# APPLYING HUMAN FACTORS DURING THE SIS LIFE CYCLE

**Dr. Beth Vail*, LeRoy Goff*, Laura Sheets, Linda Olsen and Russell Harwood**
**URS Corporation***
**2131 S. Centennial Ave., Aiken, SC 29803**
**803.502.9701/ (fax) 803.502.2701**
**beth.vail@wsms.com**

## Introduction

Safety Instrumented Systems (SIS) are widely used in U.S. Department of Energy's (DOE) nonreactor nuclear facilities for safety-critical applications. Although use of the SIS technology and computer-based digital controls, can improve performance and safety, it potentially introduces additional complexities, such as failure modes that are not readily detectable. Either automated actions or manual (operator) actions may be required to complete the safety instrumented function to place the process in a safe state or mitigate a hazard in response to an alarm or indication.

DOE will issue a new standard, *Application of Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*[1], to provide guidance for the design, procurement, installation, testing, maintenance, operation, and quality assurance of SIS used in safety significant functions at DOE nonreactor nuclear facilities. The DOE standard focuses on utilizing the process industry consensus standard, American National Standards Institute/ International Society of Automation (ANSI/ISA) 84.00.01, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*[2], to support reliable SIS design throughout the DOE complex.

SIS design must take into account human-machine interfaces and their limitations and follow good human factors engineering (HFE) practices. HFE encompasses many diverse areas (e.g., information display, user-system interaction, alarm management, operator response, control room design, and system maintainability), which affect all aspects of system development and modification. This paper presents how the HFE processes and principles apply throughout the SIS life cycle to support the design and use of SIS at DOE nonreactor nuclear facilities.

## The Operator within the SIS

For many safety applications throughout DOE facilities, manual operator action(s) are needed to provide a level of risk reduction. The operator action may or may not be in combination with other layers of protection (level of control). An operator action cannot occur in isolation; it is typically combined with systems, structures or components or programmatic administrative controls. To prevent to mitigate an unwanted safety condition, the operator must be provided with the necessary process information and properly designed controls to perform the requisite

safety action. Typically the operator will receive an alarm or monitor an indication to determine that a safety limit has been reached or exceeded.

To determine the reliability of the operator's response, several factors must be evaluated. These include the time window available to perform an action, the actual or demonstrated operator response time, operator training, and the compliance of the instrumentation/interface provided to the operator with HFE principles. These factors should be evaluated to provide the justification for the amount of risk reduction (the probability of failure on demand) that can be provided by the operator response when it is part of the safety instrumented function (SIF).

The operator response may be embedded within one of several different layers of protection - the basic process control system or the SIS. In either case, the operator responds to an alarm condition or a monitored parameter and initiates a response from the control room or directs a manual response in the facility, or out in the field, to place a component in a safe state (e.g., close a manual valve or reposition a breaker). Any SIS that requires an operator action to perform the safety function must rely on support systems (e.g., electrical power to actuate an alarm horn). When evaluating the operator action within a SIS, it is important to identify, model, and quantify, both human error and support system reliability (i.e., power provided to the alarm or indicator).

## Life Cycle Activities

The DOE Standard[1] provides information pertinent to utilizing good HFE practices. The draft standard includes a figure representing the "Application of HFE throughout the SIS Life Cycle" and table that details "Human Factors Standards and Guidance Documents" as applied to each HFE life cycle phase. The figure and table (see Appendix) are duplicated in this paper to assist the reader. A discussion of the underlying HFE principles related to both will make up the remainder of this paper.

As it relates to the SIS Life Cycle, the following HFE activities are necessary to ensure an adequately designed user-system interface for the human operator:

- Planning,
- HFE Analysis,
- HFE Requirements, Guidelines, and Conventions,
- Implementation,
- Preliminary Testing,
- Facility Installation and Validation,
- Operations and Continuous Improvement.

During the time associated with HFE Analysis activities, specific HFE documentation such as requirements, guidelines, and conventions are to be developed which serves as a basis to ensure a cohesive operator interface that follows good HFE design practices. Appendix Table 1, "Human Factors Standards and Guidance Documents", references NUREG-0700, *Human-System Interface Design Review Guidelines*[3], which provides a comprehensive review for HFE

.

