

---

# Human Factors Engineering Program Review Model

---

---

**U.S. Nuclear Regulatory Commission**

Office of Nuclear Reactor Regulation



9408220036 940731  
PDR NUREG  
0711 R PDR

## AVAILABILITY NOTICE

### Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW., Lower Level, Washington, DC 20555-0001
2. The Superintendent of Documents, U.S. Government Printing Office, Mail Stop SSOP, Washington, DC 20402-9328
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC bulletins, circulars, information notices, inspection and investigation notices; licensee event reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, international agreement reports, grant publications, and NRC booklets and brochures. Also available are regulatory guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG-series reports and technical reports prepared by other Federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions. *Federal Register* notices, Federal and State legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Administration, Distribution and Mail Services Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, for use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

---

---

# Human Factors Engineering Program Review Model

---

---

Manuscript Completed: July 1994  
Date Published: July 1994

Division of Reactor Controls and Human Factors  
Office of Nuclear Reactor Regulation  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001



## ABSTRACT

The staff of the Nuclear Regulatory Commission is performing nuclear power plant design certification reviews based on a design process plan that describes the human factors engineering (HFE) program elements that are necessary and sufficient to develop an acceptable detailed design specification and an acceptable implemented design. There are two principal reasons for this approach. First, the initial design certification applications submitted for staff review did not include detailed design information. Second, since human performance literature and industry experiences have shown that many significant human factors issues arise early in the design process, review of the design process activities and results is important to the evaluation of an overall design. However, cur-

rent regulations and guidance documents do not address the criteria for design process review. Therefore, the HFE Program Review Model (HFE PRM) was developed as a basis for performing design certification reviews that include design process evaluations as well as review of the final design. A central tenet of the HFE PRM is that the HFE aspects of the plant should be developed, designed, and evaluated on the basis of a structured top-down system analysis using accepted HFE principles. The HFE PRM consists of ten component elements. Each element is divided into four sections: Background, Objective, Applicant Submittals, and Review Criteria. This report describes the development of the HFE PRM and gives a detailed description of each HFE review element.



# CONTENTS

	<i>Page</i>
ABSTRACT .....	iii
ACKNOWLEDGMENTS .....	ix
ACRONYMS .....	xi
GLOSSARY .....	xiii
 1 INTRODUCTION .....	 1-1
1.1 Background .....	1-1
1.2 General Issues Affecting the Review of Advanced Nuclear Power Plant Human System Interfaces ....	1-1
1.2.1 Trends in Advanced Nuclear Power Plants .....	1-2
1.2.2 Advanced Technology and Human Performance .....	1-2
1.2.3 Advanced Human-System Interface Guidelines Issues .....	1-3
1.2.4 Implications for Advanced Human-System Interface Review .....	1-4
1.3 HFE PRM Rationale and Relationship to Safety .....	1-4
1.4 HFE PRM Development .....	1-6
1.4.1 Objectives .....	1-6
1.4.2 Technical Scope .....	1-6
1.4.3 Development Methodology .....	1-6
1.4.4 General HFE PRM Description .....	1-7
1.4.5 HFE PRM Applications and Interpretation .....	1-9
 2 ELEMENT 1 - HFE PROGRAM MANAGEMENT .....	 2-1
2.1 Background .....	2-1
2.2 Objective .....	2-1
2.3 Applicant Submittals .....	2-1
2.4 Review Criteria .....	2-1
2.4.1 General HFE Program Goals and Scope .....	2-1
2.4.2 HFE Team and Organization .....	2-2
2.4.3 HFE Process and Procedures .....	2-2
2.4.4 HFE Issues Tracking .....	2-3
2.4.5 Technical Program .....	2-3
 3 ELEMENT 2 - OPERATING EXPERIENCE REVIEW .....	 3-1
3.1 Background .....	3-1
3.2 Objective .....	3-2
3.3 Applicant Submittals .....	3-2
3.4 Review Criteria .....	3-2
3.4.1 Scope .....	3-2
3.4.2 Issue Analysis, Tracking, and Review .....	3-3
 4 ELEMENT 3 - FUNCTIONAL REQUIREMENTS ANALYSIS AND FUNCTION ALLOCATION .....	 4-1
4.1 Background .....	4-1
4.2 Objective .....	4-2
4.3 Applicant Submittals .....	4-2

	<i>Page</i>
4.4 Review Criteria .....	4-2
4.4.1 General Criteria .....	4-2
4.4.2 Functional Requirements Analysis .....	4-2
4.4.3 Function Allocation Analysis .....	4-4
5 ELEMENT 4 – TASK ANALYSIS .....	5-1
5.1 Background .....	5-1
5.2 Objective .....	5-1
5.3 Applicant Submittals .....	5-1
5.4 Review Criteria .....	5-1
6 ELEMENT 5 – STAFFING .....	6-1
6.1 Background .....	6-1
6.2 Objective .....	6-1
6.3 Applicant Submittals .....	6-1
6.4 Review Criteria .....	6-1
7 ELEMENT 6 – HUMAN RELIABILITY ANALYSIS .....	7-1
7.1 Background .....	7-1
7.2 Objective .....	7-1
7.3 Applicant Submittals .....	7-1
7.4 Review Criteria .....	7-3
7.4.1 Human Reliability Analysis Methodology .....	7-3
7.4.2 Integration of Human Reliability Analysis with HFE Design .....	7-4
8 ELEMENT 7 – HUMAN-SYSTEM INTERFACE DESIGN .....	8-1
8.1 Background .....	8-1
8.2 Objective .....	8-1
8.3 Applicant Submittals .....	8-1
8.4 Review Criteria .....	8-1
9 ELEMENT 8 – PROCEDURE DEVELOPMENT .....	9-1
9.1 Background .....	9-1
9.2 Objective .....	9-1
9.3 Applicant Submittals .....	9-1
9.4 Review Criteria .....	9-1
10 ELEMENT 9 – TRAINING PROGRAM DEVELOPMENT .....	10-1
10.1 Background .....	10-1
10.2 Objective .....	10-1
10.3 Applicant Submittals .....	10-1
10.4 Review Criteria .....	10-1
11 ELEMENT 10 – HUMAN FACTORS VERIFICATION AND VALIDATION .....	11-1
11.1 Background .....	11-1
11.2 Objective .....	11-2
11.3 Applicant Submittals .....	11-2
11.4 Review Criteria .....	11-2

	<i>Page</i>
11.4.1 General Criteria .....	11-2
11.4.2 Human System Interface Task Support Verification .....	11-3
11.4.3 HFE Design Verification .....	11-3
11.4.4 Integrated System Validation .....	11-3
11.4.5 Human Factors Issue Resolution Verification .....	11-4
11.4.6 Final Plant HFE/Human System Interface Design Verification .....	11-5
12 REFERENCES .....	12-1
APPENDIX A: HFE DESIGN TEAM COMPOSITION	
APPENDIX B: OPERATING EXPERIENCE REVIEW ISSUES	

## ACKNOWLEDGMENTS

In November of 1991, The Nuclear Regulatory Commission requested Brookhaven National Laboratory (BNL) to assist in developing human factors engineering review criteria for advanced reactor human-system interface design implementation process. The early drafts quickly became a common reference point for the NRC reviewers and the nuclear plant designers whose designs were under review for certification. NUREG 0711, the HFE Program Review Model, provides a consolidated source of human factors design certification review guidance for NRC reviewers.

Many people participated in the development of the Program Review Model. However, without the effort of John M. O'Hara of BNL, this report would not exist. He is the senior author and the individual who took the initial concept and developed it into a comprehensive review plan.

Thanks also to James C. Higgins and William F. Stubler of BNL who also authored substantial portions of the document.

The NRC staff who provided direction, guidance, and critical review of this report include, but are not limited to, Clare Goodman, Richard J. Eckenrode, James P. Bongarra, Greg S. Galletti, Donna L. Smith and Garmon West Jr.

BNL staff who provided insights, assistance and constructive reviews of all work associated with the project include Robert Hall, Bill Luckas, Sonja Haber, Debbie Shurberg, and Mike Barriere. Also, Dan Welch of Carlow International, Inc. provided valuable assistance to the early phases of this effort. Special thanks are given to Kathleen Nasta for her tremendous help in preparing the manuscript.

Finally, thanks to the applicants for design certification at General Electric, Combustion Engineering, and Westinghouse, who provided many insights and challenging comments on drafts of this report.

## ACRONYMS

AEOD	Office for Analysis & Evaluation of Operational Data	LOCA	loss-of-coolant accident
ACR	advanced control room	LPCI	low pressure coolant injection
ADS	automatic depressurization system	LWR	light water reactor
ALWR	advanced light water reactor	MMI	man-machine interfaces
ANS	American Nuclear Society	MIL	military
ANSI	American National Standards Institute	MUX	multiplexer
ASLB	Atomic Safety and Licensing Board	NPP	nuclear power plant
ATWS	anticipated transients without scram	NRC	Nuclear Regulatory Commission
BNL	Brookhaven National Laboratory	NRR	Office of Nuclear Reactor Regulation
BOP	balance of plant	NSSS	nuclear steam supply system
BWR	boiling water reactor	NUCLARR	Nuclear Computerized Library for Assessing Reactor Reliability
CDF	core damage frequency	OECD	Organization for Economic Cooperation and Development
CFR	<i>U.S. Code of Federal Regulations</i>	OER	operating experience review
COL	combined operating license	OSC	operational support center
CR	control room	OSHA	Occupational Safety and Health Administration
DAC	design acceptance criteria	PRA	probabilistic risk assessment
DC	direct current	PSF	performance shaping factor
DD	design description	RAMI	reliability, availability, maintainability, and inspection
DMS	data management system	RCS	reactor coolant system
DOD	Department of Defense	RHR	residual heat removal
EOF	emergency offsite facility	RPV	reactor pressure vessel
EOP	emergency operating procedure	RSS	remote shutdown system
EPG	emergency procedure guideline	SBO	station blackout
EPRI	Electric Power Research Institute	SER	significant event report
ESF	engineered safety feature	SHARP	Systematic human action reliability procedure
FSER	final safety evaluation report	SLC	standby liquid control
FW	feedwater	SPDS	safety parameter display system
GSI	generic safety issue	SRP	Standard Review Plan
GTG	generic technical guidance	SRV	safety/relief valve
HEP	human error probability	SS	shift supervisor
HFE	human factors engineering	SSAR	standard safety analysis report
HFE PRM	Human Factors Engineering Program Review Model	SSC	structure, system, and component
HRA	human reliability analysis	SSLC	safety-related system logic and control
HSI	human-system interface	STD	standard
I&C	instrumentation and control	SW	service water
IAEA	International Atomic Energy Agency	THERP	technique for human error rate prediction
IEEE	Institute of Electrical and Electronics Engineers	TMI	Three Mile Island
INSAG	International Nuclear Safety Advisory Group	TSC	technical support center
ISLOCA	interfacing system loss-of-coolant accident	URD	utility requirements document
ITAAC	inspections, tests, analyses, and acceptance criteria	USI	unresolved safety issue
LCO	limiting condition for operation	V&V	verification and validation
LCS	local control station	VDU	video display unit
LER	licensee event report	WTEC	World Technology Evaluation Center

## GLOSSARY

**Advanced control room (ACR)**—A control room that is primarily based on digital technology. ACRs typically provide the primary operator interaction with the plant via computer-based interfaces, such as video display units. This is in contrast to "conventional" control rooms, which provide the primary operator interaction with the plant via analog interfaces, such as gauges.

**Applicant**—An organization such as a nuclear plant vendor or utility that is applying to the U.S. Nuclear Regulatory Commission for design certification or plant licensing.

**Critical tasks**—Tasks that must be accomplished in order for personnel to perform their functions. In the context of probabilistic risk assessment, critical tasks are those that are determined to be significant contributors to plant risk.

**Cognitive error**—A human error that results from the characteristics of human information processing such as errors in diagnosis due to information overload.

**Component**—An individual piece of equipment such as a pump, valve, or vessel; usually part of a plant system.

**Function**—An action that is required to achieve a desired goal. Safety functions are those functions that serve to ensure higher-level objectives and are often defined in terms of a boundary or entity that is important to plant integrity and the prevention of the release of radioactive materials. A typical safety function is "reactivity control." A high-level objective, such as preventing the release of radioactive material to the environment, is one that designers strive to achieve through the design of the plant and that plant operators strive to achieve through proper operation of the plant. The function is often described without reference to specific plant systems and components or the level of human and machine intervention that is required to carry out this action. Functions are often accomplished through some combination of lower-level functions, such as "reactor trip." The process of manipulating lower-level functions to satisfy a higher-level function is defined here as a control function. During function allocation the control function is assigned to human and machine elements.

**Human-centered design goals**—Human factors engineering design goals that address the cognitive and physical support of personnel performance.

**Human factors**—A body of scientific facts about human characteristics. The term covers all biomedical, psychological, and psychosocial considerations; it includes, but is not limited to, principles and applications in the areas of human factors engineering, personnel selection, training,

job performance aids, and human performance evaluation (see "Human factors engineering").

**Human factors engineering (HFE)**—The application of knowledge about human capabilities and limitations to plant, system, and equipment design. HFE ensures that the plant, system, or equipment design, human tasks, and work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support it (see "Human factors").

**Human-system interface (HSI)**—The means through which personnel interact with the plant, including the alarms, displays, controls, and job performance aids. Generically this includes maintenance, test, and inspection interfaces as well. Local control station (LCS)—An operator interface related to nuclear power plant (NPP) process control that is not located in the main control room. This includes multifunction panels, as well as single-function LCSs such as controls (e.g., valves, switches, and breakers) and displays (e.g., meters) that are operated or consulted during normal, abnormal, or emergency operations.

**Mockup**—A static representation of an HSI (see "Simulator" and "Prototype").

**Performance shaping factors (PSFs)**—Factors that influence human reliability through their effects on performance. PSFs include factors such as environmental conditions, HSI design, procedures, training, and supervision.

**Personal Safety**—See "Safety."

**Plant**—The nuclear power plant in its entirety including all plant systems and components.

**Plant Safety**—See "Safety."

**Prototype**—A dynamic representation of an HSI that is not linked to a process model or simulator (see "Simulator" and "Mockup").

**Safety**—The term used in the following contexts in the HFE Program Review Model:

**Personal safety**—Relates to the prevention of individual accidents and injuries of the type regulated by the Occupational Safety and Health Administration.

**Plant safety**—Also called "safe operation of the plant." A general term used herein to denote the technical safety objective as articulated by the International Nuclear Safety Advisory Group of the International Atomic Energy Agency (IAEA) in the



## Introduction

**"Basic Safety Principles for Nuclear Power Plants"** (IAEA, 1988): "To prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small." See Section 1.4 for additional discussion.

**Safety evaluation**—The NRC process of reviewing an aspect of an NPP to ensure that it meets requirements and that it will perform as needed to reliably ensure plant safety.

**Safety function**—See "Function."

**Safety issue**—An item identified during plant design, operation, or review that has the potential to affect the safe operation of the plant.

