HFE SAFETY REVIEWS OF ADVANCED NUCLEAR POWER PLANT CONTROL ROOMS

N94-33613

John O'Hara
Brookhaven National Laboratory
Department of Advanced Technology
Human Factors & Performance Analysis Group
Upton, New York 11973

Advanced control rooms (ACRs) will utilize human-system interface (HSI) technologies that may have significant implications for plant safety in that they will affect the operator's overall role and means of interacting with the system. The Nuclear Regulatory Commission (NRC) reviews the human factors engineering (HFE) aspects of HSIs to ensure that they are designed to good HFE principles and support operator performance and reliability in order to protect public health and safety. However, the only available NRC guidance was developed more than ten years ago, and does not adequately address the human performance issues and technology changes associated with ACRs. Accordingly, a new approach to ACR safety reviews was developed based upon the concept of "convergent validity." This paper describes this approach to ACR safety reviews.

INTRODUCTION

Nuclear Regulatory Commission (NRC) human-system interface (HSI) reviews have typically been directed toward the unique control rooms (CRs) of individual nuclear power plants (NPPs) because these plants and their CRs were already in existence at the time the reviews were performed. Detailed plant designs were evaluated prior to making a safety determination. The NRC and the utility industry have embarked on an effort to standardize future commercial NPP designs. The NRC has issued 10 CFR 52 titled "Early site permits; standard design certifications; and combined licenses for nuclear power plants," in order to achieve these objectives and streamline the licensing process. NPP vendors have begun the design of advanced standard plants, which are being submitted to the NRC for review and certification under Part 52. The General Electric Advanced Boiling Water Reactor, Combustion Engineering System 80+, and Westinghouse AP600 are examples of designs undergoing this type of review.

These designs will employ ACRs which, in comparison to those of conventional plants, utilize increased automation and computer-based HSI technologies that will affect the operators' overall role and their means of interacting with the plant. In addition to technology differences between ACRs and conventional plants, one of the issues to emerge from the initial ACR reviews was that detailed HSI design information was not available. In part because of rapidly changing technology, much of the detailed HSI design will not be completed prior to the issuance of a design certification. Thus the NRC is performing the design certification evaluation based on a process which describes the human factors engineering (HFE) elements that are necessary and sufficient for the development and implementation of an acceptable detailed design.

Since the review of a design process has not been performed in the nuclear industry in the past, and the types of advanced technology employed in ACRs are significantly different from conventional plants, criteria for ACR review are not adequately addressed by current regulations and review guidance.[1-2] Thus, the criteria for the review of a HFE design *process* and guidelines for the review of the design *product* had to be developed. The HFE Program Review Model (PRM) and Advanced HSI design Guideline, hereafter called the "Guideline," were developed to meet these objectives. In the following sections, the issues that were considered in the development of the review criteria are discussed followed by a discussion of the PRM and Guideline development.

ISSUES IMPACTING REVIEW METHOD DEVELOPMENT

In order to develop an approach to the evaluation of ACRs, it was necessary to consider issues related to trends in advanced NPP design and related human factors issues.

Diversity in Advanced Reactor Technology: The current generation of commercial NPPs operating in the U.S. numbers more than 100; all of those are based upon light water reactor technology. Although the next generation of plants will reflect advances on this technology base, the industry has also developed designs based on different technologies, including heavy water, liquid metal, and gas-cooled reactors. One important design initiative to improve safety and reliability has been the move from "active" safety features (based upon active components such as pumps) toward more "passive" safety features (based upon natural physical processes such as convection flow, radiation cooling, and gravity). This plant diversity and the passive features introduce new and different systems for operators to monitor, control, and test. These will result in different operator roles and tasks that must be understood in performing safety reviews.

HSI Evolution: There are several important trends emerging in advanced HSI design concepts in the nuclear industry, including: (1) increased automation changing the operator's role to system monitor, supervisor, and automated system back-up; (2) centralization of controls and displays into "compact" workstations; (3) use of large display panels visible from anywhere in the ACR to present high-level information and critical parameters; (4) operator's interface with a data management system rather than with components; (5) data integration and graphic displays; and (6) decision-support aids. As these trends are implemented, they will result in a wide range of technological approaches to HSIs.