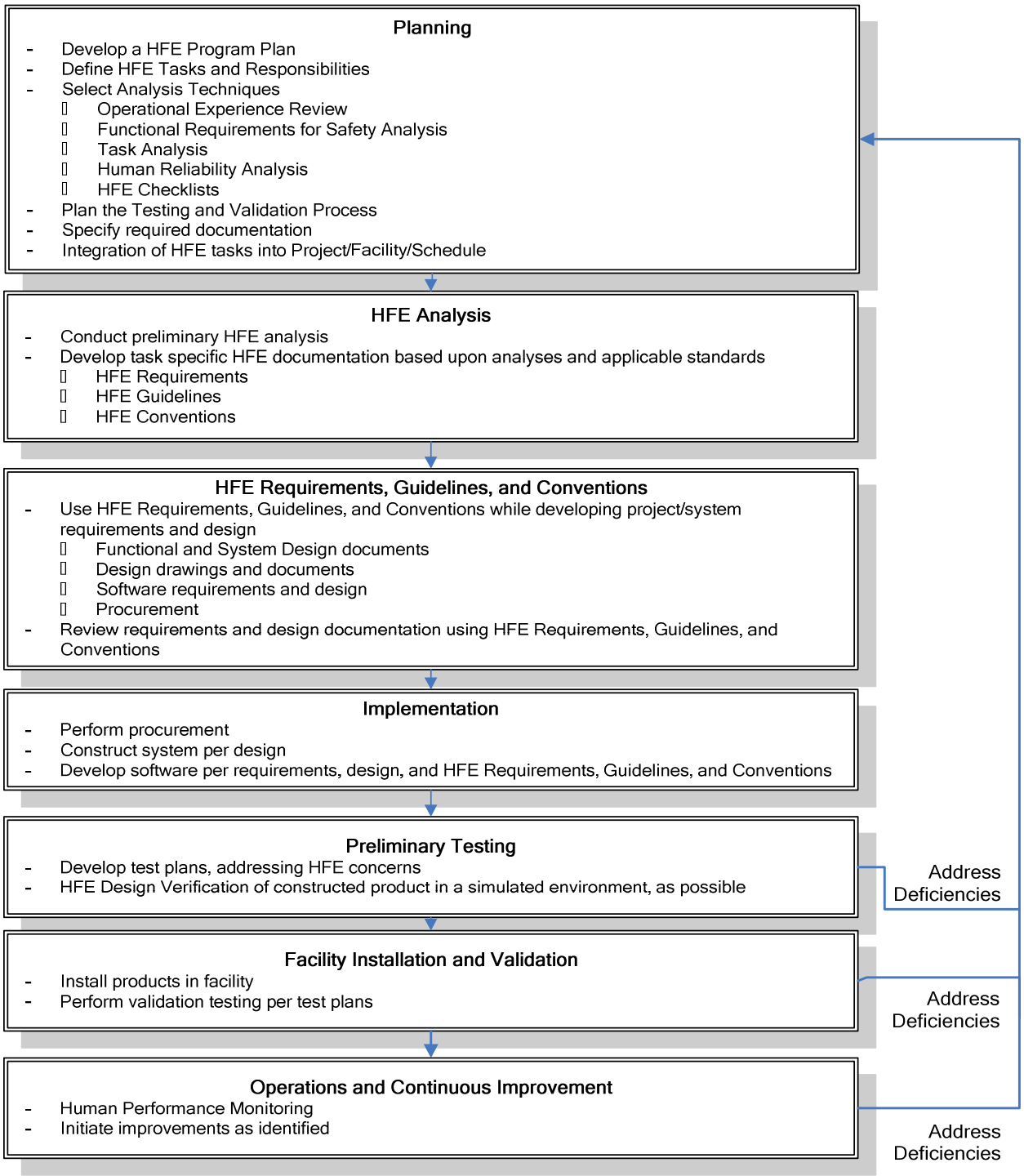


**Figure 1: Application of HFE throughout the SIS Life Cycle.**

.

principles and design guidelines. The guidance includes, but is not limited to, information in the following areas related to the human-machine interface (HMI):

- Information Display
- User-System Interaction
- Alarm Guidelines
- Workplace Design
- Local Control Stations

NUREG-0700[3] gives numerous detailed guidelines, which include descriptions and additional information. Summaries/highlights of these areas, with a focus on practical experience, follow.

**Control Room/Remote Control Panel Design**

Control room design and remote control panel design are important considerations in the SIS life cycle since safety functional requirements must address human-machine interface requirements and potential reliance on operator actions to accomplish the safety instrumented function via manual system shutdown. NUREG-0711, Rev. 2, *Human Factors Engineering Program Review Model* [1] provides a structured, life cycle analysis approach for the development, design and evaluation of a facility using accepted HFE principles.