**Safety-related**—A term applied to those NPP structures, systems, and components (SSCs) that prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public (see Appendix B to Part 50 of Title 10 of the *U.S. Code of Federal Regulations*). These are the SSCs on which the design-basis analyses of the safety analysis report are performed. They also must be part of a full quality assurance program in accordance with Appendix B.

**Simulator**—A facility that physically represents the HSI configuration and that dynamically represents the operating characteristics and responses of the plant in real time (see "Prototype" and "Mockup").

**Situation awareness**—The relationship between the operator's *understanding* of the plant's condition and its actual condition at any given time.

**State-of-the-art human factors principles**—Those principles currently accepted by human factors practitioners. "Current" is defined with reference to the time at which a program management or implementation plan is prepared. "Accepted" is defined as a practice, method, or guide that (1) is documented in the human factors literature within a standard or guidance document that has undergone a peer-review process or (2) can be justified through scientific research and/or industry practices.

**System**—An integrated collection of plant components and control elements that operate alone or with other plant systems to perform a function.

**Task**—A group of activities that have a common purpose, often occurring in temporal proximity, and that utilize the same displays and controls

**Top-down design**—A review approach starting at the "top" with high-level plant mission goals that are decomposed into functions that are allocated to human and system resources and are decomposed into tasks required to accomplish function assignments. Tasks are arranged into meaningful jobs and the HSI is designed to best support job task performance. The detailed design is the "bottom" of the top-down process.

**Vigilance**—The degree to which personnel are attentive to their current task.

**Workload**—The physical and cognitive demands placed on plant personnel.

## **Introduction**



# 1 INTRODUCTION

## 1.1 Background

The staff of the Human Factors Assessment Branch of the Nuclear Regulatory Commission (NRC) is currently evaluating the human factors engineering (HFE) programs submitted as part of the certification process for nuclear power plant (NPP) designs. The NRC has issued 10 CFR Part 52 (*U.S. Code of Federal Regulations*, Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," Title 10, "Energy") 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 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 rulemaking and includes the opportunity for a public hearing before the Atomic Safety and Licensing Board (ASLB). The certification, when issued, will 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 rulemaking.

Inspections, tests, analyses, and acceptance criteria (ITAAC) are specified as part of the standard design certification in order to ensure that an as-built plant conforms to the standard design certification. 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. After certification, the NRC will ensure that the COL applicant has performed and satisfied the ITAAC.

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.

Since human-system interface (HSI) technology is continually changing, much of the design will not be completed before a design certification is issued for the advanced reactor designs currently under review. Thus, the staff has concluded that it is necessary to perform HFE reviews of the design process as well as of the final design product for reasons discussed in detail in Section 1.2 below. The NRC is performing its evaluation based on a design and implementation process that includes the HFE program ele-

ments required to develop an acceptable detailed design and the evaluations to be performed to ensure that the final design reflects good HFE principles and that operator performance and reliability are appropriately supported in order to protect public health and safety. Along with the ITAAC as discussed above, the NRC requires the COL applicant to submit design acceptance criteria (DAC), which will ensure that the applicant properly executes the design process after certification. The NRC has 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.

In the past, staff evaluation of HFE acceptability was based on detailed plant design reviews. Thus, the staff has not conducted a design process review as part of the reactor licensing process. The evaluation criteria in Chapter 18 of the Standard Review Plan (SRP, NUREG-0800) and in "Guidelines for Control Room Design Reviews" (NUREG-0700), therefore, provide little information to support this type of evaluation. To support advanced reactor reviews, an HFE Program Review Model (HFE PRM) was developed to provide criteria for the evaluation of a design process as well as the final design implementation itself.

## 1.2 General Issues Affecting the Review of Advanced Nuclear Power Plant Human System Interfaces

In addition to the regulatory issues discussed above, other factors were considered in the development of an HFE PRM. This section gives an overview of the general issues, considerations, and theoretical factors that provided the technical basis and context for the development of the HFE PRM. A more detailed discussion can be found elsewhere (O'Hara et al., 1994). To develop an approach to the review of the NPP HFE, it was necessary to consider the factors that can be expected to affect such reviews. Several sources of information were reviewed to identify significant issues, including

- research reports and publications on advanced technology being developed for HSIs in process control application
- information available on advanced NPP control room (CR) designs
- advanced instrumentation and controls surveys conducted for the
  - NRC (Carter and Uhrig, 1990).

- International Atomic Energy Agency (IAEA, Neboyan and Kossilov, 1990).
- Organization for Economic Cooperation and Development (OECD, Kennedy, 1988).
- World Technology Evaluation Center (WTEC, White and Lanning, 1991).
- general human factors literature on human information processing and the effects of advanced technology on human performance
- existing literature on human factors standards and guidelines for advanced HSI

On the basis of a review of the above material, many factors were identified that affect the review of the HFE characteristics of new or advanced designs. These factors are organized into three categories: (1) the trends in advanced NPPs, (2) the human factors issues that are associated with advanced technology, and (3) the state-of-the-art of human factors guidelines for advanced HSIs. The implications of these factors and their impact on the HFE review are summarized in Section 1.2.4.

### 1.2.1 Trends in Advanced Nuclear Power Plants

*Diversity in Advanced Reactor Technology:* The current generation of commercial NPPs operating in the United States numbers more than 100; all are based on light water reactor technology. Although the next generation of plants will reflect advances in this technology base, the industry has also developed designs based on different technologies, including heavy water reactors, liquid metal reactors, and gas-cooled reactors. One important design initiative has been to move from "active" safety features (based on active components such as pumps) toward more "passive" safety features (based on natural physical processes such as convection flow, radiation cooling, and gravity). This plant diversity and the new passive features introduce new and different systems for operators to control, test, and monitor. There are questions as to how the operators can verify the reliable functioning of these passive systems during plant operation. Also, the role of the operator during transients and accidents changes considerably with these new passive systems. Important questions include: (1) How can operators verify during normal operation that these systems are ready for emergency operation? (2) How can proper operation be confirmed when the systems are called upon? (3) What parameters should be monitored? and (4) What is the proper operator response when the passive systems do not function properly? Clearly, advanced NPPs will result in different operator roles and tasks, different CRs, and different operator-control interfaces. The HFE PRM must be capable of

enabling reviews of all possible designs and a great diversity of operator functional roles in the system.

*Trends in HSI Evolution:* Several important trends are emerging in advanced HSI design concepts in the nuclear industry, including (1) greater use of automation and a corresponding shift of the operator's role in the system as monitor, supervisor, and backup to automated systems; (2) greater centralization of controls and displays into "compact" digital workstations; (3) use of large display panels that can be seen from anywhere in the CR to present high-level information and critical parameters; (4) a primary operator interface with a data management system (DMS) with little interaction directly with components; (5) use of data integration and graphic displays; and (6) information processing and decision-support aids. As these trends are implemented, they will result in a wide range of technological approaches to HSI and CR types from conventional to hybrid to advanced to "intelligent" CRs. In part, this is due to the tremendous flexibility offered by software-driven interfaces to provide for alternative data processing, display, and control. An HFE PRM must enable complete and consistent reviews of designs reflecting such diversity in approaches to HSI and CR design.

### 1.2.2 Advanced Technology and Human Performance

While the use of advanced technology is generally considered to enhance system performance, computer-based operator interfaces also have the potential to negatively affect human performance, spawn new types of human errors, and reduce human reliability (Coblentz, 1988; Rasmussen et al., 1987; Wiener and Nagel, 1988; Woods et al., 1990). However, since the contributors to unreliability in an advanced control room are likely to be different from those that are present in conventional CRs, they are less obvious and generally less well understood (O'Hara and Hall, 1990). Some of the factors contributing to the problems of integrating human operators and advanced systems are reviewed below. The HFE PRM must enable the reviewer to identify such concerns and evaluate their resolution.

*General State of Knowledge:* Despite the rapidly increasing utilization of advanced HSI technology in complex, high-reliability systems such as NPPs and civilian aircraft, there is broad consensus that the knowledge base for understanding the effects of this technology on human performance and system safety is in need of further research (Committee on Human Factors, 1983; Moray and Huey, 1988). The operating environment associated with advanced systems is very different from that of a conventional CR. Human information processing issues are emerging as more significant than the physical and ergonomic considerations that dominated the design of conventional HSIs. Although these issues have been recog-

nized for a long time, their full implications for human performance and system safety have only recently begun to be addressed in research, and there is not a long history of operational experience on which to draw. The National Academy of Sciences, for example, 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 (Pew et al., 1983; Moray and Huey, 1988).

*Allocation of Function and Automation:* Many human factors problems originate early in the design process. Historically, functions were allocated to automated systems largely on the basis of the capability of available technology to reliably and safely execute the function, rather than the human operator's ability to perform as part of the overall system. This was true even though the human factors problems associated with automation had been known for some time (Edwards, 1977) and the emergence of new types of human and system errors had been identified (Wiener and Curry, 1980). Increases in automation have been associated with a shift from physical to cognitive workload, with a loss of operator vigilance and a concomitant increase in vigilance-associated human errors (Warm and Parasuraman, 1987), with difficulty maintaining adequate "situation awareness" (Kibble, 1988), and with loss of skills to perform the task in the event of automated system failure. In part, many of these issues may be the result of a shift in the operator's role from that of an active, in-the-loop controller to an out-of-the-loop supervisor and monitor, together with a failure on the part of the HSI and system designers to adequately account for this shift (Moray, Lootsteen, and Pajak, 1986; Wickens and Kessel, 1981; Ephrath and Young, 1981).

*Cognitive Factors:* Computer-based HSI design requires, to a far greater extent than traditional CR designs, the specification of cognitive requirements and processing resources that the operator must utilize in task performance, that is, cognitive task analysis. That information is needed for proper design and evaluation of the interface. Four aspects of HSI are primarily responsible for this requirement. First, information is typically presented in "predigested" form; that is, raw data parameters are processed and integrated into a higher level of information, thus possibly obscuring their meaning. Second, the operator typically has much more information available, which, if not properly organized and presented, can be overwhelming. Third, information is typically resident in the "virtual" workstation of a computer-based HSI, rather than in dedicated spatial locations spread out across control stations. Information is located somewhere in a computer system that provides only a glimpse of its contents (through a display device) at any one time. A poorly designed interface can make location of information and navigation through data difficult. Fourth, the flexibility of

software-driven interfaces can increase the workload associated with managing the interface itself (e.g., accessing displays, moving windows, and setting display modes).

*System Complexity and Operator Skills:* NPP operations have always demanded a high level of skill and readiness on the part of the operating staff. These demands may increase, however, because of the need for operators to understand and evaluate the performance of advanced systems, to know their limitations, and to be ready to assume manual control when appropriate. There is a somewhat paradoxical relationship between these requirements and the day-to-day tasks that operators must perform, which in a highly automated plant are predominantly monitoring functions. Thus, there is a risk that these carefully selected and highly trained operators may be required to perform a routinely boring and monotonous job.

### 1.2.3 Advanced Human-System Interface Guidelines Issues

In the past the staff has relied heavily on the use of HFE guidelines to support the identification of potential safety issues and their resolution. NUREG-0700 and Appendix B to Section 18 of NUREG-0800 are examples of this review guidance. In this section, issues related to the use and sufficiency of HFE guidelines for review of advanced systems are considered.

*Hardware vs. Software Guidelines:* For conventional plants, NRC HSI reviews rest heavily on an evaluation of the physical aspects of the HSI using HFE guidelines such as NUREG-0700. In an advanced control room (ACR), the physical layout of the display devices and computer input devices may be less important than the design of the human-software interface, that is, the information management system and the methods with which information is displayed to the operator. This information can be displayed in a complex network of hundreds of computer displays. The difficulty of developing guidelines for human-software interfaces when compared with human-hardware interfaces has been well documented (Smith, 1988). Perhaps most significant to the evaluation of human-software interfaces is that the most important design features are often hidden to the reviewer and transparent to the operator, while important hardware design features are usually readily observable. For example, the observable display may be an end product of extensive data processing providing higher-level, more abstract displays than was the case in the "single sensor/single display" designs characteristic of conventional CRs. As a result, while hardware review guidance tends to be relatively clear and specific, software guidance tends to be stated in more general language.

*Status of Guidelines for Advanced Technology:* ACRs are based on relatively new technology that is rapidly changing. Relative to the guidelines available for traditional

hardware interfaces, the guidelines available for computer-based software interfaces have a considerably weaker research base and have not been as well tested and validated through many years of design application. Thus, the human factors guidelines available for the review of advanced CR technology are less firm and, as indicated above, are typically stated in more general terms. Further, the cognitive task requirements, critical to human-software interface design, are typically less familiar to designers and reviewers (Woods et al., 1990; Karat, 1989). These characteristics of advanced technology guidelines can make the reviewers' job more difficult (Reaux and Williges, 1988).

*Suitability of Guidelines as a Basis for Review:* Another issue related to the maturity of advanced technology guidelines is whether evaluations based only on conformance to HFE guidelines provide a sufficient basis for review. Gould has indicated that because of the nature of advanced human-system interfaces (as discussed above), a good system cannot be designed by guidelines alone (Gould, 1988). A similar conclusion resulted from an effort to evaluate a computer-based system using only guidelines (Potter et al., 1990). While HFE guideline-based reviews for ACRs are a necessary part of safety evaluations, they are not sufficient as the sole basis of a safety determination. Reviews need to be broader and consider alternative sources of evaluation data.

#### 1.2.4 Implications for Advanced Human-System Interface Review

The issues discussed above have implications for the development of an approach to the safety evaluation of the HFE aspects of advanced reactor designs. These implications are summarized below.

- (1) The review approach should provide criteria to support safety evaluations to be performed during the design process as well as for final designs. Important reasons for this include the following:
  - Advanced reactor certification applications may provide CRs designed to conceptual levels of detail only; that is, detailed designs are not available for review.
  - Many significant human factors issues arise early in design, for example, initial goals/objectives of the design and allocation of functions to human and automated task performance.
- (2) Reviews of the HSIs should extend beyond HFE guideline evaluations and should include a variety of assessment techniques, such as validations of the fully integrated system under realistic, dynamic con-

ditions using experienced, trained operators performing the types of tasks the HSI has been designed for (including various types of failures and transient conditions).

- (3) Since human-software guidelines have been found to be more difficult to review than traditional hardware guidelines, reviewers must have supplemental information, such as that provided by the outputs of the design process, for example, the results of trade studies and analyses for HSI technology selection and design.

### 1.3 HFE PRM Rationale and Relationship to Safety

The general rationale underlying the PRM's development is that "plant safety" is a concept that is not directly observed but must be inferred from available evidence. As defined in the glossary, plant safety, also called "safe operation of the plant," is a general term used herein to denote the technical safety objective as articulated by IAEA: "To prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small" (IAEA, 1988). To ensure plant safety requires "defense in depth." Defense in depth includes the use of multiple barriers to prevent the release of radioactive materials and uses a variety of programs to ensure the integrity of barriers and related systems [a detailed discussion of this approach is provided in the IAEA basic safety principles (IAEA, 1988)]. These programs include, among others, conservative design, quality assurance, administrative controls, safety reviews, personnel qualification and training, test and maintenance, safety culture, and human factors.

