute of Electrical and Electronics Engineers (1991). IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations -Description (IEEE Std. 603-1991). New York: Institute of Electrical and Electronics Engineers.

3. NRC (2007). Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 7-Instrumentation and Controls - Overview of Review Process, BTP 7-19-Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems (NUREG-0800). Washington, D.C.: U.S. Nuclear Regulatory Commission.

4. NRC (2007). Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Chapter 18-Human Factors Engineering (NUREG-0800). Washington, D.C.: U.S. Nuclear Regulatory Commission.

5. NRC (2006). Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants (Regulatory Guide 1.97). Washington, D.C.: U.S. Nuclear Regulatory Commission.

6. NRC (2004). Human Factors Engineering Program Review Model (NUREG-0711, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.

7. NRC (2002). Human-System Interface Design Review Guidelines (NUREG-0700, Rev. 2). Washington, D.C.: U.S. Nuclear Regulatory Commission.

8. NRC (1993). Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs (SECY 93-087). Washington, D.C.: U.S. Nuclear Regulatory Commission.

9. NRC (1992). Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Process (SECY 92-053). Washington, D.C.: U.S. Nuclear Regulatory Commission.

10. NRC (1973). Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems (Regulatory Guide 1.47). Washington, D.C.: U.S. Nuclear Regulatory Commission.

11. NRC (1973). Manual Initiation of Protective Actions (Regulatory Guide 1.62). Washington, D.C.: U.S. Nuclear Regulatory Commission.

3. CREDITING MANUAL OPERATOR ACTIONS IN DIVERSITY AND DEFENSE-IN-DEPTH (D3) ANALYSES

Scope

The purpose of this Interim Staff Guidance (ISG) is to define a methodology, applicable to both existing and new reactors, for evaluating manual operator action as a diverse means of coping with Anticipated Operational Occurrences and Postulated Accidents (AOO/PA) that are concurrent with a software Common Cause Failure (CCF) of the digital Instrumentation and Control (I&C) protection system. This software CCF is discussed in the Background of Branch Technical Position (BTP) 7-19, *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer - Based Instrumentation and Control Systems*, of NUREG-0800, *Standard Review Plan*.

To provide additional guidance for BTP 7-19, the NRC staff developed Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG), DI&C-ISG-02, Diversity and Defense-in-Depth Issues, Revision 1 in September of 2007. DI&C-ISG-02 specifically discusses adequate diversity and manual operator actions as follows:

> Manual operator actions may be credited for responding to events in which the protective action subject to a CCF is not required for at least the first 30 minutes and the plant response is bounded by BTP 7-19 recommended acceptance criteria.

DI&C-ISG-02 further states the following:

> The licensee or applicant should demonstrate through a suitable human factors engineering (HFE) analysis that manual operator actions that can be performed inside the control room are acceptable in lieu of automated backup functions.

Subsequent to the issuance of DI&C-ISG-02, the staff determined that further guidance was necessary for crediting manual operator action during an AOO/PA concurrent with a software CCF. This ISG provides guidance on how to "demonstrate through a suitable human factors engineering (HFE) analysis that manual operator actions that can be performed inside the control room are acceptable in lieu of automated backup functions." In addition, this guidance can be used to demonstrate the acceptability of operator actions required in less than 30 minutes.

Staff Position

A diversity and defense-in-depth (D3) analysis should include the justification of any operator actions that are credited for response to an AOO/PA concurrent with a BTP 7-19 software CCF. Manual operator actions for these scenarios should be based upon, and ultimately included within, the Emergency Operating Procedures (EOPs) and executed from the main control room (MCR).

To credit operator actions, an acceptable method would be to demonstrate that the manual actions in response to a BTP 7-19 software CCF are both feasible and reliable, given the time available, and that the ability of operators to perform credited actions reliably will be maintained for as long as the manual actions are necessary to satisfy the D3 analysis. The time available for manual actions should be based upon the methods and criteria prescribed in BTP 7-19. The time required for operator action should be estimated and validated using the guidance of this ISG. To demonstrate that the manual actions are both feasible and reliable, and that the ability to perform the actions reliably within the time available is maintained, the vendor/licensee/applicant should follow a process of analysis, validation, and long-term monitoring consistent with this ISG.

Credited manual operator actions and their associated interfaces (controls, displays, and alarms) must be specifically addressed in the vendor/licensee/applicant's HFE Program. The vendor/licensee/applicant should commit, in the D3 submittal, to include the proposed D3 coping actions in a HFE Program consistent with that described in NUREG-0711*, Human Factors Engineering Program Review Model,* and to provide the results of the HFE Program to the staff prior to implementation of the proposed action(s).