As a part of the HFE review, evaluation, and acceptance of human-machine interface designs/modifications, NUREG-0711[4] directs the analyst to NUREG-0700[3], for specific user-system interface design guidelines that can be used as acceptance criteria to ensure that the new design or modification accommodates human capabilities and limitations. Operator interfaces that communicate information between the operator and the SIS and the display of critical SIS status information necessary to maintain the SIL, should be developed and maintained utilizing human factors engineering design guidance provided in NUREG-0700[3]. Specific sections of NUREG-0700 for SIS design consideration include: Section 1, Information Display; Section 4, Alarm System; Section 5, Safety Function and Parameter Monitoring System; and Section 7, Soft Control System.

SIS design also requires that upon failure of the SIS operator interface, an alternate means is provided for the operator to bring the process or system to a safe state, ensuring that the automatic functions of the SIS are not compromised. Satisfying this requirement potentially brings manual operator actions “in the field” (i.e., at control locations outside the main process or system control room) into play. Therefore considerations of the human-machine interface design should be included for any remote control panels (e.g., valve and pump controllers), as well as the design of communication interfaces between plant personnel (e.g., main/remote control room and field control locations). NUREG-0700[3] Sections 10 and 12 provide specific design guidance for communication systems and workplace design of local control stations, respectively.

**Information Display Design**

The display of information to the operator is critical to the operator's ability to understand how a process works, the current status of the process, and the appropriate and timely response to abnormal conditions. Training cannot overcome a poorly designed interface, and this concept is

.

especially true when an operator is placed in a stressful condition. As an example, if all but one switch on an interface have the convention of "on is up" and "off is down", an operator trying to determine the cause of an alarm condition may forget (momentarily, but long enough to cause a problem/confusion) this one difference, even after being trained thoroughly on the difference.

Highlights of Information Display design principles are as follows.

- Consistent Interface Conventions - Consistent and meaningful interface design conventions should be evident for all display features (such as labels, abbreviations, symbol orientation, and color usage)
- Grouping of Information - Functional zones and equipment groupings shall be visually distinct.
- Techniques for Displaying Information Important to Facility Operation - Information presented should be the simplest information and all that is necessary to perform tasks needed to operate the facility and highlight abnormal conditions.
- Appropriate Setpoints/Alarm Limits - Setpoints (alarm limits) used to indicate a change in status should be chosen to provide users with sufficient time to respond appropriately.

**User-System Interaction**

The use of the user-system interface should be as intuitive as possible. The interface should guide the operator through the successful operation of the facility during normal and off-normal conditions, prevent multiple users from interfering with each other (including interference between computer automation and the human operator), and generally make an operator's job easier.

- Simple Input Actions - Input formats should be as simple as possible with guidance information and an organization that facilitates proper data input, including selection of pre-defined options, when possible. An information entry sequence should be designed so that its organization reflects the user's view of the task, and provides all control options that may be required.
- Facilitate Operating “Intended” Equipment - Selected items should be highlighted. Confirmation of action commanded by an operator (to be taken by a computer based system) is required prior to implementing it. In cases where a component is being manipulated, the specific component and action should be identified rather than using generic terms ("Confirm action to Open FCV-100" preferred over "Confirm action").
- Provision for Alternative Actions -Transactions should never leave the user without further available action and should provide subsequent steps or alternatives. If an automated sequence states, "Confirm valve FCV-100 is open.", and the valve is not open, the operator should be given guidance or a choice of the next available actions.
- Prevention of Conflicting Control Commands -When several users must interact with the system simultaneously, control entries by one user should not interfere with those of another. Computer automation should be viewed as a user. Operators should not interfere with automated actions which provide safety function and the computer should not prevent an operator from operating equipment as necessary (with appropriate authorization).
- Navigation - Users should be able to move easily among displays.
- Avoid Information Re-entry - Users should not be required to re-enter information already available to the system

.

**Alarm Management**

The purpose of a monitoring/control system alarm is to interrupt the operator's normal work. Too many interruptions have the potential to overwhelm an operator and result in an inappropriate operator response (e.g., fail to detect actual operational problems). The purpose of alarms is not to replace an operator's surveillance of a plant/process system. Alarms are a mechanism for informing an operator of an equipment malfunction, process deviation, or abnormal condition that requires an operator response. Using a life cycle approach to Alarm Management should improve the reliability of a SIS design that includes an operator response to an alarm.