Human factors plays a significant role in supporting plant safety and providing defense in depth. IAEA states:

One of the most important lessons of abnormal events, ranging from minor incidents to serious accidents, is that they have so often been the result of incorrect human actions. Frequently such events have occurred when plant personnel did not recognize the safety significance of their actions, when they violated procedures, when they were unaware of conditions of the plant, were misled by incomplete data or incorrect mindset, or did not fully understand the plant in their charge (p. 19, IAEA, 1988).

Thus "human factors" was established as an underlying technical principle that is essential to the successful application of safety technology for NPPs. The principle states:



Personnel engaged in activities bearing on nuclear power plant safety are trained and qualified to perform their duties. The possibility of human error in nuclear power plant operation is taken into account by facilitating correct decisions by operators and inhibiting wrong decisions, and by providing means for detecting and correcting or compensating for error (p. 19, IAEA, 1988).

IAEA further states that "attention to human factors at the design stage ensures that plants are tolerant to human error" (p. 19, IAEA, 1988).

The NRC process of reviewing an aspect of an NPP to ensure that it meets requirements and that it will perform as needed to reliably ensure plant safety is called a "safety evaluation." This evaluation includes an HFE safety evaluation.

The factors summarized in Section 1.2.4 above are consistent with the IAEA basic safety principles and have led to the development of a top-down approach for the conduct of an NRC safety evaluation of an NPP HFE program. Top-down refers to a review approach starting at the "top" with high-level plant mission goals that are broken down into the functions necessary to achieve the mission goals. Functions are allocated to human and system resources and are broken down into tasks for the purposes of specifying the alarms, information, and controls that will be required to accomplish function assignments. Tasks are arranged into meaningful jobs and the HSI is designed to best support job task performance. The detailed design (of the HSI, procedures, and training) is the "bottom" of the top-down process. The HFE safety evaluation should be broad based and include HFE aspects of normal and emergency operations, test, maintenance, etc.

The PRM is based on an approach to design review that is analogous to the defense-in-depth philosophy. When reviewing a design to make a safety evaluation, evidence is collected and weighted toward or against an acceptable finding. As in the assessment of any inferred concept, different types of information can be collected. Each has its overall correlation with plant safety and each has its strengths and weaknesses. The reviewer would like to collect as much information as possible in order to establish "convergent validity" (Campbell and Fisk, 1959), that is, to establish a consistent finding across different types of information, each with its own sources of bias and error.

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

- HFE planning (including an HFE design team, program plans, and procedures)

- design analyses and studies (including requirements, function and task analyses, technology assessments, tradeoff studies)
- design specifications and descriptions
- 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 types of information all have their strengths and weaknesses, but are probably listed in an order of increasing importance to plant safety review; that is, greater reliance should be placed on full-mission testing than on the makeup of an HFE design team and program plan. Although some may be tempted to view V&V as definitive, 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, which may not be perfect. For example, (1) the results of task analysis may be used as criteria in verifying that all required controls and displays are provided to support human 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 HSI validation. For these criteria to be credible and to establish confidence in the V&V results, one must have assurance that they were derived using appropriate and acceptable methods (which should have been laid out in an HFE program plan).

A second caution with V&V is that it is not possible to test all possible conditions of HSI usage during validation tests. In addition, validation will generally be performed using a simulator. Simulators create a somewhat artificial environment that can modify operator behavior, for example, with respect to (1) 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 it is participating in a simulated rather than a 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 likely be optimized accord-

ing to established procedures, since there are no consequences to responses made on a simulator and no conflict between safety and productivity (power production) goals. There are major consequences to real-world actions that 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 that limits the "external validity" (generalization) of the results.

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

In summary, the HFE PRM was developed to provide a means to

- review a conceptual design
- review products of the process that are important to V&V
- review and identify HFE issues that arise throughout the design process including early decisions
- address potential safety issues earlier in the design process and thus more effectively than if hardware design or the V&V stages of the design are complete, which makes the design more difficult to change

## 1.4 HFE PRM Development

The purpose of this section is to describe the development of the HFE PRM in terms of its objectives, technical scope, development methodology, and application.

### 1.4.1 Objectives

Since advanced reactor certification will be based partially on the approval of a design and implementation process plan, the staff must (1) assess whether all the appropriate HFE elements are included, (2) identify what materials are to be reviewed for each element, and (3) evaluate the proposed design acceptance criteria (DAC) and inspections, tests, analyses, and acceptance criteria (ITAAC) to

verify each of the elements. It is important to identify which aspects of the process are required to ensure that HFE design goals in support of safe plant operation are achieved and to identify the review criteria by which each element can be assessed. Review criteria independent of those provided by the designer are required to ensure that the design plan reflects acceptable human factors engineering practices at the time of the review and that it is a thorough, complete, and workable plan. The HFE PRM was developed to address this need. The specific objectives of the HFE PRM development effort were the following:

- (1) To develop a *technical basis* for the review of an applicant's HFE design process and final design implementation. The HFE PRM should be (a) based on currently accepted HFE practices, (b) well-defined, and (c) based on an approach that has been "validated" through its application to the development of complex, high-reliability systems.
- (2) To identify the HFE *elements* in a plant/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 the *components* of each HFE element that are key to a safety evaluation.
- (4) To specify the *review criteria* by which HFE elements can be evaluated.

### 1.4.2 Technical Scope

The scope of the general HFE PRM includes HSI design (including human interfaces with hardware and software), procedures, training, staffing, and the HFE aspects of human reliability analysis.

### 1.4.3 Development Methodology

A technical review of current HFE guidance and practices was conducted to identify important human factors program plan elements relevant to the technical basis of a design process review. Several types of documents were assessed:

- systems theory and engineering—general literature providing the theoretical basis for systems engineering (e.g., Gagne and Melton, 1988)
- NPP regulation—the regulatory basis for NPP review and NRC literature (e.g., 10 CFR Part 50, 10 CFR Part 52, NUREG-0800, and NUREG-0700, Appendix B)
- general HFE guidance—HFE guidance developed to be generally applicable to the design and evaluation of complex systems [e.g., Department of Defense Military Handbook (MIL-H) 46855B]

- NPP HFE guidance—standards, guidance, and recommended practices developed in the NPP industry [e.g., Institute of Electrical and Electronics Engineers (IEEE) Std. 1023-1988, International Electrotechnical Commission (IEC) 964, and Electric Power Research Institute *Advanced Light Water Reactor Utility Requirements Document*]

From this review an HSI development, design, and evaluation process was defined. Once specified, key HFE elements were identified and general criteria by which they are assessed (on the basis of a review of current literature and accepted practices in the field of human factors engineering) were developed. The HFE PRM was developed largely on the basis of applied general systems theory (Bailey, 1982; DeGreen, 1970; Gagne and Melton, 1988; Van Cott and Kinkade, 1972; Woodson, 1981) and the Department of Defense (DOD) system development process, which is rooted in systems theory (DOD, 1979b; DOD, 1990c; Kockler et al., 1990). Other DOD military standards, guidance documents, and handbooks were utilized as well (DOD, 1979a; DOD, 1981; DOD, 1983; DOD, 1985; DOD, 1989a; DOD, 1989b; DOD, 1991a; DOD, 1991b; DOD, 1991c; DOD, 1993).

Applied general systems theory provides a broad approach to system design that is based on a series of clearly defined developmental steps, each with defined goals and with specific management processes to attain them. Systems 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" (Kockler et al., 1990). DOD design requirements reflect the systems approach. Personnel are identified as a specific component of the total system (DOD, 1990b), and all system components (hardware, software, personnel, support, procedures, and training) are given detailed consideration in the design process. Since the military has been applying HFE longer than industrial and commercial system developers, the process is more formalized and contains detailed design process requirements. Thus, the DOD system development process was used as a major input to the development of the HFE PRM because of several factors.

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 ensures

- balanced influence of all required design specialties

- resolution of interface problems
- effective conduct of tradeoff analyses
- effective conduct of design reviews
- verification and validation of overall system performance

The effective integration of HFE considerations into the design is accomplished by providing (1) a structured top-down approach to system development that is iterative, integrative, interdisciplinary, and requirements driven and (2) a management structure that details the HFE considerations in each step of the overall process. A structured top-down approach to NPP HFE is consistent with the approach to new CR design described in Appendix B of NUREG-0700 (NRC, 1981) and the more recent nuclear industry standards (IEC 964; IEEE Std. 1023-1988) for advanced CR design. 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 (e.g., see Beattie and Malcolm, 1991; Stubler, Roth, and Mumaw, 1991).

The systems engineering approach was expanded to develop an HFE PRM to be used for the ACR design and implementation process review by the incorporation of NRC HFE requirements.

#### 1.4.4 General HFE PRM Description

As indicated above, a central foundation of the HFE PRM is that the HSI should be developed, designed, and evaluated on the basis of a structured top-down system analysis using accepted HFE principles based on current HFE practices. The HFE PRM decomposes the review process into ten elements reflecting four stages of design: planning, analysis, interface design, and evaluation (V&V). The PRM is illustrated in Figure 1.1. A brief description of the review objectives, acceptance criteria, and applicant products reviewed for each element follows. The HFE PRM is described in more detail in Sections 2 through 11.

Each element of the HFE PRM is divided into four sections: Background, Objective, Applicant Submittals, and Review Criteria.

- (1) *Background*—A brief explanation of the rationale and purpose is provided for each element.
- (2) *Objective*—The review objective(s) of the element is defined.

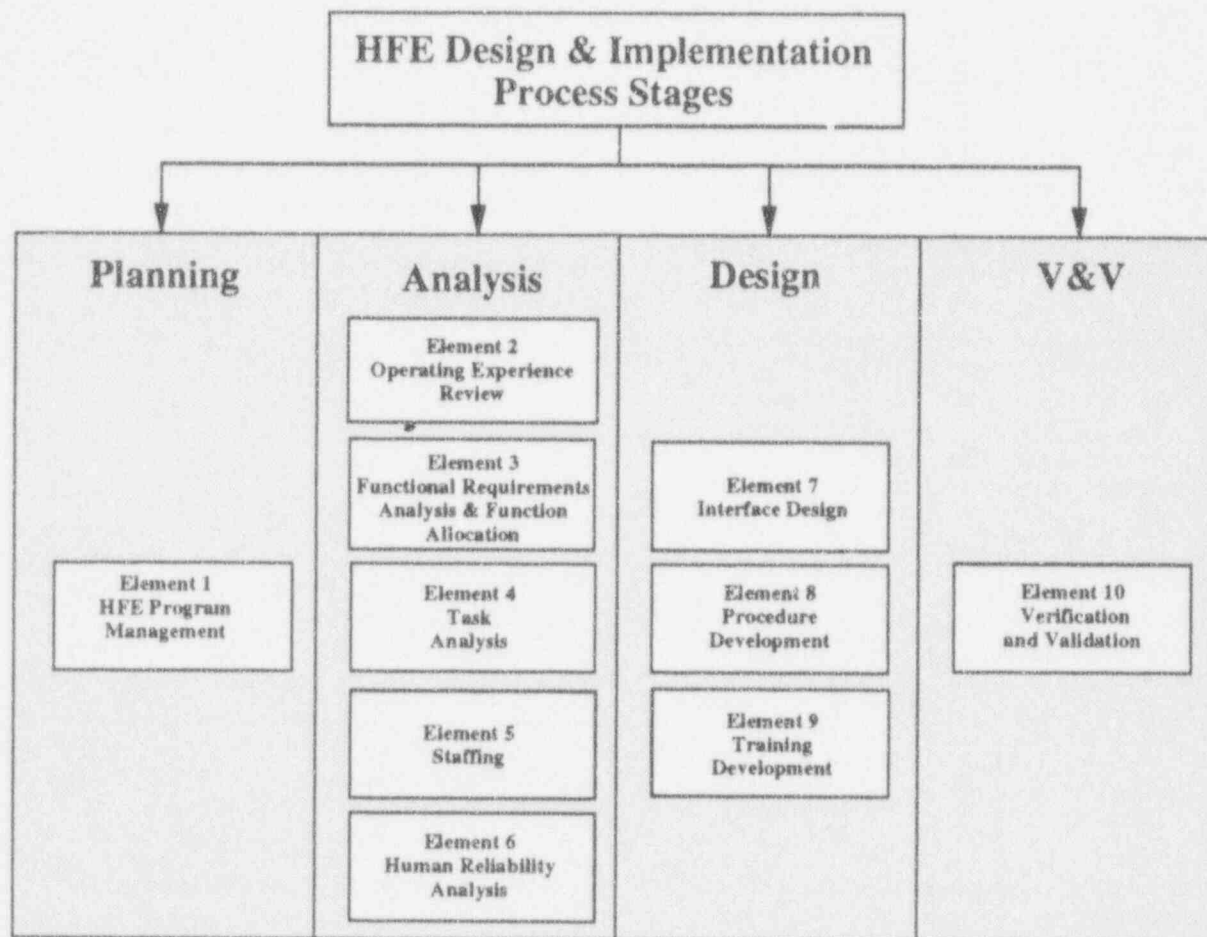


Figure 1.1 Human Factors Engineering Program Review Model

(3) *Applicant Submittals*—Materials to be provided for NRC review are listed. Generally three reports are identified: implementation plan, analysis results report, and design team review report.

- An implementation plan gives the applicant's proposed methodology for meeting the acceptance criteria of the element. An implementation plan review gives the applicant the opportunity to obtain staff review of and concurrence in the applicant's approach before conducting the activities associated with the element. Such a review is desirable from the staff's perspective because it provides the

opportunity to resolve methodological issues and provide input early in the analysis or design process when staff concerns can more easily be addressed than when the effort is completed.

- An analysis results report gives the results of the applicant's efforts on an HFE PRM element with respect to the review criteria. A reviewer will utilize the report as the main source of information for assessing the review criteria. If an implementation plan had been reviewed and found acceptable, the review of the results should be a verification that the plan had been satisfactorily followed.



- An applicant's design team review report provides the independent evaluation of the activities addressed for the element by the design team.

It is not intended that the submittals necessarily be in three reports. Rather it is important that all three types of information be available to the reviewer, that is, methodology, results, and review. In some cases an applicant may choose to provide this information in a single report. It is also possible that, for more complex elements such as HSI design or V&V, more than three reports may be submitted in order to address all HFE PRM criteria.

In addition to reports, the reviewer may review sample work products for earlier elements and implemented designs for later elements such as V&V.

- (4) *Review Criteria*—This section contains the acceptance criteria for design process products and for the final design review. Not all existing NRC detailed final design criteria are duplicated in this document. For example, NUREG-0700 contains HFE guidance for detailed control room design reviews. NUREG-0700 is only referenced in the applicable HFE PRM elements. Thus, the HFE PRM provides a combination of detailed criteria in areas historically not addressed by the staff reviews and "pointers" to the appropriate NRC documents in those areas for which existing NRC guidance is available. Thus, the HFE PRM provides a framework for organizing both new and traditional topics of staff HFE reviews.