PHASE 1: ANALYSIS

This section describes the attributes of an acceptable method of analyzing the time available and time required for manual operator actions that are to be credited in a D3 analysis.

1.A. Method

The analysis must demonstrate that:

- the time available to perform the required manual actions is greater than the time required for the operator(s) to perform the actions.
- the operator(s) can perform the actions correctly and reliably in the time available. The time available to perform the actions should be based on analysis of the plant response to the AOO/PA using realistic assumptions, and the acceptance criteria of BTP 7-19.

The time required for operator action should be based on an HFE analysis of operator response time. The HFE analysis should evaluate the documented sequence of operator actions (based on task analysis, vendor-provided Emergency Procedure Guidelines (EPGs), or plant-specific EOPs, depending on the maturity of the design) that achieves the credited operator response in the time available. The documented sequence of operator actions should be analyzed at a level of detail necessary to identify critical elements of the actions that affect time required and likelihood of successful completion of the action sequence. The vendor/licensee/applicant should establish time estimates for individual task components (including cognitive tasks such as diagnosis) and the basis for the estimates, through a method applicable to the human-system interface (HSI) characteristics of digital computer-based I&C.

Acceptable methods for deriving analysis time estimates for individual task components include, but are not limited to:

- Operator interviews and surveys
- Operating experience reviews
- Software models of human behavior, such as task network modeling
- Use of control/display mockups
- Expert panel elicitation[1]
- ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions*[2]

Prior experience with tasks or subtasks similar to the actions proposed to be credited in the D3 analysis may provide valuable insights for the analysis/estimates of operator response times. Operating experience review (OER) data used to provide input to the analysis/estimates of operator response times should be supplemented with information about the similarities and differences between the credited actions and the actions identified in the OER.

A time margin should be added to the analyzed time(s). One acceptable method is for the time margin to equal the maximum recovery time for any single credible operator error. Inclusion of such margins provides assurance that manual actions can be performed with a high level of reliability. The basis for the specific time margin used in the analysis should be justified and documented. Insights from the HFE program, especially the Human Reliability Assessment, should be used. The identification of potential errors, error detection methods, and error recovery paths in event trees may be used to provide estimates of how much margin should be added to the operator response time estimates.

1.B. Review Criteria

The responsible reviewers evaluate vendor/licensee/applicant's submittals for compliance with the following criteria:

- The analysis establishes the time available using an analysis method and acceptance criteria consistent with the guidance of BTP 7-19. The basis for the time available is documented.

- The analysis of the time required is based on a documented sequence of operator actions (based on task analysis, vendor-provided EPGs, or plant-specific EOPs, depending on the maturity of the design).

- The sequence of actions uses only alarms, controls, and displays that would be available in the MCR and operable during the assumed CCF scenario(s), as documented in the Failure Modes and Effects Analysis.

[1] For an example of an expert panel elicitation, see NUREG-1852, *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire.*

[2]ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions*, provides an acceptable task decomposition methodology for this purpose. However, the time intervals described in ANSI/ANS 58.8 were validated using analog controls and, therefore, may not be appropriate.

- The estimated time response of operators is sufficient to allow successful execution of applicable steps in the symptom/function-based EOPs.

- The initial MCR operating staff size and composition assumed for the analysis of time required is the same as the minimum MCR staff defined in the plant's Technical Specifications.

- If credited manual actions require additional operators beyond the Technical Specification minimum crew, the justification for timely availability of the additional staffing is provided and the estimate of time required includes any time needed for calling in additional personnel.

- The analysis of the action sequence is conducted at a level of detail sufficient to identify critical elements of the actions, including cognitive elements such as diagnosis and selection of appropriate response, that affect time required and the potential for operator error.

- The analysis of the action sequence identifies credible operator errors and the estimate of time required includes sufficient margin for recovery from any single credible operator error.

PHASE 2: PRELIMINARY VALIDATION

This section describes the attributes of an acceptable method for preliminarily validating the time required to take manual operator actions that are credited in a D3 analysis.

Note: Licensees upgrading existing plants should skip this phase and go directly to Phase 3, Integrated System Validation (ISV). A preliminary validation is only required for those vendors/applicants who are using the 10 CFR Part 52 process.

2.A. Method

The preliminary validation should provide independent confirmation of the validity of the "time required" estimate derived in the Phase 1 Analysis through the use of diverse methods such as the following:

- Tabletop analysis
- Walkthrough/talkthrough analysis
- Software models of human behavior, such as task network modeling
- Use of control/display mockups
- Man-in-the-loop prototype testing
- Pilot testing
- Real-time validation on a suitable[2] part-task simulator

Note: The preceding list is not all-inclusive – other validation methods may be used if sufficient technical justification is provided.