While the use of advanced technology is generally considered to enhance system performance, advanced HSIs also have the potential to negatively impact human performance, spawn new types of errors, and reduce human reliability.[3-6] Despite its increasing utilization in complex systems such as NPPs and aircraft, there is a consensus that further research is needed to understand the effects of this technology on human performance and system safety.[7-8] With the trends in control room design, cognitive issues are emerging as more significant than the physical and ergonomic considerations which dominated the design of conventional HSIs. For example, increases in automation and poor allocation of function decisions that occur early in the design process have been associated with a shift from physical to cognitive workload, loss of operator vigilance, increase in human errors,[9] difficulty maintaining adequate "situation awareness,"[10] and decay of task performance skills when required because of automated system failure. Thus, the National Academy of Sciences has identified areas such as automation, supervisory control, and human-computer interface as high priority research areas for the human factors community in general and for the commercial nuclear industry in particular.[7,8] The review process should be sensitive to known and emerging human performance issues and design considerations that give rise to them.

Guidelines to Support Design and Evaluation: For conventional plants, NRC CR reviews rest heavily on an evaluation of the physical aspects of the HSI using HFE guidelines.[2] In an ACR, the physical layout of the display devices and computer input devices may be less important than the design of the human-software interface. Information in ACRs can be presented in a complex network of hundreds of displays. The difficulty of developing HFE guidelines for the adequate design of human-software interfaces has been well documented.[11] Significant to the evaluation of human-software interfaces is that many of the important design features are often hidden to the reviewer (and transparent to the operator). For example, the observed display may be an end product of extensive data processing and integration which results in higher-level, more abstract information than was the case in "single sensor/single display" designs characteristic of conventional CRs). As a result, while hardware guidelines tend to be relatively clear and specific, software guidelines tend to be stated in more general language and have a considerably weaker research/experience base. Thus, an evaluation of ACRs cannot rest on HFE guidelines alone.[12-13] Weakness in a guideline-based evaluation will have to be compensated for with other evaluation methods.

The issues discussed above have implications for the development of an approach to the safety review of the HFE aspects of advanced reactor designs. First, an evaluation methodology should provide guidance for reviews to be performed throughout the design process to final design and be sensitive to HFE issues at each point. Second, evaluation methods will have to provide for the review of a broad range of advanced HSI technologies. Third, reviews should extend beyond HFE guideline-based evaluations and include a diversity of evaluation techniques. These factors have led to the technical approach reflected in the PRM and Guideline development described in the following sections.

HFE PROGRAM REVIEW MODEL

PRM Development

The general philosophy underlying the PRM's development is that "safety" is a concept that is not directly observed but must be inferred from available evidence. When reviewing a design to make a safety assessment, different types of information obtained from different assessment methods are weighted towards or against an acceptable finding. Each method has its correlation with safety and each has its own sources of bias and error. The reviewer would like to collect as much information as possible in order to establish "convergent validity"[14]; i.e., to establish a coherent finding across different evaluation methods. This approach is similar to a "defense-in-depth" concept applied to HFE/HSI evaluation.

The types of information that can provide assessments of HSI safety include: (1) HFE Planning including an HFE design team, program plans and procedures; (2) design analyses and studies including requirements/function/task analyses, technology assessments, trade-off studies, etc.; (3) design specifications and descriptions; and (4) verification and validation (V&V) analyses of the final design, e.g., compliance with accepted HFE guidelines and operation of the integrated system with operators performing the required tasks under actual (or simulated) conditions). The greatest confidence in a finding that a design is safe can be obtained from one which was: (1) developed by a qualified HFE design team using an acceptable HFE program plan; (2) the result of appropriate HFE studies and analyses which provided accurate and complete inputs to the design process and to V&V assessment criteria; (3) designed using proven technology based upon human performance and task requirements incorporating accepted HFE standards and guidelines; and (4) evaluated with a thorough V&V test program. The PRM was developed around this concept.