The HFE PRM states that the applicant should develop each element using accepted HFE practices as specified by applicable regulatory documents and HFE codes, standards, and guidelines. Each of the HFE PRM elements provides a list of such documents that may be used. Although these documents contain generally recognized acceptable approaches for the conduct of the HFE activity described by the element, there are some qualifiers:

- Each individual document listed for a given element does not necessarily address all aspects of that element. In the conduct of a review of each element, a combination of the applicable sections of several of the identified documents may be appropriate.
- A specific document may not be applicable to a specific design review; for example, NUREG-0700 may not be applicable to a digital, video display unit (VDU)-based control room.
- There may be inconsistencies or contradictions within and between documents. Such conflicts may be resolved on a case-by-case basis.
- It should not be inferred that the listed documents provide complete guidance for each and every activity encompassed by the element. HFE is still an evolving discipline; therefore, not all HFE activities are adequately covered in codes, standards, and guidelines.
- Alternative approaches to those described in the referenced documents may be acceptable if judged by the reviewer to have a firm rationale. Proposed alternative approaches should be evaluated on a case-by-case basis.

#### 1.4.5 HFE PRM Applications and Interpretation

The HFE PRM was developed specifically to address the programmatic review of HSIs for advanced reactor designs. The HFE PRM is specified in a somewhat generic form and must, therefore, be tailored to the requirements of each specific review. For example, since the elements are iterative and overlapping, the technical criterion for a given element may be deferred to another element if the applicant provides an acceptable justification. Thus, because of the unique demands of each review, tailored versions of the model may be developed to support the staff reviews of individual applicant's HFE programs.

For a 10 CFR Part 52 review, the HFE PRM does not define which elements must be completed for design certification and which may be deferred to later. It is the responsibility of the applicant for design certification to indicate which aspects of each element are completed and to be reviewed under design certification evaluations. Those HFE PRM criteria not completed should be specifically addressed in ITAAC/DAC or COL action items. All HFE PRM criteria should be met before plant startup.



## HFE Management

## **Element 1**

# **HFE Program Management**

## 2 ELEMENT 1 - HFE PROGRAM MANAGEMENT

### 2.1 Background

The overall purpose of the HFE program review is to ensure that:

- The applicant has integrated HFE into plant development, design, and evaluation.
- The applicant has provided HFE products (e.g., HSIs, procedures, and training) that make possible safe, efficient, and reliable performance of operation, maintenance, test, inspection, and surveillance tasks.
- The HFE program and its products 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)] and satisfies all specific regulatory requirements as stated in 10 CFR.

State-of-the-art human factors principles are defined as those principles currently accepted by human factors practitioners. "Current" is defined with reference to the time when a program management or implementation plan is prepared. "Accepted" is defined as a practice, method, or guide that is (1) documented in the human factors literature within a standard or guidance document that has undergone a peer-review process or (2) can be justified through scientific research and/or industry practices.

To accomplish these programmatic objectives, an adequate HFE program plan is required which is implemented by a qualified HFE design team. The term "HFE design team" is generically used within the HFE PRM to refer to the primary organization or function within the organization that is responsible for HFE within the scope of the HFE PRM. There is, however, no assumption that HFE is the responsibility of a single organization or that there is an organizational unit called the HFE design team.

### 2.2 Objective

The objective of this review is to ensure that the applicant has an HFE design team with the responsibility, authority, placement within the organization, and composition to ensure that the design commitment to HFE is achieved. Also, the team should be guided by an HFE program plan to ensure the proper development, execution, oversight, and documentation of the HFE program. This plan should describe the technical program elements ensuring that all aspects of HSI are developed, designed, and evaluated on the basis of a structured top-down systems analysis using accepted HFE principles.

### 2.3 Applicant Submittals

The applicant should provide the following for staff review: HFE program plan describing the applicant's HFE goals/objectives, technical program to accomplish the objectives, HFE design team, and the management and organizational structure to allow the technical program to be accomplished.

The reviewer may also audit the issue tracking system against Section 2.4.4 below.

### 2.4 Review Criteria

Element 1 review topics include

- general HFE program goals and scope
- HFE team and organization
- HFE process and procedures
- HFE issues tracking
- technical program

#### 2.4.1 General HFE Program Goals and Scope

- (1) *HFE Program Goals*—The general objectives of the program should be stated in "human-centered" terms, which, as the HFE program develops, should be defined and used as a basis for HFE test and evaluation activities. Generic "human-centered" HFE design goals include the following:

- Personnel tasks can be accomplished within time and performance criteria.
- The HSI will support a high degree of operating crew "situation awareness."
- The plant design and allocation of functions will provide acceptable workload levels to ensure a balance between vigilance and operator overload.
- The operator interfaces will minimize operator error and will provide for error detection and recovery capability.

- (2) *Assumptions and Constraints*—The design assumptions (or constraints) should be clearly identified. An assumption or constraint is an aspect of the design, such as a specific staffing plan or the use of specific HSI technology, that is an input to the HFE program rather than the result of HFE analyses and evaluations.

- (3) *Applicable Facilities*—The HFE program should address the main control room, remote shutdown facility, technical support center (TSC), emergency operations facility (EOF), and local control stations (LCSs).
- (4) *Applicable HSIs*—The applicable HSIs included in the HFE program should include all operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures).
- (5) *Applicable Plant Personnel*—Plant personnel who should be addressed by the HFE program include licensed control room operators as defined in 10 CFR Part 55 and the following categories of personnel defined by 10 CFR 50.120: nonlicensed operators, shift supervisor, shift technical advisor, instrument and control technician, electrical maintenance personnel, mechanical maintenance personnel, radiological protection technician, chemistry technician, and engineering support personnel. In addition, any other plant personnel who perform tasks that are directly related to plant safety should be addressed.
- (6) *Technical Basis*—The following documents may be used as guidance (per Section 1.4.4):

*U.S. Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy."

*U.S. Code of Federal Regulations*, Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," Title 10, "Energy."

*U.S. Code of Federal Regulations*, Part 55, "Operator's Licenses," Title 10, "Energy."

IEEE Std. 1023-1988: *IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations*, 1988 (Institute of Electrical and Electronics Engineers).

MIL-H-46855B: *Human Engineering Requirements for Military Systems, Equipment and Facilities*, 1979 (Department of Defense).

AR 602-1: *Human Factors Engineering Program*, 1983 (Department of Defense).

DI-HFAC-80740: *Human Engineering Program Plan*, 1989 (Department of Defense).

AR 602-2: *Manpower and Personnel Integration (MANPRINT) in the Materiel Acquisition Process*, 1990 (Department of Defense).

DOD-HDBK-763: *Human Engineering Procedures Guide*, 1991 (Department of Defense).

## 2.4.2 HFE Team and Organization

- (1) *Responsibility*—The team should be responsible (with respect to the scope of the HFE program) for (a) the development of all HFE plans and procedures; (b) the oversight and review of all HFE design, development, test, and evaluation activities; (c) the initiation, recommendation, and provision of solutions through designated channels for problems identified in the implementation of the HFE activities; (d) verification of implementation of team recommendations; (e) assurance that all HFE activities comply with the HFE plans and procedures; and (f) scheduling of activities and milestones.
- (2) *Organizational Placement and Authority*—The primary HFE organization(s) or function(s) within the organization of the total program should be identified, described, and illustrated (e.g., charts to show organizational and functional relationships, reporting relationships, and lines of communication). When more than one organization is responsible for HFE, the lead organizational unit responsible for the HFE program plan should be identified. The team should have the authority and organizational placement to ensure that all its areas of responsibility are accomplished and to identify problems in the implementation of the HSI design. The team should have the authority to control further processing, delivery, installation, or use of HFE/HSI products until the disposition of a nonconformance, deficiency, or unsatisfactory condition has been achieved.
- (3) *Composition*—The HFE design team should include the expertise described in Appendix A.
- (4) *Team Staffing*—Team staffing should be described in terms of job descriptions and assignments of team personnel.

## 2.4.3 HFE Process and Procedures

- (1) *General Process Procedures*—The process through which the team will execute its responsibilities should be identified. The process should include procedures for
  - assigning HFE activities to individual team members
  - governing the internal management of the team
  - making management decisions regarding HFE
  - making HFE design decisions

- governing equipment design changes
  - design team review of HFE products
- (2) *Process Management Tools*—Tools and techniques (e.g., review forms) to be utilized by the team to ensure they fulfill their responsibilities should be identified.
  - (3) *Integration of HFE and Other Plant Design Activities*—The integration of design activities should be identified, that is, the inputs from other plant design activities to the HFE program and the outputs from the HFE program to other plant design activities. The iterative nature of the HFE design process should be addressed.
  - (4) *HFE Program Milestones*—HFE milestones should be identified so that evaluations of the effectiveness of the HFE effort can be made at critical check points and show the relationship to the integrated plant sequence of events. A relative program schedule of HFE tasks showing relationships between HFE elements and activities, products, and reviews should be available for review.
  - (5) *HFE Documentation*—HFE documentation items should be identified and briefly described along with the procedures for retention and access.
  - (6) *HFE in Subcontractor Efforts*—HFE requirements should be included in each subcontract and the subcontractor's compliance with HFE requirements should be periodically verified.

#### 2.4.4 HFE Issues Tracking

- (1) *Availability*—A tracking system should be available to address human factors issues that are (a) known to the industry (defined in the operating experience review, see Element 2) and (b) identified throughout the life cycle of the HFE/HSI design, development, and evaluation. Issues are those items that need to be addressed at some later date and thus need to be tracked to ensure that they are not overlooked. An existing tracking system may be adapted to serve this purpose.

- (2) *Method*—The method should document and track HFE issues from identification until elimination or reduction to an acceptable level.
- (3) *Documentation*—Each issue or concern that meets or exceeds the threshold established by the design team should be entered into the system when first identified, and each action taken to eliminate or reduce the issue or concern should be thoroughly documented. The final resolution of the issue should be documented in detail, along with information regarding design team acceptance.
- (4) *Responsibility*—When an issue is identified, the tracking procedures should spell out individual responsibilities for issue logging, tracking and resolution, and resolution acceptance.

#### 2.4.5 Technical Program

- (1) The general development of implementation plans, analyses, and evaluation of the following should be identified and described:
  - operating experience review
  - task analysis
  - staffing
  - human reliability analysis
  - HSI design
  - procedure development
  - training development
  - human factors verification and validation
- (2) The HFE requirements imposed on the design process should be identified and described. The standards and specifications that are sources of HFE requirements should be listed.
- (3) HFE facilities, equipment, tools, and techniques (such as laboratories, simulators, rapid prototyping software) to be utilized in the HFE program should be specified.



OER



## **Element 2**

### **Operating Experience Review**



### 3 ELEMENT 2 - OPERATING EXPERIENCE REVIEW

#### 3.1 Background

The accident at Three Mile Island (TMI) in 1979 and other reactor incidents have brought to light significant problems in the actual design and design philosophy of nuclear power plant (NPP) HSIs. Many recommendations have been made as a result of these accidents and incidents, and utilities have implemented both NRC-mandated changes and additional improvements on their own initiative. However, the design changes were based on the constraints associated with backfits to existing control rooms (CRs) using early 1980s technology, which limited the scope of corrective actions that might have been considered; that is, more effective fixes can be made when designing a new CR with the modern technology typical of advanced control rooms.

The main purpose of the operating experience review (OER) is to identify HFE-related safety issues. The OER provides information regarding the performance of fully integrated predecessor systems in a way analogous to full-mission validation tests, which provide information about the achievement of HFE design goals in support of

safe plant operation for the integrated system under review. The issues and lessons learned regarding operating experience provide a basis for improving the plant design in a timely way, that is, at the beginning of the design process.

The resolution of OER issues may involve function allocation, changes in automation, HSI equipment design, procedures, training, and so forth. Thus, problems and issues encountered in previous designs can 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.

Thus, OER information contributes to other HFE PRM elements. These inputs are summarized in Table 3.1. As indicated in the table, OER can contribute to review and evaluation considerations as well as system design considerations. For example, OER can be used in the selection of specific failure scenarios to incorporate in validation testing and can be used as a basis to select specific performance measures for the evaluation (e.g., to measure an aspect of human performance identified in OER as being problematic).

Table 3.1 The role of operating experience review in the HFE program

HFE TOPIC	CONTRIBUTION
HFE Program Management	<ul style="list-style-type: none"> <li>• HFE issue tracking system</li> </ul>
Functional Requirements Analysis and Function Allocation	<ul style="list-style-type: none"> <li>• Basis for initial requirements</li> <li>• Basis for initial allocations</li> <li>• Identification of need for modifications</li> </ul>
Task Analysis, Human Reliability Analysis, and Staffing	<ul style="list-style-type: none"> <li>• Critical human actions and errors</li> <li>• Problematic operations and tasks</li> <li>• Staffing shortfalls</li> </ul>
Human-System Interface, Procedures, and Training Development	<ul style="list-style-type: none"> <li>• Trade study evaluations</li> <li>• Potential design solutions</li> <li>• Potential design issues</li> </ul>
Verification and Validation	<ul style="list-style-type: none"> <li>• Tasks to be evaluated</li> <li>• Event and scenario selection</li> <li>• Performance measure selection</li> <li>• Issue resolution verification</li> </ul>

The technical basis for including an OER element in the HFE PRM is founded in nuclear industry regulations, standards, and recommended practices. As stated in 10 CFR 50.34 (f)(3)(i), the NRC requires that procedures be provided "for evaluating operating, design and construction experience and for ensuring that applicable impor-

tant industry experiences will be provided in a timely manner to those designing and constructing the plant." NUREG-0700 identifies OER as important to the evaluation of HSIs and includes an examination of available documents (such as licensee event reports (LERs), outage analysis reports, modifications to technical specifications,

documents (such as licensee event reports (LERs), outage analysis reports, modifications to technical specifications, and licensee internal memoranda and reports) and operator surveys and interviews. The International Atomic Energy Agency in the "Basic Safety Principles for Nuclear Power Plants" (IAEA, 1988) stated that "organizations concerned ensure that operating experience and the results of research relevant to safety are exchanged, reviewed and analyzed, and that lessons learned are acted on" (p. 22). OER has also been identified by the Institute of Electrical and Electronics Engineers (IEEE) as an element important to NPP design (IEEE Std. 1023-1988, see Section 6.3) and evaluation (IEEE Std. 845-1988, see Section 6.1.2).

The Electric Power Research Institute has required the formal integration of OER into the design of advanced NPPs in *Advanced Light Water Reactor Utility Requirements Document* (ALWR URD) in Requirement 3.1.3.1, "Resolution of Past Problems." Thus, OER is widely recognized as an activity important to safe and efficient plant design. It was, therefore, included in the HFE PRM as a formal element for review.

## 3.2 Objective

The objective of this review is to ensure that the applicant has identified and analyzed HFE-related problems and issues encountered in previous designs that are similar to the current design under review so that they are avoided in the development of the current design or, in the case of positive features, to ensure that they are retained.