[2] A suitable part-task simulator is one of demonstrated scope and fidelity sufficient for the conduct of the specific validation.

The vendor/applicant should use several diverse methods to estimate operator response times to maximize the cross-validation value of the methods. For example, when the design has advanced to the point where a part-task simulator is available, the vendor/applicant should use it to cross-validate previous time estimates derived from other activities, such as expert elicitation, tabletop analysis, or walkthrough/talkthrough. It is expected that the vendor/applicant will estimate operator response time using as realistic an environment as is available at the time of the preliminary validation.

The group of individuals who conduct the preliminary validation of the analysis should not include individuals who conducted the analysis. Independence between these groups will help to ensure that any undocumented assumptions and analytical methods used in the analysis are identified and documented during the analysis. However, it is recognized that communication between the groups will be necessary, especially after the preliminary validation is complete. The processes of validation and design are iterative and feedback from the preliminary validation should be used to refine the design, the procedures, and the training provided to the operators.

The preliminary validation should be rigorous and conducted by operators, system technical experts, and human factors experts. These personnel should be instructed to verify that the analysis is logical for its purpose, contains a sufficient level of detail (including adequate notes), and presents no physical or spatial difficulty for performance. The language and the level of information presented in the documented sequence of manual operator actions should be compatible with the minimum number, qualifications, training, and experience of the operating staff.

Operators and system technical experts should be instructed to ensure that the documented sequence of manual operator actions, independent of the time required, is technically correct and will achieve the desired technical result(s). These personnel should be instructed to verify the correspondence between the documented sequence of manual operator actions and the existing or planned displays and controls to be used by the operator, including correspondence in labeling, units of measure, and operation of controls. Walkthrough/talkthrough of planned displays and controls for new plants should be conducted to the extent practical, according to the state of the design and supplemented as necessary by use of such aids as arrangement diagrams, vendor drawings, and panel fabrication drawings.

Results shall be documented in the D3 analysis for NRC review. Preliminary validation results should be such that there is high confidence that the time required for manual operator actions will satisfy the success criteria for the integrated system validation described below. Unacceptable preliminary validation results should result in modification of the D3 coping strategy. Modification of the D3 coping strategy will require re-analysis, re-validation and re-submittal for NRC staff review. If a successful manual action strategy cannot be achieved, diverse automation is required.

At this point, the complete D3 analysis, which provides time available and time required, and the supporting analyses, may be submitted for NRC review. When the NRC reviewers have established that there is high confidence that the manual operator actions will be accomplished correctly, reliably, and within the time available, they may provide a safety determination conditioned upon the completion of any related HFE open items, Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC), or Combined Operating License (COL) open items.

2.B. Review Criteria

The responsible reviewers evaluate vendor/applicant's submittals for compliance with the following criteria:

- The preliminary validation is conducted as an independent confirmation of the Phase 1 Analysis that compared time available and estimated time required.

- The preliminary validation is conducted by a multi-disciplinary team with the knowledge and skills necessary to verify the rigor and assumptions of the analysis and validate the analysis conclusions regarding the ability of operators to perform the actions reliably within the time available.

- The preliminary validation uses two or more methods to validate the analysis.

- The preliminary validation results support the conclusion that the time required, including margin, to perform individual steps and the overall documented sequence of manual operator actions is reasonable, realistic, repeatable, and bounded by the Phase 1 Analysis documentation.

Unacceptable preliminary validation should result in modification of the D3 coping strategy. Modification of the D3 coping strategy would require re-analysis, re-validation and re-submittal for NRC staff review. If a successful manual action strategy cannot be achieved, diverse automation is required.

PHASE 3: INTEGRATED SYSTEM VALIDATION

This section describes the attributes of an acceptable method for conducting an ISV of manual operator actions that are to be credited in a D3 analysis.

3.A. Method

ISV is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, procedures, training, staffing and qualification, and physical environment) meets performance requirements and acceptably supports safe operation of the plant. The vendor/licensee/applicant should conduct an ISV of manual actions credited in the D3 analysis using a plant-referenced simulator in real time. Using the validation guidance in NUREG-0711, the vendor/licensee/applicant should measure operator response times (performance times) of all licensed operating crews in representative event simulations, i.e., AOO/PAs with concurrent software CCF. Performance times should be compared to the time available (per D3 analysis results) and previous estimates of time required. The digital I&C system timing analysis results in support of determining the time available should be validated as necessary by testing on integrated digital I&C systems and components.