There were four specific objectives of the PRM development:

- to develop a model to serve as a technical basis for the review of the development and design of HSIs that is (1) based upon currently accepted practices, (2) well-defined, and (3) validated through experience with the development of complex, high-reliability systems;
- to identify the HFE elements in a system development, design, and evaluation process that are necessary and sufficient requisites to successful integration of the human component in complex systems;
- to identify which aspects of each HFE element are key to a safety review and are required to monitor the process; and
- to identify the types of acceptance criteria by which HFE elements can be evaluated.

To meet these objectives, a technical review of current HFE guidance and practices was conducted along two dimensions: *Technical Basis* (literature providing the theoretical and regulatory basis for evaluating the conduct of HFE); and *Application* (literature reflecting the practice of HFE for development, design and evaluation of complex, high-reliability systems). General systems literature, as well as literature focused specifically on the nuclear industry, was reviewed. From this review a generic system development, design, and evaluation process was defined. Once specified, key HFE elements were identified, and general criteria by which they are assessed (based upon a review of current literature and accepted practices in the field of human factors engineering) were developed.

The PRM was based largely on applied general systems theory[15-16] and the DoD system development process which is rooted in systems theory.[17] Applied general systems theory provides a broad approach to system design and development based on a series of clearly defined developmental steps, each with clearly defined goals and with specific management processes to attain them. System engineering has been defined as "...the management function which controls the total system development effort for the purpose of achieving an optimum balance of all system elements. It is a process which transforms an operational need into a description of system parameters and integrates those parameters to optimize the overall system effectiveness."[17]

The effective integration of HFE considerations into the design is accomplished by: (1) providing a structured top-down approach to system development which is iterative, integrative, interdisciplinary and requirements driven, and (2) providing a management structure which details the HFE consider-

ations in each step of the overall process. A structured top-down approach to NPP HFE is consistent with recent nuclear industry standards for advanced control room design[18-19] and with the recognition in the nuclear industry that human factors issues and problems emerge throughout the NPP design and evaluation process. The systems engineering approach was expanded to develop a PRM to be used for the advanced control room design and implementation process review by the incorporation of NRC HFE requirements.

PRM Description

In this section an overview of the PRM is presented to generally describe the HFE elements, the products reviewed for each element, and the acceptance criteria used to evaluate the element.

The PRM is intended as the programmatic approach to achieving a design commitment to HFE. The overall commitment and scope of the HFE effort can be stated as follows: Human-system interfaces (HSI) should be provided for the operation, maintenance, test, and inspection of the NPP that reflect state-of-the-art human factors principles. For the purposes of PRM development "state of the art" human factors principles were defined as those principles currently accepted by human factors practitioners. "Current" is defined with reference to the time at which an HSI is developed. "Accepted" is defined as a practice, method, or guide which is (1) documented in the human factors literature within a standard or guidance document that has undergone a peer-review process, and/or (2) justified through scientific/industry research practices.

The PRM developed to achieve this commitment contains eight elements. Each consists of an overall objective and factors that must be considered in the review process. A very brief description of each element follows. A more complete description along with specific review criteria for each element can be found elsewhere.[20]

Element 1: Human Factors Engineering Program Management - To assure the integration of HFE into system development, an HFE Design Team and an HFE Program Plan should be established to assure the proper development, execution, oversight, and documentation of the program. As part of the program plan an HFE issues tracking system (to document and track resolution of problems, concerns, issues) should be established.

Element 2: Operating Experience Review - The accident at Three Mile Island in 1979 and other reactor incidents have illustrated significant problems in the actual design and the design philosophy of NPP HSIs. There have been many studies as a result of these incidents and utilities have implemented both NRC mandated changes and additional improvements on their own initiative. Problems and issues encountered in similar systems of previous designs should be identified and analyzed so that they are avoided in the development of the current system or, in the case of positive features, to ensure their retention.