## 3.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan, analysis results report, and HFE design team evaluation report. For a description of these submittals see Section 1.4.4.

The reviewer may also audit the issue tracking system for examination of OER issue treatment.

## 3.4 Review Criteria

### 3.4.1 Scope

- (1) *Predecessor Plant and Systems*—The review should include information pertaining to the human factors issues related to the predecessor plant(s) or highly similar plants and plant systems.
- (2) *Recognized Industry HFE Issues*—See Appendix B for a list of recognized nuclear power industry issues, organized into the following categories
  - unresolved safety issue/generic safety issue

- TMI issues
- NRC generic letters and information notices
- Office for Analysis and Evaluation of Operational Data studies
- low power and shutdown issues
- applicable operating plant event reports

(3) *Related HSI Technology*—The OER should address related HSI technology. For example, if touch screen interfaces are planned, HFE issues associated with their use should be reviewed.

(4) *Operator Interviews*—Operator interviews should be conducted to determine operating experience related to predecessor plants or systems. The following topics should be included in the operator interviews as a minimum:


- Plant Operations
  - normal plant evolutions (e.g., startup, full power, and shutdown)
  - instrument failures [e.g., safety-related system logic and control unit, fault tolerant controller (nuclear steam supply system), local "field unit" for multiplexer (MUX) system, MUX controller (balance of plant), break in MUX line]
  - HSI equipment and processing failure (e.g., loss of video display units, loss of data processing, loss of large overview display)
  - transients (e.g., turbine trip, loss of off-site power, station blackout, loss of all feedwater, loss of service water, loss of power to selected buses or CR power supplies, and safety/relief valve transients)
  - accidents (e.g., main steam line break, positive reactivity addition, control rod insertion at power, control rod ejection, anticipated transient without scram, and various-sized loss-of-coolant accidents)
  - reactor shutdown and cooldown using remote shutdown system
- HFE/HSI Design Topics
  - alarm and annunciation
  - display

- control and automation
- information processing and job aids
- real-time communications with plant personnel and other organizations
- procedures, training, staffing, and job design

### 3.4.2 Issue Analysis, Tracking, and Review

- (1) *Analysis Content*—The issues should be analyzed with regard to the identification of

- human performance issues, problems, and sources of human error
  - design elements that support and enhance human performance
- (2) *Documentation*—The analysis of operating experience should be documented in an evaluation report.
  - (3) *Incorporation Into the Tracking System*—Each operating experience issue determined to be appropriate for incorporation in the design (but not already addressed in the design) should be documented in the HFE tracking system.



## Function Analysis

## **Element 3**

# **Functional Requirements Analysis and Allocation**

## 4 ELEMENT 3 - FUNCTIONAL REQUIREMENTS ANALYSIS AND FUNCTION ALLOCATION

### 4.1 Background

This element consists of two distinct review activities: functional requirements analysis and function allocation. Functional requirements analysis is the identification of those functions that must be performed to satisfy plant safety objectives, that is, to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. It is conducted to (1) determine the objectives, performance requirements, and constraints of the design; (2) define the functions that must be accomplished to meet the objectives and required performance; (3) define the relationships between functions and plant processes (e.g., plant configurations or success paths) responsible for performing the function; (4) provide a framework for understanding the role of controllers (whether personnel or system) for controlling plant processes.

Function allocation is the analysis of the requirements for plant control and the assignment of control functions to (1) personnel (e.g., manual control), (2) system elements (e.g., automatic control and passive, self-controlling phenomena), and (3) combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup). Function allocation seeks to enhance overall plant safety and reliability by exploiting the strengths of personnel and system elements, including improvements that can be achieved through the assignment of control to these elements with overlapping and redundant responsibilities. Function allocation should be based on HFE principles using a structured and well-documented methodology that seeks to provide personnel with logical, coherent, and meaningful tasks. It should not be based solely on technology considerations that allocate to plant personnel everything the designers cannot automate. Such an approach results in an ad hoc set of activities that is likely to negatively affect operator performance.

NRC review of function allocation is important to ensuring plant safety. One of the major trends in advanced plant design is an increase in automation for those tasks traditionally performed by the operator. Increases in automation result in a shift of the operator's function from that of a direct manual controller to a supervisory controller and system monitor. This type of role change may be viewed as positive from a reliability standpoint, since the human operator is considered one of the more unpredictable components in the system. It is generally presumed that automation will enhance overall system reliability by removing or reducing the need for human action. However, problems arise when functions are automated

largely on the basis of the capability of available technology rather than consideration of the operator's performance as an integral component in the overall system. Bastl noted that "data from accident and significant event reports, together with a review of past and current design processes, reveal that plant designers often do not demonstrate the use of a systematic method for making the necessary series of critical decisions which allocate functions to men or machines, that is to establish the extent and role of automation" (Bastl et al., 1991).

Problems associated with human interaction with automated systems have been attributed to poor situation awareness (Kibble, 1988). Maintaining situation awareness is difficult when the operator is largely removed from the control loop; that is, the operator's role is shifted from a manual controller to a supervisor and monitor (Wickens and Kessel, 1981; Ephrath and Young, 1981). With respect to automation in civil aviation, Sexton observed that if "decisions are automatically made without providing the rationale to the pilot, the ability to stay ahead of the aircraft is lost. Complacency and inability to take timely and proper action result" (Sexton, 1988). Increases in automation have frequently been associated with loss of operator vigilance and situation awareness resulting in an increase in vigilance-associated human errors (Warm and Parasuraman, 1987). In addition, new types of human errors emerge related to the setup, monitoring, and interaction with the automated system (Wiener and Curry, 1980).

Automation has been associated with other effects on personnel performance, such as a shift from a highly physical to a highly cognitive workload (rather than the expected reduction in overall workload), workload transition difficulties (i.e., going from a low activity monitoring period to a highly active but more uncertain time at the beginning of a process disturbance), and the potential erosion of the skills to perform the task in the event of automated system failure. Since many advanced NPP designs still require the operator to assume control under certain circumstances and to act as the last line of defense, the consequences of poor integration of the operator in the plant design can be quite serious.

Passive systems rely on natural forces such as gravity instead of mechanical forces such as pumps to perform their functions. From the perspective of the role of plant personnel, passive systems can be considered a special form of automation because initiation and control of these functions often do not require personnel actions. As with other automatic systems, personnel may be responsible for monitoring the availability and operational status of the passive system. However, because of the passive nature of the phenomena being monitored, special burdens



may be placed on plant personnel. In addition, activation of a passive system may have important consequences to plant availability or productivity goals; thus, the role of personnel may include decisions and actions to prevent or delay the activation of the passive system. These decisions and actions should be addressed in the functional requirements analysis.

For many plant designs, the functional requirements and function allocations of a new design may be based largely on a predecessor design. Many functional requirements and function allocations of the new plant may be the same as those of the predecessor. This reflects the evolutionary nature of technology development especially when applied to complex, high-reliability systems. In such cases, operating experience review (OER) becomes an essential component of the technical basis and rationale for the functional requirements and function allocations. The HFE PRM review methodology accommodates the review of advanced plant designs that are closely linked to predecessor designs as well as advanced plant designs that are not as closely based on a predecessor design.

Figure 4.1 presents an overview of the functional requirements analysis and function allocation issues and activities. It shows that both the nature of the function and the way that it is allocated to personnel and system elements can be considered "modified" with respect to comparisons to predecessor plants.

## 4.2 Objective

The objective of this review is to ensure that the applicant has defined the plant's safety functional requirements and that the function allocations take advantage of human strengths and avoid allocating functions that would be negatively affected by human limitations.

## 4.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan, analysis results report, and HFE design team evaluation report. For a description of these submittals see Section 1.4.4.

## 4.4 Review Criteria

### 4.4.1 General Criteria

- (1) Functional requirements analysis and function allocation should be performed using a structured, documented process reflecting HFE principles.
- (2) The following documents may be used as guidance (per Section 1.4.4):

IAEA-TECDOC-668: *The Role of Automation and Humans in Nuclear Power Plants*, 1992 (Inter-

national Atomic Energy Agency – International Working Group on NPP Control and Instrumentation).

NUREG/CR-2623: *The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review*, 1982 (NRC – H. Price).

NUREG/CR-3331: *A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control*, 1983 (NRC – R. Pulliam et al.).

IEC 964: *Design for Control Rooms of Nuclear Power Plants*, 1989 [International Electrochemical Commission (Bureau Central de la Commission Electrotechnique Internationale)].

MIL-H-46855B: *Human Engineering Requirements for Military Systems, Equipment and Facilities*, 1979 (Department of Defense).

AD/A223 168: *Systems Engineering Management Guide*, 1990 (Department of Defense – Defense Systems Management College – F. Kockler et al.).

### 4.4.2 Functional Requirements Analysis

- (1) Safety functions (e.g., reactivity control) should be defined. These include functions required to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant processes (plant system configurations or success paths) that are responsible for or capable of carrying out the function should be clearly defined (box 1 of Figure 4.1).
- (2) Safety functions and processes of the new plant should be compared to those of the predecessor plant, if any, to document functions and processes that are (a) new, (b) changed, and (c) deleted. These should be referred to as the "modified" processes. Safety processes that have not been modified should be documented as unchanged (box 2 of Figure 4.1).
- (3) The technical basis for modified processes should be documented (e.g., rationale for a passive cooling system) (box 3 of Figure 4.1).
- (4) A summary description should be provided for each plant process (unchanged or modified) which includes
  - purpose of the process
  - conditions that indicate that the process is required

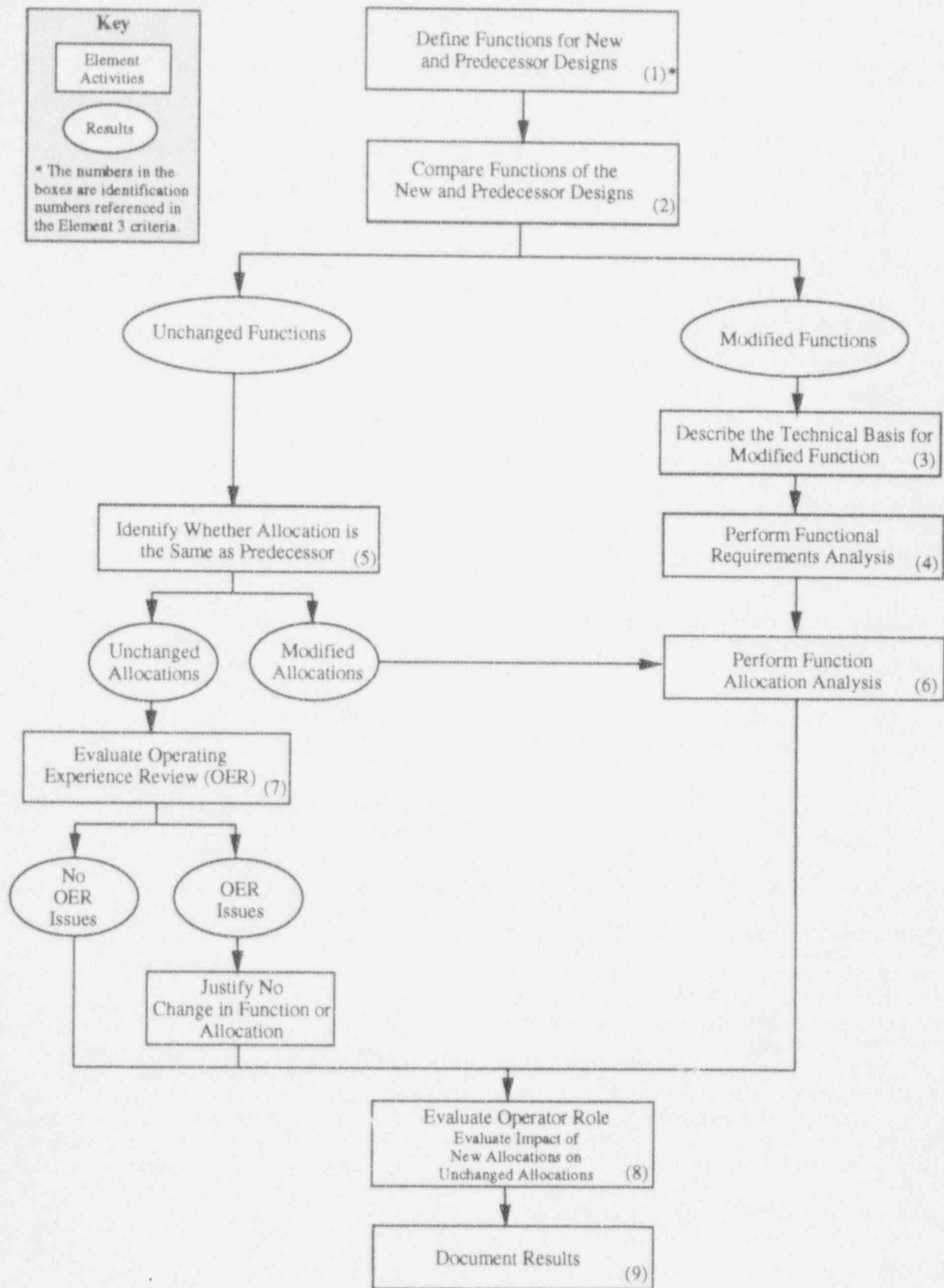


Figure 4.1. Functional Requirements Analysis and Function Allocation



- parameters that indicate that the process is available
- parameters that indicate the process is operating (e.g., flow indication)
- parameters that indicate the process is achieving its purpose (e.g., reactor vessel level returning to normal)
- parameters that indicate that operation of the process can or should be terminated

Note that parameters may be described qualitatively (e.g., high or low). Specific data values or setpoints are not necessary at this stage.

- (5) Safety functions should be described initially in graphic form (e.g., functional flow block diagram). Function diagramming should be done at several levels, starting at top-level functions where a very general picture of major functions is described, and continuing to the plant process level and to lower levels until a specific critical end-item requirement will emerge (e.g., a piece of equipment, software, or an operator). The functional decomposition should address the following levels (see Figure 4.1)
  - high-level functions [e.g., maintain reactor coolant system (RCS) integrity and critical safety functions (e.g., maintain RCS pressure control)]
  - individual plant processes
  - specific plant systems and components
- (6) Detailed narrative descriptions should be developed for each of the identified modified processes and for their relationship to the overall plant configuration design. Information provided in the summary description for criterion 4 above should be described in greater detail.
- (7) The functional requirements analysis should be kept current over the life cycle of design development and held until decommissioning so that it can be used for design when modifications are considered.
- (8) The following should be verified:
  - All the processes necessary for the achievement of safe operation are identified.
  - All requirements of each process are identified.

