Conf-930401--17

BNL-NUREG-48657

Human Factors Engineering Program Review Model for Advanced Nuclear Power Reactors

John O'Hara and James Higgins
Brookhaven National Laboratory
Upton, New York 11973

Clare Goodman, Greg Galletti and Richard Eckenrode
U.S. Nuclear Regulatory Commission
Rockville, Maryland 20852

ABSTRACT

One of the major issues to emerge from the initial design reviews under the certification process was that detailed human-system interface (HSI) design information was not available for staff review. To address the lack of design detail issue, the Nuclear Regulatory Commission (NRC) is performing the design certification reviews based on a design process plan which describes the human factors engineering (HFE) program elements that are necessary and sufficient to develop an acceptable detailed design specification. Since the review of a design process is unprecedented in the nuclear industry, the criteria for review are not addressed by current regulations or guidance documents and, therefore, had to be developed. Thus, an HFE Program Review Model was developed. This paper will describe the model's rationale, scope, objectives, development, general characteristics, and application.

The staff of the Nuclear Regulatory Commission (NRC), Human Factors Assessment Branch is currently evaluating the human factors engineering (HFE) programs submitted as part of the certification process for advanced reactor designs. NRC human-system interface (HSI) reviews have typically been directed toward existing control rooms (CRs) or existing systems (such as SPDS). However, the NRC and the utility industry have embarked on an effort to improve and standardize future commercial nuclear power plant 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 encourage standardization and to streamline the licensing process. Nuclear plant designers and vendors have begun the design of advanced standard plants, which are being submitted to the NRC for review and approval 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.

The licensing process of Part 52 consists of a Final Design Approval by the NRC followed by a standard design certification that is issued as an NRC Rule. This will require formal rule-making and include the opportunity for a public hearing before the Atomic Safety and Licensing Board (ASLB). The certification, when issued, would be valid for 15 years (renewable). During its tenure neither the NRC nor the designer can change or impose new requirements on the standard design certification without a new rule-making. Utilities would have the option of purchasing the standard design and utilizing it as already approved by the NRC.

In order to ensure that an as-built plant conforms to the standard design certification, inspections, tests, analyses, and acceptance criteria (ITAAC) must be specified as part of the standard design certification. After certification, the NRC will ensure that the design has met the ITAAC. A utility desiring to license and operate a nuclear power plant under Part 52, will obtain a Combined Operating License (COL), which authorizes both construction and operation in one step. The COL applicant may propose a new design or reference an existing standard design certification.

In order to obtain a standard design certification under Part 52, a designer must submit a Standard Safety Analysis Report (SSAR) to the NRC for review. The NRC's review of the SSAR is issued as a Final Safety Evaluation Report (FSER) which will form the basis for the Final Design Approval.

One of the major issues to emerge from the initial CR design reviews under the certification process was that detailed HSI design information was not available for staff review as part of the design certification evaluation. In the past the staff has reviewed detailed plant designs prior to making a safety determination. However, because of continually changing technology, much of the HSI design will not be completed prior to the issuance of a design certification for the evolutionary and passive designs currently under review. To address the issue of lack of design detail, the NRC is performing the design certification evaluation based on a design implementation process plan which describes the HFE program elements required to develop an acceptable detailed design specification. Along with the design process, NRC will require the applicant to submit ITAAC/Design Acceptance

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

Criteria (DAC), which will ensure that the design process is properly executed by the COL applicant. The NRC specified that the design and implementation process should contain descriptions of all required human factors activities that are necessary and sufficient for the development and implementation of the HSIs. It should also include an identification of predetermined NRC conformance review points and the ITAAC/DAC.

This process is very different from the typical HSI reviews conducted by the NRC in the past. The present NRC review criteria presented in the Chapter 18 of the Standard Review Plan (SRP)[1] and in NUREG-0700[2] provide little information to the reviewer for this type of evaluation. Since the review of a design process is unprecedented in the nuclear industry, the criteria for review are not addressed by current regulations and guidance documents and had to be developed. The staff, in conjunction with Brookhaven National Laboratory, has developed an HFE Program Review Model. This paper will describe the model's rationale, scope, objectives, development, general characteristics, and application.

