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

Revision 0
(Initial Issue for Use)

September 28, 2007 ML072540140

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-05

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

Interim Staff Guidance

Revision 0
(Initial Issue for Use)

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. The staff intends to continue interacting with stakeholders to refine digital I&C ISGs and to update associate guidance and generate new guidance where appropriate.

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.