#### 4.4.3 Function Allocation Analysis


- (1) Processes that were identified as unchanged should be reviewed to determine (a) those for which the control function allocation between personnel and system elements is unchanged and (b) those for which the function allocation has changed (e.g., through the increased use of automation). This latter group should be described as having modified function allocations (box 5 of Figure 4.1). The level of automation should be briefly described (e.g., fully automatic, fully manual, automatic with manual backup) for each unchanged function with unchanged allocation.
- (2) Unchanged processes that have *modified* function allocations should be analyzed in terms of resulting human performance requirements based on the expected user population. A rationale for the resulting allocation should be provided. This analysis should reflect, as much as possible at this stage of design, (a) sensitivity, precision, time, and safety-related requirements; (b) required reliability; and (c) the number and level of skills of personnel required to operate and maintain the system (box 6 of Figure 4.1).
- (3) Modified processes (identified in Element 3) should also be analyzed in terms of resulting human performance requirements based on the expected user population. A rationale for the resulting allocation should be provided. This analysis should also reflect, as much as possible at this stage of design, (a) sensitivity, precision, time, and safety requirements; (b) required reliability; and (c) the number and level of skills of personnel required to operate and maintain the system (box 6 of Figure 4.1).
- (4) The allocation criteria, rationale, analyses, and rules used in the analysis of function allocation should be documented (box 6 of Figure 4.1).
- (5) The results of analyses and tradeoff studies should support the adequate configurations of personnel and system-performed control functions. Analyses should confirm that the personnel element can properly perform tasks allocated to them while maintaining operator situation awareness, workload, and vigilance. Proposed function assignment should take the maximum advantage of the capabilities of humans and machines without imposing unfavorable requirements on either (box 6 of Figure 4.1).
- (6) The OER should be used to address the case of modified processes. Problematic OER issues should be considered during the function allocation analyses for modified functions (box 6 of Figure 4.1).
- (7) The OER should be used to address the case of unchanged functions that have unchanged control

function allocations. If problematic OER issues are identified, then an analysis should be performed to (a) justify the original analysis of the function, (b) justify the original human-machine allocation, and (c) identify solutions such as training, personnel selection, and procedure design that will be implemented to address the OER issues (box 7 of Figure 4.1).

- (8) All function allocations should be reviewed to evaluate the effect of new control function allocations on

unchanged control function allocations (box 8 of Figure 4.1).

- (9) Control functions should be re-allocated in an iterative manner, in response to developing design specifics, operating experience, and the outcomes of ongoing analyses and trade studies.
- (10) The technical basis on which the control function allocation analysis was performed should be documented (box 9 of Figure 4.1).



## Task Analysis

**Element 4**  
**Task Analysis**

## 5 ELEMENT 4 - TASK ANALYSIS

### 5.1 Background

Task analysis is the evaluation of the performance demands on plant personnel to identify the task requirements for accomplishing the functions allocated to them (Drury et al., 1987). It is a very important activity because it defines the human-system interface (HSI) requirements for task accomplishment by supporting personnel (and by exclusion, what is not needed in the HSI). Personnel perform tasks to meet their functional responsibilities. Although there is no precise definition of a task with respect to the level of abstraction, a task is a group of related activities that have a common objective or goal. The results of task analysis are identified as inputs in many of HFE PRM elements. For example, task analysis also forms the basis for

- evaluating function allocations, that is, for examining the capability of plant personnel to accomplish tasks assigned to them
- providing a basis for staffing and job design
- providing detailed task requirements to support detailed procedure development
- identifying training requirements
- defining task support verification requirements for the HFE PRM Element 10 verification and validation review

### 5.2 Objective

The objective of this review is to ensure that the applicant's task analysis identifies the behavioral requirements of the tasks the personnel subsystem is required to perform. The task analysis should

- provide one of the bases for making design decisions, for example, determining before hardware fabrication, to the extent practicable, whether system performance requirements can be met by combinations of anticipated equipment, software, and personnel
- ensure that human performance requirements do not exceed human capabilities
- be used as basic input for developing procedures
- be used as basic information for developing staffing, training, and communication requirements of the plant

- form the basis for specifying the requirements for the displays, data processing, and controls needed to carry out tasks

### 5.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan, analysis results report, and HFE design team evaluation report. For a description of these submittals, see Section 1.4.4.

### 5.4 Review Criteria

- (1) The scope of the task analysis should include selected representative and important tasks from the areas of operations, maintenance, test, inspection, and surveillance. The analyses should be directed to the full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions. The analyses should include tasks performed in facilities applicable to the HFE program (as defined in Element 1).
- (2) Tasks should be linked using a technique such as operational sequence diagrams. A review of the descriptions and operational sequence diagrams should identify which tasks can be considered "critical" in terms of importance for function achievement, potential for human error, and impact of task failure. Human actions that are found to affect plant risk by means of probabilistic risk assessment (PRA) importance and sensitivity analyses should also be considered "critical." All critical tasks should have specific task analyses performed for them. To determine PRA/human reliability analysis (HRA) critical human actions, internal and external initiating events and actions affecting the PRA Level I and II analyses should be considered (see Element 6 for an explanation of PRA/HRA). Where critical functions are automated, the analyses should consider all human tasks including monitoring of the automated system and execution of backup actions if the system fails.
- (3) Task analyses should begin on a gross level and involve the development of detailed narrative descriptions of what personnel must do. They should define the nature of the input, process, and output required by and of personnel. Detailed task descriptions should address (as appropriate) the following:
  - Information Gathering
    - information required (parameters, units, precision, accuracy)

- information source (alarm, displays, verbal communication, etc.)
  - Decisionmaking Requirements
    - description of the decisions to be made (relative, absolute, probabilistic)
    - evaluations to be performed
    - decisions that are probable based on the evaluation (opportunities for cognitive errors, such as capture error, will be identified and carefully analyzed)
  - Response Requirements
    - action to be taken
    - overlap of task requirements (serial vs. parallel task elements)
    - frequency
    - time available for operator response based on plant response characteristics
    - temporal constraints (task ordering)
    - tolerance and accuracy
    - operational limits of personnel performance
    - operational limits of machine and software
    - body movements required by action taken
  - Feedback Requirements
    - feedback required to indicate adequacy of actions taken
  - Workload
    - cognitive
    - physical
    - estimation of difficulty level
  - Task Support Requirements
    - special and protective clothing
    - job aids or reference materials required
    - tools and equipment required
  - computer processing support aids
  - Workplace Factors
    - workspace envelope required by action taken
    - work environment (e.g., lighting, heat, noise, and radiation)
    - workspace location
  - Staffing and Communication Requirements
    - number of personnel, their technical specialty, and specific skills
    - communications required, including type
    - personnel interaction when more than one person is involved
  - Hazard Identification
    - identification of hazards involved
- (4) The task analysis should be iterative and become progressively more detailed over the design cycle. It should be detailed enough to identify information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls for human task accomplishment.
  - (5) The task analysis should incorporate job design issues such as the number of crew members crew member skills allocation of monitoring and control tasks to the (a) formation of a meaningful job and (b) management of crew member's physical and cognitive workload.
  - (6) The task analysis results should be used to define a minimum inventory of alarms, displays, and controls necessary to perform crew tasks based on both task and instrumentation and control requirements.
  - (7) The task analysis results should provide input to the HSI design, procedure development, and personnel training programs.
  - (8) The following documents may be used as guidance (per Section 1.4.4):
 

NUREG/CR-3371: *Task Analysis of Nuclear Power Plant Control Room Crews*, 1983 (NRC - D. Burgy et al.).

IEC 964: *Design for Control Rooms of Nuclear Power Plants*, 1989 [International Electrotechnical Commission (Bureau Central de la Commission Electrotechnique Internationale)].

DI-H-7055: *Critical Task Analysis Report*, 1979  
(Department of Defense).

MIL-STD-1478: *Task Performance Analysis*, 1991d  
(Department of Defense).



Staffing

## **Element 5**

### **Staffing**

## 6 ELEMENT 5 – STAFFING

### 6.1 Background

Plant staffing as identified in Element 1 (see Section 2.4.1, "General HFE Program Goals and Scope," Criterion 5, "Applicable Plant Personnel") is an important consideration throughout the design process. Initial staffing levels may be established as design goals early in the design process on the basis of experience with previous plants, customer requirements, initial analyses, and Government regulations. However, staffing goals and assumptions should be examined for acceptability as the design of the plant proceeds. Other elements of the HSI design process provide information with which staffing levels can be evaluated and modified, as appropriate.

### 6.2 Objective

The objective of this review is to ensure that the applicant has analyzed the requirements for the number and qualifications of personnel in a systematic manner that includes a thorough understanding of task requirements and applicable regulatory requirements.

### 6.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan, analysis results report, and HFE design team evaluation report. For a description of these submittals see Section 1.4.4.

### 6.4 Review Criteria

- (1) The staffing analysis should determine the number and background of personnel required during the full range of plant conditions and tasks including operational tasks (normal, abnormal, and emergency), plant maintenance, and plant surveillance and testing. The scope of personnel that should be considered is identified in Element 1 (see Section 2.4.1, Criterion 5).
- (2) Staffing levels should be based on an analysis of
  - initial HSI staffing goals and their bases including staffing levels of predecessor systems and a description of significant similarities and differences between predecessor and current systems
  - required actions determined from the task analysis
  - availability of operators considering other activities that may be ongoing and for which

operators may take on responsibilities outside the control room (e.g., fire brigade)

- the physical configuration of the control room and control consoles
  - the availability of plant information from individual operator workstations from individual and group view HSI interfaces
  - required interaction between operators for diagnosis, planning, and control activities
  - required interaction between personnel for administrative, communications, and reporting activities
  - actions required by 10 CFR 50.47 (and NUREG-0654) to meet an initial accident response in key functional areas as required by the emergency plan)
  - staffing requirements described in NUREG-0800, Section 13.1.2-13.1.3, "Operating Organization," and 10 CFR 50.54
- (3) The staffing analysis should be iterative; that is, initial staffing goals should be reviewed and modified as the analyses associated with other HFE PRM elements are completed.
  - (4) The staffing analysis should consider the issues associated with the following HFE PRM elements and then compare these issues to staffing assumptions regarding the number and qualifications of operations personnel. The basis for staffing should be modified to address these issues:
    - Operating Experience Review
      - operational problems and strengths that resulted from staffing levels in predecessor systems
    - Function Analysis and Allocation
      - mismatches between functions allocated to the operator and the qualifications of anticipated operators
    - Task Analysis
      - the knowledge, skills, and abilities required for operator tasks addressed by the task analysis
      - requirements for operator response time and workload

- requirements for operator communication and coordination
  - the job requirements that result from the sum of all tasks allocated to each individual operator both inside and outside the control room
  - Human Reliability Assessment
    - the effect of overall staffing levels on plant safety and reliability
    - the effect of overall staffing levels and the coordination of individual operator roles on critical human actions
    - the effect of overall staffing levels and the coordination of individual operator roles on human errors associated with the use of advanced technology
  - HSI Design
    - staffing demands resulting from the locations and use (especially concurrent use) of controls and displays
    - the requirements for coordinated actions between individual operators
  - Procedures
    - staffing demands resulting from requirements for concurrent use of multiple procedures
    - skills, knowledge, abilities, and authority required of operators by the procedures
  - Training
    - crew coordination concerns that are identified during the development of training
  - Verification and Validation
    - ability of minimum size operating crew to control plant during validation scenarios
    - ability of operators to effectively communicate and coordinate actions during all validation scenarios
    - ability of operators to maintain awareness of plant conditions and operator actions throughout all validation scenarios
- (5) The following documents may be used as guidance (per Section 1.4.4):
- 10 CFR 50.54: *U.S. Code of Federal Regulations, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy."*
- 10 CFR 50.47: *U.S. Code of Federal Regulations, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy."*
- NUREG-0800: *Standard Review Plan, Rev. 1, Sections 13.1.2-13.1.3, 1984 (NRC).*
- NUREG-0654: *Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, 1980 (NRC).*
- Regulatory Guide 1.114: *Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit, May 1989 (NRC).*
- ANSI/ANS 3.1-1981: *Selection, Qualification, and Training of Personnel for Nuclear Power Plants, 1981 (American Nuclear Society).*

## Human Reliability

## **Element 6**

# **Human Reliability Analysis**



## 7 ELEMENT 6 – HUMAN RELIABILITY ANALYSIS

### 7.1 Background

Human reliability analysis (HRA) seeks to evaluate the potential for and mechanisms of human error that may affect plant safety. Thus, it is an essential element in the achievement of the HFE design goal of providing operator interfaces that will minimize operator error and will provide for error detection and recovery capability. HRA has quantitative and qualitative aspects, both of which are useful for HFE purposes. HRA should be conducted as an integrated activity in support of both HFE/HSI design activities and probabilistic risk assessment (PRA) activities. The PRA/HRA should be initially performed early in the design process to provide design insights and guidance both for systems design and for HFE purposes. The quality of the HRA depends in large part on the analyst's understanding of personnel tasks, the information related to those tasks, and the factors that influence human performance of those tasks. As a result, the HRA could be performed iteratively as the design progresses. At the very least, the initial PRA/HRA should be finalized when the plant design and HFE are complete. Figure 7.1 illustrates the relationship between the PRA/HRA and the rest of the HFE program, including the concept of an initial PRA/HRA and then a final one at completion of design. The discussions in the remainder of this HRA element will have to be judgmentally applied in appropriate portions to the earliest PRA/HRA (depending on the amount of design information that is available) and applied in full to the final PRA/HRA.

The development of information to facilitate the understanding of causes and modes of human error is an important human factors activity. The HRAs should make use of descriptions and analyses of operator functions and tasks as well as the operational characteristics of HSI components. HRA can provide valuable insight into desirable characteristics of the HSI design. Consequently, the HFE/HSI design effort should give special attention to those plant scenarios, critical human actions, and HSI components that have been identified by PRA/HRA as being critical to plant safety and reliability.

Although there are many different approaches to the conduct of HRA, there are several analysis components that are necessary for an acceptable HRA. These include

- multidisciplinary team to analyze human actions within the context of the PRA
- availability of information related to those factors that affect human performance, such as accident analyses (indicating time available for

action), task analyses, procedures, and HSI design details

- detailed analyses of human actions with an emphasis on human error mechanisms
- availability of appropriate sources of human error data for the types of human actions that are modeled
- sensitivity and uncertainty analyses to evaluate human error probability estimates
- integration of PRA and HRA activities into plant design activities
- thorough documentation of the HRA process

Thus, there are important interfaces between the HFE program and risk analyses. The objective and criteria associated with this element are intended to ensure the acceptability of this activity.

### 7.2 Objective

The objectives of this review are to ensure the following:

- The applicant has analyzed the potential effects of human error on plant safety and reliability in a manner that is consistent with current, accepted principles and practices of HFE and HRA/PRA and has identified human actions that are important to plant risk.
- The applicant has addressed human error mechanisms in the design of the plant HFE, that is, the HSIs, procedures, shift staffing, and training, in order to minimize the likelihood of personnel error and to provide for error detection and recovery capability.
- The HRA activity effectively integrates the HFE program activities and PRA/risk analysis activities.

### 7.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan and HFE design team evaluation report. For a description of these submittals see Section 1.4.4.