RATIONALE

The general philosophy underlying the model's development is that "safety" is a concept that is not directly observed but must be inferred from available evidence. When reviewing a design in order to make a safety assessment, evidence is collected and weighted towards or against an acceptable finding. As in the assessment of any inferred concept, different types of data can be collected. Each has its overall correlation with safety and each has its strengths and weaknesses. The reviewer would like to collect as much data as possible in order to establish "convergent validity"[3]; i.e., to establish a consistent finding across different types of data, each with its own sources of bias and error. This approach is similar to a "defense-in-depth"[4] concept applied to HFE/HSI evaluation.

The types of information that can provide assessments of HSI safety include:

- HFE Planning (including an HFE design team, program plans and procedures),
- Design analyses and studies (including requirements/function/task analyses, technology assessments, trade-off studies, etc.),
- Design specifications and descriptions, and
- 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).

These categories of information all have their strengths and weaknesses, but are probably listed in an order of increasing correlation with safety, i.e., greater reliance on full-mission testing should be made as compared with the make-up of an HFE design team and program plan. It is tempting to view V&V as definitive, but it also is subject to error. There are two principal reasons for this. First, the criteria used in V&V evaluations are often derived from the analyses performed during the design process. For example, (1) the results of task analysis may be used as criteria in the verifying that all required controls and displays are provided to support crew functions; (2) the guidance developed in the design specification may be used to verify conformance to HFE standards and principles; and (3) the performance requirements developed in the system requirements and function analyses may be used as performance criteria in full-mission testing. For these criteria to be credible and to establish confidence in the V&V results, safety evaluators must have assurance that the criteria were derived using appropriate and acceptable methods (which should have been laid out in an HFE program plan).

Second, full-mission evaluations (e.g., Validation) cannot test all possible conditions of HSI usage and will generally be performed using a simulator which creates a somewhat artificial environment which can modify crew behavior; e.g., (1) with respect to the influence of performance shaping factors (PSFs), and (2) important human information processing parameters. With respect to PSFs, simulator exercises will not reflect with high fidelity the influence of all important factors (such as stress, noise, and chaos/distractions) that will affect human performance during real-world operations. With respect to human information processing, important aspects of human cognition and performance (such as signal detection threshold, event probability estimation, and response selection) are affected by the operating crew's understanding that they are participating in a simulated rather than real situation. For example, when a simulator exercise begins, the operator knows something other than normal operations are likely. Unlike the real world, very low probability events are likely to occur and will be anticipated by the crew. Thus, the operator's attention is aroused and focused on event occurrence and detection. When a situation does occur, the crew's response will be likely be optimized according to established procedures since there are no consequences to responses made on a simulator and no conflict between safety and productivity goals. There are major consequences to real-world actions which will affect an operator's probability and timing of taking actions. All of these factors require the recognition of uncertainties in the use of simulator data. A good V&V plan can help reduce these threats to the validity of the results, but they cannot be completely eliminated. Therefore, the generalization from simulation to real-world contains uncertainty which limits the "external validity" (generalizability) of the results.

Thus, the greatest confidence in a finding that a design is safe can be placed in one which has the following characteristics: (1) it was developed by a qualified HFE design team including all the skills required using an acceptable HFE program plan; (2) it was the result of appropriate HFE studies and analyses which provide accurate and complete inputs to the design process and inputs to V&V assessment criteria; (3) it was designed using proven technology based upon human performance and task requirements incorporating accepted HFE standards and guidelines; and (4) it was evaluated with a thorough V&V test program.

MODEL SCOPE

The overall scope of the HFE Program Review Model was limited by two factors. First, those elements of a complete HFE program that are already adequately addressed by existing NRC requirements for license applicants were excluded from the scope of the model (e.g., training program development, and detailed site-specific procedure development). Second, those aspects of review that are the responsibility of other NRC review teams were also excluded. This category includes human reliability analysis which, while important to HFE program development, is the responsibility of other reviewers.

MODEL DEVELOPMENT OBJECTIVES AND METHOD

Review criteria are required to assure that the design reflects currently acceptable HFE practices. Thus, a technical basis for review of a design process was developed and is described in this section. The specific objectives of the model development effort were:

1. To develop an HFE program review model to serve as a technical basis for the review of the development and design of HSIs. The model requirements were that it be: (1) based upon currently accepted practices, (2) well-defined, and (3) validated through experience with the development of complex, high-reliability systems.

2. 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.