Element 3: System Function Requirements Analysis - System requirements should be analyzed to identify those functions which must be performed to satisfy the objectives of each function area. System function analysis should: (1) determine the objective, performance requirements, and constraints of the design; and (2) establish the functions which must be accomplished to meet the objectives and required performance.

Element 4: Allocation of Function - The allocation of functions should take advantage of human strengths and avoid allocating functions which would be adversely impacted by human limitations. A structured and well-documented methodology of allocating functions to personnel, system elements, and personnel-system combinations should be developed.

Element 5: Task Analysis - Task analysis should provide the systematic study of the behavioral requirements of the tasks that the personnel subsystem is required to perform in order to achieve the functions allocated to them. The task analysis should: (1) form the basis for specifying the requirements for the displays, data processing and controls needed to carry out crew tasks; (2) provide one basis for making design decisions; e.g., determining before hardware fabrication whether system performance requirements can be met by combinations of anticipated equipment,

software, and personnel; (3) assure that human performance requirements do not exceed human capabilities; (4) be used as basic information for developing procedures, and (5) be used as basic information for developing staffing, skill, training, and communications requirements.

Element 6: Human-System Interface Design - Human engineering principles and criteria should be applied along with all other design requirements to identify, select, and design the particular equipment to be operated/maintained/controlled by plant personnel.

Element 7: Plant and Emergency Operating Procedure Development - Plant and Emergency Operating Procedures should be developed to support and guide human interaction with plant systems and to control plant-related events and activities. Human engineering principles and criteria should be applied along with all other design requirements to develop procedures that are technically accurate, comprehensive, explicit, easy to utilize, and validated.

Element 8: Human Factors Verification and Validation (V&V) - V&V evaluations should assure that the performance of the HSI achieves, when all elements are fully integrated into a system, (1) all HFE design goals as established in the program plan; (2) all system functional requirements, and (3) all requirements to support human operations, maintenance, test, and inspection task accomplishments. Four types of evaluations should be performed:

1. Human Factors Issue Resolution Verification - All issues documented in the Human Factors Issue Tracking System of Element 1 should be resolved.

2. HSI Task Support Verification - All controls, displays, alarms, and data processing that are required to accomplish human safety-related tasks and actions should be available.

3. HFE Verification - All controls, displays, alarms, and data processing support provided by the HSI should be appropriate to the crew tasks and designed according to accepted HFE guidelines, standards, and principles.

4. Integrated System Validation - The integration of HSI elements with each other and with personnel should be validated through dynamic task performance evaluation. The evaluations should have as their objectives: (1) demonstrating the adequacy of entire HSI configuration for achievement of safety goals, (2) confirmation of function allocation and the structure of tasks assigned to personnel, (3) adequacy of staffing and the HSI to support the staff in the accomplishment of their tasks, (4) adequacy of procedures, (5) confirmation of the adequacy of the dynamic aspects of all HSIs for task accomplishment, and (6) evaluation and demonstration of tolerance of the design to human error and system failures.

ADVANCED HSI DESIGN REVIEW GUIDELINE

Guideline Development

While the PRM addresses the design process, guidance is needed to support the review of detailed HSI design products of that process (as part of PRM Element 8 described above). The Advanced HSI Design Review Guideline was developed to provide these review criteria and was intended to update the available CR review guideline.[2] In the discussion below, the term "Guideline" (with a capitol "G") refers to the entire document, while the term "guideline" refers to the individual guidelines within the document. A more detailed description of the Guideline development and contents is available elsewhere.[21]

Based upon an evaluation of research and industry experience related to the integration of personnel into advanced systems, a set of High-Level Design Review Principles was developed (see Table 1). These principles provide the generic HSI characteristics necessary to support operator performance and make systems more tolerant to human errors when they occur. Since these principles are stated at a fairly general level, they were further developed to a level of detail sufficient to support HSI review and evaluation. The principles were translated into terms that could be applied to specific applications by developing guidelines for the review of the specific types of technology (e.g., graphic

displays and expert systems).