In selecting personnel for event simulations, consideration should be given to the assembly of both nominal and minimum crew configurations, including shift supervisors, reactor operators, shift technical advisors, etc., that will participate in the validation tests. The composition of operations personnel need only include personnel who are relevant to the credited actions.

Acceptable validation results will provide the basis for meeting the license application or amendment request approval requirements of the NRC staff. Unacceptable validation results should result in modification of the D3 coping strategy.

Modification of the D3 coping strategy would require reanalysis, re-validation and re-submittal for NRC staff review. If a successful manual action strategy cannot be achieved, diverse automation is required.

The ISV shall be implemented and documented as an ITAAC item or COL action item for plants licensed under 10 CFR Part 52 or as a License Condition for operating plants that have not upgraded the plant-referenced simulator in advance of the control room modifications. The complete D3 analysis, which provides time available and time required, the supporting analyses, and validation results shall be submitted for final NRC review and closure of any HFE open items, ITAAC, COL action items, or License Conditions.

3.B. Review Criteria

The responsible reviewers evaluate vendor/licensee/applicant's submittals for compliance with the following criteria:

General

- The ISV is completed as part of the HFE program that is implemented in accordance with NUREG-0711.

Simulator

- The ISV is conducted using a plant-referenced simulator that meets the functional and fidelity requirements of the adopted ANSI/ANS 3.5, Nuclear Power Plant Simulators for Use in Operator Training and Examination, and is capable of real time, high fidelity plant simulation of the BTP 7-19 software CCF concurrent with an AOO/PA.
    - The simulator accurately represents Digital I&C CCFs and digital failure modes.
    - The plant-referenced simulator used for the validation of manual operator actions demonstrates expected plant response to operator input and to normal, transient, and accident conditions to which the simulator has been designed to respond.
    - The plant-referenced simulator is designed and implemented so that it is sufficient in scope and fidelity to allow conduct of the evolutions associated with AOO/PA, including manual operator actions, as applicable to the design of the reference plant.
- The simulator accurately represents the HSI available and the postulated HSI failure(s) for the software CCF condition.

Personnel

- Participants in the validation are the plant personnel who would normally perform the credited actions.

- Actions to be performed by licensed operators are validated using individuals holding an operating license for the unit on which the actions are to be credited.

- Actions allocated to non-licensed operators are validated using non-licensed personnel trained in accordance with a program that meets the requirements of 10 CFR 50.120.

- The MCR operating staff size and composition used in the event simulations is the same as was used for the analysis and preliminary validation.

- All crews are included as part of the ISV.

Operational Conditions

- Event simulations for the ISV include a range of representative CCF and digital failure modes, postulated HSI failures, and operational conditions in which credited actions may be required.

Performance Times

- For each AOO/PA, the mean performance time~~s~~ of the crews is less than or equal to the estimated time required derived from the analysis phase.

- For each AOO/PA, the performance time for each crew, including margin determined in the time required analysis, is less than the analyzed time available.

PHASE 4: MAINTAINING LONG-TERM INTEGRITY OF CREDITED MANUAL ACTIONS IN THE D3 ANALYSIS

4.A. Method

Among other factors, changes in plant design, EOPs, and operator training can affect the ability of operators to correctly and reliably perform manual actions. Accordingly, the vendor/licensee/applicant should establish a strategy for long-term monitoring of operator ability to reliably perform the manual operator actions credited in a D3 analysis. The scope of the performance monitoring strategy should provide adequate assurance that integrated system performance will be maintained within the bounds established by the ISV and continue to support the associated D3 analysis.

There is no expectation for the vendor/licensee/applicant to periodically repeat the full ISV; however, there should be sufficient controls to provide reasonable confidence that operators will maintain the skills necessary to accomplish the credited actions. The results of the monitoring need not be reported to the NRC, but should be retained onsite for inspection.

Consistent with 10 CFR Part 50, Appendix B, Criterion III, Design Control, Criterion V, Instructions, Procedures and Drawings, and Criterion VI, Document Control, the

vendor/licensee/applicant should have in place sufficient configuration and design controls to assure that procedure steps that direct the credited action are administratively protected from inadvertent change, and that the design program has sufficient controls to assure that the design will continue to support the D3 analysis when the plant or MCR is modified.

Consistent with 10 CFR Part 50, Appendix B, Criterion II, Quality Assurance Program, in addition to the operations organization, training should also be provided to design personnel for the purpose of understanding the critical link between manual operator actions performed in response to a BTP 7-19 software CCF and the plant equipment used to implement these actions. Instructors should ensure that trainees understand the philosophy behind the approach of the EOPs.