3. To identify which aspects of each HFE element are key to a safety review and are required to monitor the process.

4. To identify the types of acceptance criteria by which HFE elements can be evaluated.

A technical review of current HFE guidance and practices was conducted to identify important human factors program plan elements relevant to a design process review. The review 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, were reviewed. Thus, the sources reviewed included a wide range of nuclear industry and non-nuclear industry documents, including those currently under development as part of the Department of Defense (DoD) MANPRINT program.[5]

From this review a generic system development, design, and evaluation process was defined. Once specified, key HFE elements were identified, 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 HFE Program Review Model was developed based largely on applied general systems theory[6-8] and the DoD system development process which is rooted in systems theory.[9-13] A full list of documents contributing to the technical basis of the Model are provided elsewhere.[14]

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."[9]

Utilization of the DoD system development as an input to the development of the Generic HFE Program Model was based on several factors. DoD policy identifies the human as a specific element of the total system.[13] A systems approach implies that all system components (hardware, software, personnel, support, procedures, and training) are given adequate consideration in the developmental process. A basic assumption is that the personnel element receives serious consideration from the very beginning of the design process. In addition, the military has applied HFE for the longest period of time (as compared with industrial-commercial system developers). Their process is more highly evolved and formalized and represents the most highly developed model available. Finally, since military system development and acquisition is tightly regulated by federal, DoD, and military branch laws, regulations, requirements, and standards, the model provides the most finely grained, specifically defined HFE process available.

Within the DoD system, the development of a complex system begins with the mission or purpose of the system, and the capability requirements needed to satisfy mission objectives. Systems engineering is essential in the earliest planning period to develop the system concept and to define the system requirements. During the detailed design of the system, systems engineering provides:

- balanced influence of all required design specialties,
- resolution of interface problems,
- the effective conduct of trade-off analyses,
- the effective conduct of design reviews, and
- the verification and validation of system performance.

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 considerations in each step of the overall process. A structured top-down approach to nuclear plant HFE is consistent with the approach to new control room design as described in Appendix B of NUREG-0700[2] and the more recent nuclear industry standards for advanced control room design.[15-16] The approach is also consistent with the recognition in the nuclear industry that human factors issues and problems emerge throughout the NPP design and evaluation process and therefore, human factors issues are best addressed with a comprehensive top-down program.[17-18] The systems engineering approach was expanded to develop an HFE Program Review Model to be used for the advanced control room design and implementation process review by the incorporation of NRC HFE requirements.

GENERAL MODEL DESCRIPTION

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

The model 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" (10 CFR 50.34(f)(2)(iii)) as required by 10 CFR 52.47(a)(1)-(ii). For the purposes of model development "state of the art" human factors principles was 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 model developed to achieve this commitment contains eight elements. Each element consists of an overall objective and factors that must be considered in the review process. In its general form, the materials reviewed for each element consists of an Implementation Plan, Analysis Report, and HFE Design Team Review Report. However, the specific submittals must be tailored to each unique review. A very brief description of each element follows. A more complete description along with specific review criteria for each element can be found elsewhere.[14]

Element 1: Human Factors Engineering Program Management - To assure the integration of HFE into system development and the achievement of the goals of the HFE program, 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 HFE related problems/concerns/issues and their solutions throughout the HFE program) 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 accidents incidents. Utilities have implemented both NRC mandated changes and additional improvements on their own initiative. However, the changes were formed based on the constraints associated with backfits to existing CRs using early 1980's technology which limited the scope of corrective actions that might have been considered, i.e., more effective fixes could be used in designing a new CR with the modern technology typical of advanced CRs. 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 Functional Requirements Analysis - System requirements should be analyzed to identify those functions which must be performed to satisfy the objectives of each functional 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 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 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 tasks; (2) provide one of the bases for making design decisions; e.g., determining before hardware fabrication, to the extent practicable, 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 manning, skill, training, and communication requirements of the system.

Element 6: Human-System Interface Design - Human engineering principles and criteria should be applied along with all othe. 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 - The objective of the V&V evaluations should be to 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; and (2) all system functional requirements, and (3) all requirements to support human operations, maintenance, test, and inspection task accomplishments. The successful incorporation of human factors engineering into the final HSI design should be thoroughly evaluated through a series of specific verification evaluations and the integrated system should be validated using HFE evaluation procedures, guidelines, standards, and principles. 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 verified as adequately addressed.

2. HSI Task Support Verification - All controls, displays, alarms, and data processing that are required to accomplish human safety-related tasks and actions [as defined by the task analysis, EOP analysis, and probabilistic risk assessment/human reliability analysis (PRA/HRA)] should be verified as available through the HSI.