Conditions under which an alarm is to be defined are as follows:

- All alarms shall require an operator action - if it doesn't require an operator action, then it is not an alarm condition.
- All alarms shall be distinct - multiple alarms that signify the same thing and require the same operator response should be eliminated or grouped to be presented to the operator as a single alarm.
- Alarms and alarm limits shall be created so that they are timely - items that are expected to be detected during normal surveillance (e.g., parameter takes > 30 minutes to reach abnormal range) are not alarmed until an operator action is required.

Annunciation and display of alarms should be as follows:

- All alarms shall have identified alarm priorities based on the Alarm Management Philosophy (importance / response time / complexity of operator response).
- All alarms shall have an audible annunciation.
- Alarm limit changes and alarm suppression required due to changes in operational state shall be identified.

Documentation of alarm information should include the following:

- Alarm Type (specific alarm on a process measurement, e.g., low process variable)
- Alarm Management Philosophy/ Alarm Priority
    - "Drop what you are doing and start response now."
        - Operation outside of this limit threatens safety envelope or is outside safety envelope
        - Alarm response requires complex operator interaction (including interaction with other plant systems)
        - A unique (not the obvious) technical response is required
        - Response required within 5-15 minutes
    - "Wrap up your current task and start response quickly."
    - "Start response soon"
        - instrument malfunction where the instrument does not have an associated process alarm
        - condition which must be evaluated to restart processing
- Alarm class (a group of alarms with common alarm management requirements)
- Alarm limit value or logical condition (e.g., off-normal)
- Operator action (response)

.

- Consequence of inaction or incorrect action
- Need for advanced alarm handling techniques, such as alarm suppression logic

**System Maintainability**

Human factors engineering requirements are to be defined for the maintenance interfaces of the SIS life cycle. Many of the HFE principles and guidance for the maintenance interfaces are addressed in NUREG-0700[3] and DOE-HDBK-1140-2001, *Human Factors/ Ergonomics Handbook for the Design and Ease of Maintenance*[5]. Designing for SIS maintainability should promote good instrumentation-maintainer interfaces, consistent labeling, minimize the potential for human errors during maintenance activities, and provide indication of display failure.

Accessibility requirements should be considered in the design of the maintenance of the SIS life cycle. Technicians should have adequate room to access components within the instrumentation cabinet, to prevent inadvertent tripping of a circuit breaker. Environmental considerations such as illumination are included in the design requirements to ensure adequate lighting inside cabinets. Although HFE analyses may not be needed for the design of many maintenance interfaces, typically HFE analyses can be used to resolve human performance issues (e.g., time to repair a SIS component) involved with the maintenance task. These maintenance tasks may need a formal HFE evaluation to substantiate performance assumptions that were derived from other analyses.

Bypasses may be necessary for certain maintenance activities. Leaving systems in bypass however, is potentially dangerous. With many systems, when an input is in bypass, there is no indication at the panel of the true state of the input[6]. How do you know whether the signal is healthy or not before you turn the bypass off? What if the input goes into alarm while it is in bypass? How can you tell? The system should be designed so that even when an input is in bypass, the true state indication of the field device is provided.

NUREG-0711[4] references additional reviews and analyses that may be applicable for the maintenance design of SIS life cycle. There may be maintenance tasks that are implicit or even explicitly considered in risk assessment, for example, time to repair a component. Those maintenance tasks may need a formal human factors evaluation to substantiate assumptions on their performance that have been made in other analyses. Activities necessary for SIS life cycle maintenance should be planned and controlled, and maintenance personnel should have the necessary experience, proper training, and adequate equipment to perform their expected safety functions.

Major considerations related to SIS life cycle maintenance activities are:

- Design consideration of the Maintainer as a User (i.e., assess maintenance activities to determine an optimum maintenance interface for the SIS such as diagnostic displays, glove boxes, or system location).
- Procedures, measures, and techniques are applied during/ for maintenance activities that provide clear guidance for conducting work in support of safe and reliable SIS operation.
- SIS component proof testing and preventive maintenance activities are identified, planned, scheduled, and conducted.

.

- Verification processes are performed that demonstrate worker adherence to SIS maintenance procedures.
- Clear indications of the true state are provided for functions that are bypassed.