Table 1. High-Level Design Review Principles

Category	Principle
General	Safety, Cognitive Compatibility, Physiological Compatibility, Simplicity of Design, Consistency
Primary Task Design	Situation Awareness, Task Compatibility, User-Model Compatibility, Organization of HSI Elements, Logical/Explicit Structure, Timeliness, Controls/Displays Compatibility, Feedback
Secondary Task Control	Cognitive Workload, Response Workload
Task Support	Flexibility, User Guidance & Support, Error Tolerance & Control

The effort to develop detailed guidelines began with an identification of existing human factors guidance documents for advanced HSIs. Through a review of the human factors literature, approximately 50 guideline efforts were identified. To identify those that would serve as the "primary sources" for the Guideline, a high priority was given to establishing the validity of the prior guidelines; i.e., assuring that they were based upon empirical research and/or accepted human engineering practice. Validity was defined in terms of two aspects of document development. "Internal" validity was evaluated by the degree to which the individual guidelines within a document were based upon empirical research and provided an audit trail to that research. "External" validity was evaluated as a function of the degree to which the guidelines were subjected to independent peer review. The peer review process was considered a good method of screening guidelines for conformance to accepted human engineering practices. In general, documents which had strong validity were considered primary source documents to serve as a basis for the Guideline.

The guidelines from the primary sources were edited to combine similar guidelines and to transform the material into a standardized format. Where compound guidelines were encountered (several guidelines in a single statement) an effort was made to break them into logical units and represent the units as separate guidelines. Conflict resolution between guidelines was handled on a case-by-case basis.

Guideline Description

The guidelines were organized into seven major sections which are described below. Each of these sections contains a set of general guidelines and more detailed guidelines addressing specific HSI implementations, techniques, and formats.

Information Display - This section deals primarily with the formatting of text and graphic visual displays. Guidance is provided in top-down fashion beginning with display formats (such as topology displays and trend graphs), display format elements (such as labels, icons, symbols, color, coding, etc.), data quality and update rate, and display devices.

User-System Interaction - This section addresses the modes of interaction between the operator and the HSI. Topics include dialog format, navigation, display controls, entering information, system messages, prompts, and system response time. This section also contains guidelines pertaining to methods for ensuring the integrity of data such as inadvertent change or deletion of data, minimization of data loss due to computer failure, and protection of data such as setpoints.

Process Control and Input Devices - This section addresses information entry, operator dialog, display control, information manipulation, and system response time. Considerations of display-control integration are also included here.

Alarms - This section is currently a place holder for the results of another NRC research project to develop review guidance in the area of advanced alarm systems.

Analysis and Decision Aids - This section addresses the use of knowledge-based systems.

Inter-Personnel Communication - This section contains guidelines for activities related to speech and computer-mediated communication between plant personnel, e.g., preparing, addressing, transmitting and receiving messages.

Workplace Design - This section addresses the organization of displays and controls within individual workstations and control room configuration and environment.

In addition to a hard-copy document, the Guideline has been developed as an interactive, computer-based review aid. Each guideline in the database is represented by several primary fields: guideline number, title, guideline statement, additional information, and source (link to primary source document). Other user assistance fields are also available, e.g., to provide location (in the document) information and a note pad for users to append comments related to specific guidelines. The interactive document will facilitate review planning, guideline access and evaluation, data analysis, and report preparation. Guideline maintenance such as editing and the incorporation of new guidelines as they become available is also supported. Availability of the Guideline on a portable computer will also facilitate in-the-field reviews. An Apple Macintosh™ computer and Hypercard™ software were selected for prototyping. The prototype user interface provides for many document functions such as instant table of contents (ToC) access, context index, glossary, and place markers. Users can automatically go to desired sections by clicking on the ToC or index.

CONCLUSIONS

A framework for the review of ACRs has been developed. Safety evaluations are based upon the information from both the design process and its products. The PRM provides criteria for the review of the design process and the Guideline provides criteria for the review of the HSI resulting from the process. This framework is being used to support the NRC reviews of the HFE programs for the current ACR designs being evaluated for design certification.

ACKNOWLEDGEMENT

This research is being performed under the auspices of the U.S. Nuclear Regulatory Commission.