3. HFE Verification - All controls, displays, alarms, and data processing support provided by the HSI should be verified to be appropriate to the crew tasks and designed according to accepted HFE guidelines, standards, and principles. If HFE issues were identified during the review conducted as part of Element 6, resolution of those issues may also be verified as part of the HFE Verification.

4. Integrated System Validation - The integration of HSI elements with each other and with personnel should be evaluated and validated through dynamic task performance evaluation using evaluation tools which are appropriate to the accomplishment of this objective under a range of operational conditions, including normal and off-normal conditions. The evaluations should have as their objectives:

- Adequacy of entire HSI configuration for achievement of safety goals,
- Confirmation of function allocation and the structure of tasks assigned to personnel,
- Adequacy of staffing and adequacy of the HSI to support the staff in the accomplishment of their tasks,
- Adequacy of procedures,
- Confirmation of the adequacy of the dynamic aspects of all HSIs for task accomplishment, and
- Evaluation and demonstration of tolerance of the design to human error and system failures.

MODEL APPLICATION

The model is specified in a generic form and must, therefore, be tailored to the requirements of each specific review. Tailored versions of the model are currently being developed to support the staff reviews of the HFE programs for the General Electric Advanced Boiling Water Reactor, Combustion Engineering System 80+, and Westinghouse AP600.

While the HFE review model and its elements were developed specifically to address the programmatic review of HSIs for advanced reactor designs, the principles apply to the review of retrofits and modifications to control rooms and HSIs in existing plants as well. However, the detailed scope to the model's requirements may not be fully applicable to retrofits/modifications to existing plants and may also have to be tailored to specific reviews.

REFERENCES

1. U.S. NUCLEAR REGULATORY COMMISSION, "Standard Review Plan," NUREG-0800, Revision 1, Washington, D.C. (1984).

2. U.S. NUCLEAR REGULATORY COMMISSION, "Guidelines for Control Room Design Reviews," NUREG-0700, U.S. Government Printing Office, Washington, D.C. (1981).

3. CAMPBELL, D. and FISK, D., "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," Psychological Bulletin, 56, 81-105 (1959).

4. INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, "Basic Safety Principles for Nuclear Power Plants," Safety Series No. 75-INSAG-3, Vienna, Austria: International Atomic Energy Agency (1988).

5. BOOHER, H. R. (Ed.), MANPRINT: An Approach to Systems Integration, Van Nostrand Reinhold, New York (1990).

6. BAILEY, R. W., Human Performance Engineering: A Guide for System Designers, Prentice-Hall, Inc., Englewood Cliffs, New Jersey (1982).

7. GAGNE, R. M. and MELTON, A. W. (Eds.), Psychological Principles in System Development, Holt, Rinehart and Winston, New York.

8. VAN COTT, H. P., and KINKADE, R. G., "Human Engineering Guide to Equipment Design," U.S. Government Printing Office, Washington, D.C., 1-16 (1972).

9. 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, Virginia (1990).

10. DEPARTMENT OF DEFENSE, "System Engineering Management Plan," DI-MGMT-81024, Office of Management and Budget, Washington, D.C. (1990).

11. DEPARTMENT OF DEFENSE, "Human Engineering Requirements for Military Systems, Equipment and Facilities," MIL-H-46855B, Office of Management and Budget, Washington, D.C. (1979).

12. DEPARTMENT OF DEFENSE, "Human Engineering Procedures Guide," DOD-HDBK-763, Office of Management and Budget, Washington, D.C. (1979).

13. DEPARTMENT OF DEFENSE, "Manpower and Personnel Integration (MANPRINT) in the Material Acquisition Process," AR 602-2, Department of the Army, Washington, D.C. (1990).

14. O'HARA, J. and HIGGINS, J., "HFE Program Review Model and Acceptance Criteria for Evolutionary Reactors, BNL Technical Report L2314-5-7/92, Brookhaven National Laboratory, Upton, New York (1992).

15. 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).

16. IEEE, "IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations," Standard 1023-1988 (1988).

17. BEATTIE, J. and MALCOLM, J., "Development of a Human Factors Engineering Program for the Canadian Nuclear Industry," Proceedings of the Human Factors Society - 35th Annual Meeting, Human Factors Society, Santa Monica, California (1991).

18. STUBLER, W., ROTH, E., and MUMAW, R., "Evaluation Issues for Computer-Based Control Rooms," Proceedings of the Human Factors Society - 35th Annual Meeting, Human Factors Society, Santa Monica, California (1991).