Consistent with 10 CFR Part 50, Appendix B, Criterion III, Design Control, and Criterion XVI, Corrective Action, long-term monitoring should have a formal mechanism for feedback such that results, including problems identified by the operating staff during operations or training, are brought to the attention of the reference plant operations department management and the design organization. The vendor/licensee/applicant may integrate, or coordinate, their long-term monitoring with existing programs for monitoring operator performance, such as periodic operator surveys or the licensed operator training program.

4.B. Review Criteria

The responsible reviewers evaluate vendor/licensee/applicant's submittals for compliance with the following criteria:

- A long-term monitoring strategy is developed and documented by the vendor/licensee/applicant that is capable of tracking performance of the manual operator actions to demonstrate that performance continues to support the associated D3 analysis.

- The program is structured such that corrective actions are formal, effective, and timely.

Rationale

Guidance for HFE analyses that would be suitable to support D3 analyses is described in NUREG-0711. The staff has a high degree of confidence that a vendor/licensee/applicant using the NUREG-0711 model will provide adequate HSI design to allow operators to accomplish the manual actions required by their designs. However, the typical HFE Program per NUREG-0711 does not conclude until just before fuel load or startup. This ISG provides guidance for a methodology that provides early feedback in the design and regulatory review process and allows the vendor/licensee/applicant to move forward with relative confidence that credited manual operator actions will be demonstrated as both feasible and reliable in the ISV. Ultimately, NRC approval of manual operator actions under this ISG will be based on successful completion of associated HFE open items, COL action items, ITAAC, or License Conditions related to the actions credited in the D3 analyses.

REFERENCES

American National Standards Institute (1994). *Time Response Design Criteria for Safety-Related Operator Actions* (ANSI/ANS 58.8-1994). La Grange Park, IL: American National Standards Institute.

NRC (2007), *Interim Staff Guidance on Diversity and Defense-in-Depth Issues*, (DI&C-ISG-02), September 26, 2007. Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (2007), *Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,"* (NUREG-0800) March 2007. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2007). *Standard Review Plan*, *Chapter 18 - Human Factors Engineering (*NUREG-0800) March 2007. Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (2004). *Human Factors Engineering Program Review Model* (NUREG-0711, Rev. 2). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (2007). *Standard Review Plan*: *Chapter 13, Conduct of Operations* (NUREG-0800) March 2007. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2007). *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to fire*, (NUREG-1852) October 2007. Washington, DC: U.S. Nuclear Regulatory Commission.

U.S. Code of Federal Regulations (revised periodically), Part 50, *"Domestic Licensing of Production and Utilization Facilities,"* Title 10, "Energy," Washington, DC : U.S. Government Printing Office

U.S. Code of Federal Regulations (revised periodically), Part 52, "*Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants,"* Title 10, "Energy," Washington, DC: U.S. Government Printing Office.

BIBLIOGRAPHY

American National Standards Institute (1998). *Nuclear Power Plant Simulators for Use in Operator Training and Examination* (ANSI/ANS-3.5-1998). La Grange Park, IL: American National Standards Institute.

EPRI/MPR (2008), *A Methodology to Determine the Acceptability of Manual Operator Action Response Times for a BTP 7-19 Software Common Cause Failure,* (EPRI 1015312, Rev. E), July 2008. Alexandria, Va., MPR Associates, Inc.

IEEE *Guide for the Evaluation of Human-System Performance in Nuclear Power Generating Stations*, (IEEE Std 845-1999), IEEE Power Engineering Society, June 1999.

Ness, James W., Tepe, Victoria, Ritzer, Darren, eds., *The Science and Simulation of Human Performance,*" The Science of Human Performance: Methods and Metrics"*,* P.157-173, Emerald Group Publishing, 2004.

NRC (2007), *Guidance for the Review of Changes to Human Actions,* (NUREG-1764, Rev. 1). September 2007. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2005*), Good Practices for Implementing Human Reliability Analysis,* (NUREG-1792) April 2005. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (2000), *A Study of Control Room Staffing Levels for Advanced Reactors* (NUREG/IA-0137), November, 2000, Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (2007). *Standard Review Plan*: *Chapter 13, Conduct of Operations* (NUREG-0800) March 2007. Washington, D.C.: U.S. Nuclear Regulatory Commission.

NRC (1997). *Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times* (Information Notice 97-78). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (1980). *Clarification of TMI Action Plan Requirements* (NUREG-0737 and supplements). Washington, DC: U.S. Nuclear Regulatory Commission.

O'Hara, J., Stubler, W., Brown, W. and Higgins, J. (1997). *Integrated System Validation: Methodology and Review Criteria* (NUREG/CR-6393). Washington, DC: U.S. Nuclear Regulatory Commission.