## Software Quality Assurance Integration with Human Factors Engineering

The DOE Standard[1] provides information concerning Software Quality Assurance (SQA) for safety software. It provides a table ("Crosswalk of SQA Work Processes with Acceptable Industry and Other Implementation Guidance Standards") that has details for SQA activities. Several of these work processes are similar to HFE work processes:

- Software Project Management and Quality Assurance Planning
- Software Procurement and Supplier Management
- Software Requirements Identification and Management
- Software Design and Implementation
- Verification and Validation

### Planning

Integrating the overlapping areas of SQA and HFE life cycles streamlines the work for the facility/project. A Human Factors Engineering Plan (HFEP) should address the integration with the Software Quality Assurance Plan (SQAP). Generally, the tasks required by the HFEP are to be developed and approved according to the requirements of the SQAP.

### Procured (Acquired) Software

NQA-1 (referenced by the SQA crosswalk table) or other documents which drive SQA requirements would have guidelines/requirements for Acquired Software. Performance requirements or acceptance criteria for the software would be developed. At the time these documents are written, HFE needs consideration and incorporation into these documents. An HFE task analysis is to be performed to determine the basic functionality required of the operator interface, in areas such as information display, user-system interaction, and alarm management. Analysis techniques would vary according to the type of interface and type of process. If the system is to be installed in an existing facility or plant, the “rule of thumb” is to use the same basic type of interface that is used elsewhere in the facility. HFE requirements based on the analysis would be included in the procurement documentation.

### Software Requirements

As with procured software, an HFE task analysis is to be performed to determine the basic functionality required of the operator interface, in areas such as information display, user-system interaction, and alarm management. Analysis techniques will vary according to the type of interface and type of process. If the system is installed in an existing facility or plant, the “rule of thumb” is to use the same basic type of HSI that is used elsewhere in the facility. If a system with a similar HSI and a similar process is available, informal operator interviews and simulator walk-through would be appropriate. If a similar HSI and a similar process are not available, a

.

walk through of an HFE checklist by a person with knowledge of the planned process would be appropriate. A listing of applicable HFE guidelines and conventions would be developed. A requirements specification for software would be prepared that incorporates the HFE guidelines/conventions to be used.

**Software Design**

HFE requirements should be considered from the earliest stages of the design process. A determination must be made (as part of the normal design process) as to which functions should be performed automatically by the system (such as interlocks, advanced control strategies, and sequenced operations) versus the functions to be performed by the operator. The ability of an operator to perform necessary tasks and to operate equipment safely and efficiently must also be considered.

As the design matures, HFE guidelines/conventions in the requirements documentation must be satisfied. A checklist of HFE criteria should be used to ensure that HFE requirements have been met in the design.

**Implementation**

The HFE information in the Requirements and Design documentation must be satisfied during the implementation of software configuration/computer program development. A checklist of HFE criteria may again be used to document how the implementation of the design fulfills the criteria.

**Acceptance Testing (Verification and Validation)**

The operator interface should be reviewed against the established requirements specification and design to ensure that HFE concerns are addressed appropriately. These reviews may be incorporated as part of the acceptance testing. Where human actions are credited by an authorization basis document, the test plan shall include steps to show that the operator is able to respond in a timely manner (e.g., operator can respond to the SIS alarm and perform the required manual action). Off-line testing/ simulator trials may be performed, if available and applicable.

**Continuous Improvement**

The facility should be monitored for potential HFE improvements in the user-system interface. Some examples may be:

- Initial attempts at applying HFE to alarms may be fine-tuned.
- Some parts of the system may be taken out of service, and this may affect some aspects of HFE (e.g., unnecessary controls being present).

Changes/modifications should be implemented using normal software configuration management practices. Any documentation developed or changed as a result of a modification (such as Requirements, Design, or Test Plans) should address applicable HFE criteria.

.

## Conclusions

When operator response is credited as part of a SIS, incorporation of sound HFE principles in the SIS design and throughout the SIS life cycle is important to ensure that the SIS will perform its intended SIF when relied upon. Incorporating HFE early in the SIS design process is typically less costly than re-design efforts that may have to occur when human performance problems appear during process operations. Integration of the overlapping areas of SQA and HFE design life cycles streamlines the necessary work for the facility or project.

## Acknowledgements

The preceding paper is based on the information compiled by the authors over the course of serving on the Human Factors Engineering subcommittee and as Working Group members for the Department of Energy technical standard development project on how digital instrumentation and controls are accounted for in safety system design and maintenance. The effort was led by DOE headquarters Office of Nuclear Safety, Quality Assurance, and Environment (HS-20). The affiliations of the co-authors are: Dr. Beth Vail, URS Safety Management Solutions, Aiken SC; LeRoy Goff, URS, Waste Treatment Project, Hanford; Laura Sheets, Savannah River Nuclear Solutions (SRNS), Savannah River Site (SRS); Linda Olsen, independent consultant, Amarillo, TX; Russell Harwood, DOE Office of River Protection, Hanford. Mr. Rich Izard, of SRNS, SRS, also participated as a subcommittee representative.