The reviewers should also review a PRA/HRA report and an analysis results report that documents the integration of the HRA with the HFE design as described in this element.

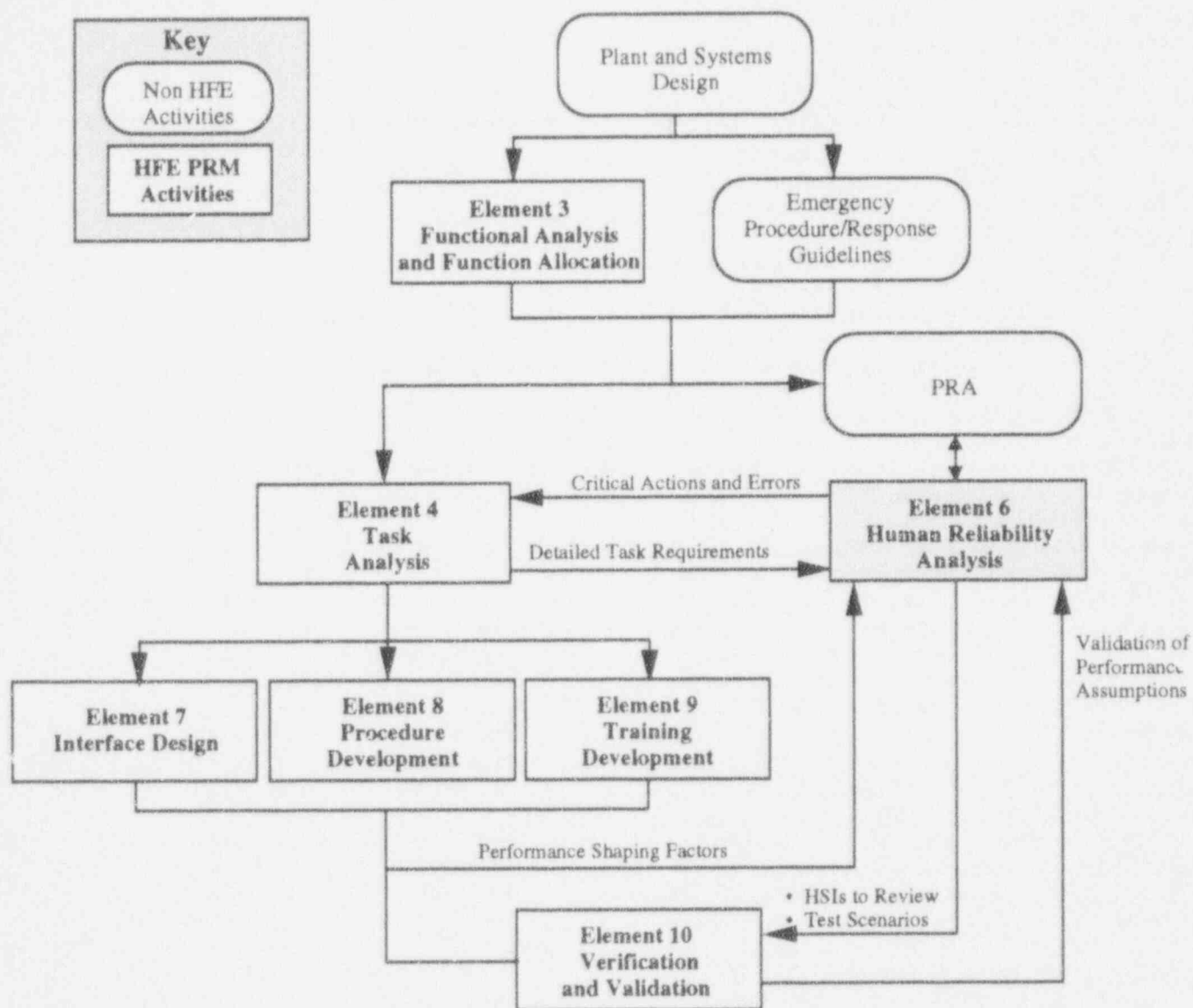


Figure 7.1. The Role of Human Reliability Analysis in the HFE Program

## 7.4 Review Criteria

### 7.4.1 Human Reliability Analysis Methodology

- (1) The analysis should meet all applicable 10 CFR regulatory requirements [e.g. 10 CFR 50.34(f)(1)(i)].
- (2) In addition to the HFE design team skills identified in Element 1, additional skills should be included to support the HRA
  - HRA methods and human error probability (HEP) quantification techniques
  - plant and system PRA models
- (3) The HRA should follow a structured, systematic process to ensure that human reliability issues are addressed consistently and to facilitate reporting and review of results. The HRA process should address the following topic areas: select and train the team, familiarize the team with plant, build initial plant model, screen human interactions, quantify human interactions, update plant model, and review results.
- (4) A thorough HRA documentation system should be established, including a description of the analyses, an audit trail for each analysis performed and each HEP derived, supporting rationale, and source materials. The documentation system should be structured to reflect the structure of the HRA process so that the outcomes of the various steps of the process are identified.
- (5) HRA should minimally be performed early in the design effort as an input to the HFE program and again when the detailed design is available to better assess the influences of detailed task requirements and performance shaping factors (PSFs).
- (6) Human actions should be adequately modeled in the PRA event and fault trees to support a determination of risk-significant human actions. The PRA/HRA should address a broad diversity of human interactions with the plant systems and components, for example,
  - actions before and during accident
  - errors of omission and commission
  - miscalibration and component restoration errors
  - recovery actions

Events and HSI components identified as problematic by the operating experience review (OER) and operator functions that were identified as new or modified by the function allocation analysis should be considered for inclusion in the HRA.
- (7) The analysis of human actions should include the identification of PSFs, that is, factors that influence human reliability through their effects on performance. PSFs include factors such as environmental conditions, HSI design, procedures, training, and supervision. The considerations should include the influences of the advanced technologies such as system automation, decision aids, and artificial intelligence on human performance.
- (8) Screening analyses should be used to identify human actions that are important to plant risk and plant safety for more detailed analyses.
- (9) Human-system analyses and evaluations should be used to provide an understanding of task requirements including (a) demands placed on plant personnel, (b) interfaces with plant equipment, and (c) time constraints within which critical tasks must be accomplished. Within the constraints associated with the timing of the HRA (i.e., early or late in the design process), information source materials used for defining and analyzing operator tasks should at a minimum include (a) descriptions and analyses of operator tasks developed during the task analysis (Element 4), (b) emergency procedure guidelines and plant procedures (Element 8), and (c) descriptions and analyses of HSI design characteristics (Element 7). Materials such as procedural guidance and control room design information should be used by the HRA team to provide an understanding of human involvement in controlling the plant.
- (10) Human error quantification, including quantification methods [such as the technique for human error rate prediction (THERP), Swain and Guttman, 1983], performance models (such as action dependency), human error data sources (such as the "Nuclear Computerized Library for Assessing Reactor Reliability" (NUCLARR), Gertman et al., 1990), and PSFs should be specifically identified and selected on the basis of their appropriateness to the types of actions being analyzed. When data from PRAs, performed for other plants, are to be used in the HRA, a rationale should be provided to justify its use including any modifications of these data.
- (11) Because of the inherent uncertainty of numerical estimation, sensitivity and uncertainty analyses should be performed.
- (12) The following documents may be used as guidance (per Section 1.4.4):

10 CFR 50.34(f)(1)(i): *U.S. Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy."

NUREG/CR-2300: *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, 1983 (NRC).

NUREG/CR-2815: *Probabilistic Safety Analysis Procedures Guide*, 1985 (NRC - Bari).

NUREG/CR-3485: *PRA Review Manual*, 1985 (NRC - El-Bassioni et al.).

NUREG/CR-4772: *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, February 1987 (NRC).

P1082/D8-1990: *A Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations*, 1990 (Institute of Electrical and Electronics Engineers).

EPRI NP-3583: *Systematic Human Action Reliability Procedure (SHARP)*, 1984, (Electric Power Research Institute - Hannaman and Spurgin).

#### 7.4.2 Integration of Human Reliability Analysis With HFE Design

- (1) Critical human actions should be identified from the PRA/HRA and used as input to the HFE design effort. These critical actions should be developed from the Level 1 (core damage) PRA and Level 2 (release from containment) PRA including both internal and external events. They should be developed using selected (more than one) importance measures and

HRA sensitivity analyses to ensure that an important action is not overlooked because of the selection of the measure or the use of a particular assumption in the analysis.

- (2) The details of human performance of critical human actions and their associated tasks and scenarios identified through the initial PRA/HRA should be specifically addressed during Element 4, Task Analysis. This will help ensure that these tasks are within acceptable human performance capabilities (e.g. within time and workload requirements).
- (3) Critical human actions that are identified by means of PRA/HRA as posing serious challenges to plant safety and reliability should be *re-examined* by function allocation analysis, task analysis, HSI design, or procedure development to change either the operator task or the control and display environment to reduce or eliminate undesirable sources of error.
- (4) The use of PRA/HRA results by the HFE design team should be specifically addressed; that is, how are critical personnel tasks addressed (through HSI design, procedural development, and training) under the HFE program to minimize the likelihood of operator error and provide for error detection and recovery capability.
- (5) HRA assumptions such as decisionmaking and diagnosis strategies for dominant sequences should be validated by walkthrough analyses with personnel with operational experience using a plant-specific control room mockup, prototype, or simulator. Reviews should be conducted before the final quantification stage of the PRA (as per item 5 of Section 7.4.1 above).



**HSI Design**

## **Element 7**

# **Human-System Interface Design**



## 8 ELEMENT 7 - HUMAN-SYSTEM INTERFACE DESIGN

### 8.1 Background

The human-system interface (HSI) design process represents the translation of function and task requirements into a detailed HSI product, that is, the alarms, displays, controls, and task support aids that comprise the HSI. The selection of available HSIs and the design of new HSIs should be the result of a process that considers function and task requirements, operational considerations (e.g., the full-mission context within which the HSI will be used), and the crew's personal safety and comfort. The HSI should be designed using a structured methodology. The methodology should guide designers in the identification of what information and controls are required, the identification and selection of candidate HSI approaches, and the detailed design of the HSIs. It should include the development and use of HFE guidelines and standards and how to resolve conflicts in guidance that arise. It should also address the use of analysis and evaluation methodologies for dealing with design issues. The availability of an HSI design methodology will help ensure standardization and consistency in the application of HFE principles.

Issues related to the detailed design of specific aspects of the HSI should be resolved during HSI design activities rather than at verification and validation (V&V). For example, considerations as to acceptable display formats or alarm system processing should be resolved during the Element 7 activities and reviewed rather than deferred to V&V (as described in Section 11), at which point making modifications to the design is significantly more difficult.

### 8.2 Objective

The objective of this review is to evaluate the HSI design process and the detailed HSI design that is a product of that process. The review should ensure that the applicant has appropriately translated function and task requirements to the detailed HSIs through the systematic application of HFE principles and criteria.

### 8.3 Applicant Submittals

The applicant should provide the following documents for staff review: Implementation Plan, Analysis Results Report, and HFE Design Team Evaluation Report. For a description of these submittals, see Section 1.4.4.

Other design-related HSI documents should be reviewed, such as applicant-developed guidance documents and detailed trade studies, technology assessments, or tests or experiment reports developed to support the HSI design. In addition, a variety of mockups, prototypes, or similar

physical representations of the HSI design may be available for preliminary review of the design implementation.

### 8.4 Review Criteria

- (1) *HSI Design Process Guidance*—The HSI design process should be organized and documented to support its standardized and consistent use by members of the design team and their contractors. Guidance should be provided to the team for accomplishing the following (each is defined in the criteria to follow)
  - task-related HSI requirements
  - general HSI design
  - detailed HSI design
  - HSI evaluation
  - HSI design documentation
- (2) *HSI Design Scope*—The scope of the HSI design should include
  - the overall work environment
  - workspace layout (e.g., control room and remote shutdown facility layouts)
  - control panel and console design
  - control and display device layout
  - information and control interface design details, such as graphic display formats, symbols, dialog design and input methods
- (3) *Task-Related HSI Requirements*—This criterion addresses the identification of the HSI requirements to support human functions and tasks using the results of earlier HFE PRM elements as a basis. The requirements should address alarms, displays, controls, and operator aids. For example, the range and accuracy of displayed information should be consistent with operator information requirements for making decisions regarding the plant state. Precision requirements for the display of plant information (e.g., number of demarcations on a scale) should be defined to a level that is consistent with task requirements without burdening the operator with unnecessary detail (e.g., excessive number of decimal places). Units of measurement should be defined to be consistent across related operator tasks (e.g., operators should not have to convert values from one measurement system to another). The technical

basis for task-related HSI requirements should be documented.

- (4) *HSI Characteristics*—The HSI should provide the task-required alarms, displays, controls, and operator aids (as defined in criterion 3) for process monitoring, decision-making, and control. The HSI design should support human performance and usability through the following characteristics:

- Compatibility with the cognitive and physiological capabilities of plant personnel
- Minimization of the demands of secondary tasks. Secondary tasks are activities performed when interfacing with the system, but that are not directed to the primary task of process monitoring, decision-making, and control. Examples include efforts operators must expend managing the interface, such as navigation through displays, managing windows, and accessing data. Although necessary, performance of secondary tasks detracts from the crew's performance of primary tasks.
- Support for the use of the HSI, such as providing (1) flexibility (e.g., multiple means to carry out actions or verify automatic actions), (2) guidance on HSI use, and (3) error tolerance and mitigation
- Accommodation of human performance under the range of conditions, for example, normal as well as credible extreme conditions. The design process should take into account the use of the HSI over the duration of a shift and in plausible scenarios that may result in reduced visibility and ventilation or control room evacuation. The design of non-control room HSIs, such as local control stations, should address constraints imposed by the environment (e.g., noise, temperature, contamination) and by protective clothing.

- (5) *General HSI Design Feature Selection*—This criterion addresses the selection of general HSI design features, such as the selection of a large-screen control room display panel (as opposed to workstation displays only), or to utilize touch screen controls (as opposed to hard controls or trackballs). The selection of general features should be based upon a consideration of alternative approaches for addressing the HSI design characteristics (as identified in Criterion 4 above). Evaluation methods can include operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations. Such evaluations should

consider the strengths and limitations of design options. The process for evaluating alternatives and the justification for the final selection should be documented.

- (6) *Guidelines for Detailed HSI Design*—The applicant should utilize HFE guidelines for the detailed design of the selected general HSI features, layout, and environment. This will facilitate the standard and consistent application of HFE principles to the detailed design. Generic HFE guidance documents should be tailored to the applicant's specific HSI design and documented in a guidance or specification document. HFE guidance documents should contain statements of their intended scope, references to source materials, instructions for their proper use, and procedures to be followed when discrepancies are found.

- (7) *Analysis for Detailed HSI Design*—Design details, problems, issues that are not well defined by guidelines, or conflicting guidelines should be analyzed. Analysis methods can include operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations. For example,

- Mockups and models may be used to resolve access, workspace and related HFE problems and incorporate these solutions into system design.
- Dynamic simulation and HSI prototypes should be considered for use to evaluate design details of equipment requiring critical human performance or equipment not adequately addressed by guidelines.