REFERENCES

1. U.S. Nuclear Regulatory Commission, "Standard Review Plan, Rev. 1," NUREG-0800, U.S. Nuclear Regulatory Commission, Washington, DC, 1984.

2. U.S. Nuclear Regulatory Commission, "Guidelines for Control Room Design Reviews," NUREG 0700, Washington, DC, 1981.

3. Coblentz, A., "Vigilance and Performance in Automated Systems," NATO ASI SERIES D, Vol. 49, Kluwer Academic Publishers, Boston, MA, 1988.

4. Rasmussen, J., Duncan, K., and Leplat, J., NEW TECHNOLOGY AND HUMAN ERROR, J. Wiley and Sons, Publishers, New York, NY, 1987.

5. Wiener, E., and Nagel, D. (Eds.), HUMAN FACTORS IN AVIATION, Academic Press, New York, NY, 1988.

6. O'Hara, J., "The Effects of Advanced Technology Systems on Human Performance and Reliability," Proceedings of the Topical Meeting on Nuclear Plant Instrumentation, Control, and Man-Machine Interface Technologies, LaGrange Park, Illinois, 1993.

7. Committee on Human Factors, "Research Needs for Human Factors," National Research Council, National Academy of Sciences, Washington, DC, 1983.

8. Moray, N., and Huey, B., (Eds.), "Human Factors Research and Nuclear Safety," National Research Council, National Academy of Sciences, Washington, DC, 1988.

9. Warm, J., and Parasuraman, R. (Eds.), "Vigilance: Basic and Applied Research," HUMAN FACTORS, Vol. 29, Special Issue, 1987, 623-740.

10. Kibble, M., "Information Transfer from Intelligent EW Displays," Proceedings of the Human Factors Society - 32nd Annual Meeting, 1988, 107-110.

11. Smith, S., "Standards Versus Guidelines for Designing User Interface Software," HANDBOOK OF HUMAN-COMPUTER INTERACTION, Elsevier Science Publishers, Amsterdam, 1988.

12. Reaux, R., and Williges, R., "Effects of Level of Abstraction and Presentation Media on Usability of User-System Interface Guidelines," Proceedings of the Human Factors Society - 32nd Annual Meeting, 1988.

13. Potter, S., Cook, R., Woods, D., and McDonald, J., "The Role of Human Factors Guidelines in Designing Usable Systems: A Case Study of Operating Room Equipment," Proceedings of the Human Factors Society - 34th Annual Meeting, 1990.

14. Campbell, D., and Fisk, D., "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," PSYCHOLOGICAL BULLETIN, Vol. 56, 1959, 81-105.

15. Bailey, R.W., HUMAN PERFORMANCE ENGINEERING: A GUIDE FOR SYSTEM DESIGNERS, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1982.

16. Gagne, R.M., and Melton, A.W. (Eds.), PSYCHOLOGICAL PRINCIPLES IN SYSTEM DEVELOPMENT, Holt, Rinehart and Winston, New York, NY.

17. Kockler, F., Withers, T., Podiack, J., and Gierman, M., "Systems Engineering Management Guide," Department of Defense AD/A223 168), Defense Systems Management College, Fort Belvoir, VA, 1990.

18. International Electrotechnical Commission, "International Standard: Design for Control Rooms of Nuclear Power Plants," IEC 964, Bureau Central de la Commission Electrotechnique Internationale, Geneva, Switzerland, 1989.

19. Institute of Electrical and Electronics Engineers (IEEE), "IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations," STD 1023-1988, IEEE, New York, 1988.

20. O'Hara , J. and Higgins, J., " HFE program review model and acceptance criteria for evolutionary reactors," TR NO. L2314-5-7/92, Brookhaven National Laboratory, Upton, New York, 1992.

21. O'Hara, J., Brown, W, Baker, C., Welch, D., Granda, T. and Vingelis, P., "Advanced Human System Interface Design Review Guideline," DRAFT NUREG/CR-5908, Brookhaven National Laboratory, Upton, New York, 1993.