## References

1. DOE-STD-XXXX-YR (Draft), *Application of Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities*, Department of Energy, TBD.

2. American National Standards Institute/ International Society of Automation (ANSI/ISA) 84.00.01, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*, 2006.

3. NUREG-0700, Rev. 2, *Human Machine Interface Design Review Requirements*, US Nuclear Regulatory Commission, May 2002.

4. NUREG-0711, Rev 2, *Human Factors Engineering Program Review Model,* US Nuclear Regulatory Commission, February 2004.

5. DOE-HDBK-1140-2001, *Human Factors / Ergonomics Handbook for the Design For Ease of Maintenance*, Department of Energy, February 2001.

6. Gruhn, P. and Cheddie, H.L., *Safety Instrumented Systems: Design, Analysis and Justification,* 2nd Edition, The Instrumentation, Systems and Automation Society (ISA), 2006, p. 193-194.

.

# Appendix

## Table 1: Human Factors Standards and Guidance Documents

| HFE Phase | Standard/Document | HFE Guidance Provided |
|---|---|---|
| Planning | DOE-HDBK-1140-2001, *Human Factors Ergonomics Handbook for Ease of Maintenance* | Provides guidelines for ease of maintenance. |
| | NUREG-0711, *Human Factors Engineering Program Review Model,* Rev. 2 | Defines an approach for ensuring that the HFE aspects of a facility are developed, designed, and evaluated on the basis of a structured analysis using accepted HFE principles. |
| | EPRI 1008122, *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation and Maintenance* | General analytical tool for considering system design and required operator actions. It includes a comparison of how control room operators perform control room tasks and or respond to alarm conditions in traditional analog control rooms versus a modernized control room that incorporates digital instrument and control systems. |
| | IEEE-Std-845, *IEEE Guide to Evaluation of Man-Machine Performance in Nuclear Power Generation Station Control Room and Other Peripheries* | Provides guidance for the selection and application of human factors techniques to carry out the following tasks:<br>▪ Evaluation of a given man-machine design in control rooms and other control areas to ascertain the degree of design adequacy;<br>▪ Determination, as needed, of changes to increase acceptability of a man-machine design; and<br>▪ Determination of the relative adequacy of alternative designs. |
| | ANSI/IEEE-Std-1023, *Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities* | Helps in evaluating the effect that automated system actions have on the operator's understanding of process operations and the potential for operator confusion. Also, it provides general guidance to address human error and the implementation of design features to mitigate undesirable consequences associated with anticipated human errors. |

.

## Table 1: Human Factors Standards and Guidance Document (continued)s

| HFE Phase | Standard/Document | HFE Guidance Provided |
|---|---|---|
| HFE Analysis (Requirements, Guidelines, Conventions) and Requirements & Design | ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions* | Provides guidelines to be applied in determining time requirements for safety-related operator response. |
| | DOE-HDBK-1140-2001, (Same as Planning) | (See Planning) |
| | DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Reports* | Provides guidance in identifying the human-machine interfaces required for ensuring safety function during normal, abnormal, and emergency operations. This guide also identifies interfaces for surveillance and maintenance of safety systems, structures, and components during normal operations. |
| | EPRI 1008122 (Same as Planning ) | (See Planning) |
| | ANSI/ISA 18.2, *Management of Alarm Systems for the Process Industries* | Covers all aspects of alarm management. |
| | MIL-STD-1472, *Department of Defense Design Criteria Standard – Human Engineering* | Presents human engineering design criteria, principles and practices to be applied in the design of systems, equipment and facilities. |
| | NUREG-0700, *Human-System Interface Design Review Guidelines,* Rev. 2 | Provides a comprehensive review for HFE principles and design guidelines, regardless of the platform. |
| Implementation | ANSI/ANS 3.5, *Nuclear Power Plant Simulators for Use in Operator Training and Examination* | Provides guidance for simulator model requirements. |
| Testing | NUREG-0711, *Human Factors Engineering Program Review Model,* Rev. 2 | Defines an approach to ensure that the HFE aspects of the facility are developed, designed, and evaluated on the bases of a structured analysis using accepted HFE principles. |
| Continuous Improvement | NUREG-0711, (Same as Testing) | (See Testing) |

.