- (8) *HSI Evaluation*—The HSI should be evaluated in an ongoing fashion to ensure its acceptability for task performance and conformance to HFE, criteria, standards, and guidelines. Special attention should be given to those HSIs that are unique or safety related. This should be done to ensure that poor design solutions do not remain undetected until Element 10 V&V, at which time design changes become more difficult.

Aspects of the HSI that are at variance with design guidance or for which HFE guidance is lacking should be analyzed. The applicant may use many means to resolve these issues, including operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations.

Evaluations should be conducted to ensure that the HSI includes all information and controls re-

quired to perform operator tasks and that extraneous controls and displays not required for the accomplishment of any tasks are excluded.

The outcomes of these evaluations and rationale for resulting design decisions should be documented and available for review.

- (9) *HSI Design Documentation*—The HSI design should be documented to include:

- the detailed HSI description, including the format and performance characteristics
- the basis for the HSI design characteristics with respect to operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations

- (10) The following documents may be used as guidance (per Section 1.4.4):

Regulatory Guide 1.22: *Periodic Testing of Protection System Actuation Functions* (NRC).

Regulatory Guide 1.47: *Bypassed and Inoperable Status Indication for NPP Safety Systems* (NRC).

Regulatory Guide 1.62: *Manual Initiation of Protective Actions* (NRC).

Regulatory Guide 1.81: *Shared Emergency and Shutdown Electrical Systems for Multi-Unit NPPs* (NRC).

Regulatory Guide 1.97: *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environmental Conditions During and Following an Accident* (NRC).

Regulatory Guide 1.108: *Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at NPPs* (NRC).

Regulatory Guide 1.105: *Instrumentation Setpoints* (NRC).

NUREG-0696: *Functional Criteria for Emergency Response Facilities*, 1980 (NRC).

NUREG-0700: *Guidelines for Control Room Design Reviews*, 1981 (NRC).

NUREG-0800: *Standard Review Plan*, Rev. 1, 1984 (NRC).

NUREG/CR-5908: *Advanced Human-System Interface Design Review Guideline*, 1994 (NRC – J. O'Hara et al.).

Draft NUREG/CR-6105: *Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems*, 1993 (NRC – J. O'Hara et al.).

Draft NUREG/CR-6146: *Local Control Stations: Human Engineering Issues and Insights*, 1993 (NRC – W. Brown et al.).

EPRI-ALWR URD: *Advanced Light Water Reactor Utility Requirements Document*, Volume II, *Evolutionary Plant*, Rev. 4, 1992 (Electric Power Research Institute).

EPRI NP-3659: *Human Factors Guide for Nuclear Power Plant Control Room Development*, 1984 (Electric Power Research Institute – R.G. Kinkade and J. Anderson).

EPRI NP-3701: *Computer-Generated Display System Guidelines*, Volumes 1 and 2, 1984 (Electric Power Research Institute – R. Frey et al.).

EPRI NP-4350: *Human Engineering Design Guidelines for Maintainability*, 1985 (Electric Power Research Institute – R. Pack et al.).

IEC-964: *Design for Control Rooms of Nuclear Power Plants*, 1989 [International Electrotechnical Commission (Bureau Central de la Commission Electrotechnique Internationale)].

ANSI HFS-100: *American National Standard for Human Factors Engineering of Visual Display Terminal Workstations*, 1988 (American National Standards Institute).

MIL-HDBK-759A: *Human Factors Engineering Design for Army Materiel*, 1981 (Department of Defense).

MIL-STD-1472D: *Human Engineering Design Criteria for Military Systems, Equipment and Facilities*, 1989 (Department of Defense).

DOD-HDBK-761A: *Human Engineering Guidelines for Management Information Systems*, 1990 (Department of Defense).

ESD-TR-86-278: *Guidelines for Designing User Interface Software*, 1986 (Department of Defense).

## Procedures

**Element 8**

**Procedure Development**



## 9 ELEMENT 8 - PROCEDURE DEVELOPMENT

### 9.1 Background

While in the nuclear industry, procedure development has historically been considered the responsibility of individual utilities, the rationale for including a procedure development element in the HFE PRM is that procedures are considered an essential component of the HSI design and should be a derivative of the same design process and analyses as the other components of the HSI (e.g., displays, controls, operator aids) and subject to the same evaluation processes. In the current fleet of plants, technically detailed, human-factored emergency operating procedures (EOPs) were an improvement after the accident at Three Mile Island (TMI) to support safe operations. After TMI the NPP owners groups developed generic technical guidance (GTG); utilities then produced emergency procedures based on the GTG. Thus, procedure development programs were conducted by the individual utilities and have not been part of HSI design activities. However, since procedures were developed after the plant HSI (e.g., control room) design, they were essentially retrofitted to suit the existing interface. Further, since procedures were developed by individual utilities, their development and final implementation varied greatly. As a result, human factors problems existed and identification, access, interpretation, and validation of procedures remained a problem for years in some plants (as indicated by the NRC emergency operating procedure (EOP) inspection series) (Lapinsky, 1989; Galletti and Sutthoff, 1992). In addition, inconsistencies between procedures and the HSI have been a source of difficulty for operators.

For new plant designs and advanced reactors, these problems should clearly be addressed and solved as part of the design process. To accomplish this objective, GTG and, if possible, procedures should be developed as part of the same design process as that for the other components of the HSI to ensure their full integration as part of the HSI. The same human factors analyses, such as task analyses, should be used to guide control panel as well as procedure development. The same human factor principles should be applied to both aspects of the interface to ensure complete integration and consistency. Further, procedures should be evaluated in conjunction with the HSI; that is, procedures are a significant aspect of system verification and validation (Element 10).

### 9.2 Objective

The objective of this review is to ensure that the applicant's procedure development program will result in procedures that support and guide human interaction with plant systems and 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.

### 9.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan, analysis results report, and HFE design team evaluation report. For a description of these submittals, see Section 1.4.4.

In addition, GTG and draft procedures should be available for review.

### 9.4 Review Criteria

- (1) The scope of the procedures covered in the element are
  - GTG
  - plant and system operations (including startup, power, and shutdown operations)
  - abnormal and emergency operations
  - preoperational, startup, and surveillance tests
  - alarm response
- (2) The basis for procedure development should include
  - plant design bases
  - system-based technical requirements and specifications
  - task analyses results
  - critical human actions identified in the HRA/PRA
  - initiating events to be considered in the EOPs, including those events in the design bases
  - GTG
- (3) A writers guide should be developed to establish the process for developing technical procedures that are complete, accurate, consistent, and easy to understand and follow. The guide should contain sufficiently objective criteria so that procedures developed in accordance with it are consistent in organization, style, and content. The guide should be used for all procedures within the scope of this element. It should provide instructions for procedure content and format including the writing of action



steps and the specification of acceptable acronym lists and acceptable terms to be used.

- (4) The content of the procedures should incorporate the following elements:

- title
- statement of applicability
- references
- prerequisites
- precautions (including warnings, cautions, and notes)
- limitations and actions
- required human actions
- acceptance criteria
- checkoff lists

- (5) In addition to the general procedure elements identified in Criterion 4 above, GTG should be symptom-based with clearly specified entry conditions.

- (6) All procedures should be verified and validated. A review should be conducted to ensure they are correct and can be carried out. Their final validation should be performed in a simulation of the integrated system as part of the verification and validation activities described in Element 8.

- (7) An analysis should be conducted to determine the impact of providing computer-based procedures (either partial or complete) and to specify where such an approach would improve procedure utilization and reduce operating crew errors related to procedure use.

- (8) A plan for procedure maintenance and control of updates should be developed.

- (9) The physical means by which operators access and use procedures, especially during operational events, should be evaluated as part of the HFE design process. This criterion generally applies to both hard-copy and computer-based procedures, although the nature of the issues differs somewhat depending on the implementation. For example, the process should address the storage of procedures, ease of operator access to the correct procedures, and laydown of hard-copy procedures for use in the control room, remote shutdown facility, and local control stations.

- (10) The following documents may be used as guidance (per Section 1.4.4):

NUREG-0800: *Standard Review Plan*, Rev. 1, 1984 (NRC).

NUREG-0899: *Guidelines for the Preparation of Emergency Operating Procedures*, 1982 (NRC).


NUREG-1358: *Lessons Learned From the Special Inspection Program for Emergency Operating Procedures*, 1989 (NRC).

NUREG-1358: *Lessons Learned From the Special Inspection Program for Emergency Operating Procedures*, Supplement 1, 1989 (NRC).

NUREG/CR-5228: *Techniques for Preparing Flowchart Format Emergency Operating Procedures*, Volumes 1 and 2, 1989 (NRC - V. Barnes et al.).

NRC Regulatory Guide 1.33 (Rev. 2): *Quality Assurance Program Requirements*, 1978 (NRC).

ANS 3.2-1988: *Administrative Controls and QA for the Operational Phase of NPPs*, 1988 (American Nuclear Society).



**Training**

## **Element 9**

# **Training Program Development**

## 10 ELEMENT 9 - TRAINING PROGRAM DEVELOPMENT

### 10.1 Background

Training of plant personnel is an important factor in ensuring safe and reliable operation of nuclear power plants. Advanced nuclear power plants may pose demands on the knowledge, skills, and abilities of operational personnel that are different from those posed by traditional plants. These demands stem from differences in operator responsibilities resulting from advanced plant design features (e.g., passive systems and increased automation) and differences in operator task characteristics resulting from advances in HSI technologies.

A systems approach to the training, as defined in 10 CFR 55.4, is required of the licensee by 10 CFR 52.78 and 50.120. Training design is to be based on the systematic analysis of job and task requirements. The HFE analyses associated with the HSI design process provide a valuable understanding of the task requirements of operations personnel. Therefore, training program development should be coordinated with the other elements of the HFE design process.

### 10.2 Objective

The objective of this review is to ensure that the combined operating license (COL) applicant establishes an approach for the development of personnel training that incorporates the elements of a systems approach to training, and

- evaluates the knowledge and skill requirements of personnel
- coordinates training program development with the other elements of the HFE design process
- implements the training in an effective manner that is consistent with human factors principles and practices

### 10.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plan and a results report.

### 10.4 Review Criteria

- (1) The training program should be developed in accordance with 10 CFR 50.120, 10 CFR Part 55, and other relevant requirements to ensure that personnel have the qualifications commensurate with the performance requirements of their jobs. Training should address
  - the full range of positions of operational personnel including licensed and nonlicensed personnel whose actions may affect plant safety
  - the full range of plant functions and systems including those that may be different from those in predecessor plants (e.g., passive systems and functions)
  - the full range of relevant HSI components (e.g., main control room, remote shutdown panel, local control stations) including characteristics that may be different from those in predecessor plants (e.g., display space navigation, operation of "soft" controls)
  - the full range of plant conditions
- (2) Training program development should address applicable requirements of NUREG-0800 Section 13.2 ("Training"), 10 CFR 50.120, 10 CFR Part 55, and other applicable regulations.
- (3) A systems approach to training as defined in 10 CFR 55.4 should be used. The training development implementation plan should be consistent with the following five elements:
  - systematic analysis of jobs to be performed
  - learning objectives derived from the analysis that describe desired performance after training
  - training design and implementation based on the learning objectives
  - evaluation of trainee mastery of the objectives during training
  - evaluation and revision of the training based on the performance of trained personnel in the job setting
- (4) The roles of all organizations, especially the COL applicant and vendors, should be specifically defined for the development of training requirements, development of training information sources, development of training materials, and implementation of the training program. For example, the role of the vendor may range from merely providing input materials (e.g., emergency procedure guidelines) to conducting portions of specific training programs.
- (5) The qualifications of organizations and personnel involved in the development and conduct of training should be defined.

- (6) The overall scope of training should be defined including the following:

- categories of personnel (e.g., senior reactor operator) to be trained
- specific plant conditions (normal, upset, and emergency)
- specific operational activities (e.g., operations, maintenance, testing and surveillance)
- HSI components (e.g., main control room, emergency operations facility, remote shut-down panel, local control stations)

The scope of training should include the training of personnel participating in verification and validation of the plant design (Element 10).

- (7) Learning objectives should be derived from the analysis that describes desired performance after training. This analysis should include but not be limited to training issues identified in the following HFE PRM elements:

- Operating Experience Review—previous training deficiencies and operational problems that may be corrected through additional and enhanced training, and positive characteristics of previous training programs
- Function Analysis and Allocation—functions identified as new or modified
- Task Analysis—tasks identified during task analysis as posing unusual demands including critical tasks identified by PRA/HRA, new or different tasks, and tasks requiring high coordination, high workload, or special skills
- Human Reliability Assessment—requirements for coordinating individual roles to reduce the likelihood and/or consequences of human error associated with critical human actions and the use of advanced technology
- HSI Design—design features whose purpose or operation may be different from the past experience or expectations of personnel
- Plant Procedures—tasks that have been identified during procedure development as being problematic (e.g., procedure steps that have undergone extensive revision as a result of plant safety concerns)

- Verification and Validation (V&V)—training concerns identified during V&V, including HSI usability concerns identified during validation or suitability verification and operator performance concerns (e.g., misdiagnoses of plant event) identified during validation trials

- (8) Learning objectives should also be derived from knowledge and skill requirements derived from the final safety analysis report, system description manuals and operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the staff as being important to training.
- (9) The design of the training program should be defined to specify how learning objectives will be conveyed to the trainee. The use of lecture, simulator, and on-the-job training to convey particular categories of learning objectives should be defined. Specific plant conditions and scenarios to be used in training programs should be defined. Training implementation considerations such as the temporal order and schedule of training segments should be defined. The training program specifications should include justifications based on HFE principles of training, training practices, and other criteria.
- (10) Facilities and resources such as plant-referenced simulator and part-task training simulators required to satisfy training design requirements should be defined.
- (11) Methods for evaluating trainee mastery of training objectives should be defined, including written and oral tests and walkthrough and simulator exercises. Evaluation criteria for training objectives should be defined for individual training modules. Methods for assessing overall proficiency should be defined and coordinated with regulations, where applicable.
- (12) Methods for verifying the accuracy and completeness of training course materials should be defined.
- (13) Methods for evaluating the overall effectiveness of the training programs should be defined, including review of operator performance in tests and walkthrough and simulator exercises and on-the-job performance.
- (14) Procedures for refining and updating the content and conduct of training should be established, including procedures for tracking training course modifications.
- (15) The following documents may be used as guidance (per Section 1.4.4):

10 CFR 50.120: *U.S. Code of Federal Regulations*, Part 50, "Training and Qualification of Nuclear Power Plant Personnel," Title 10, "Energy."

10 CFR Part 55: *U.S. Code of Federal Regulations*, Part 55, "Operators' Licenses," Title 10, "Energy."

NUREG-0800: *Standard Review Plan*, 1984 (NRC).

ANSI/ANS 3.1-1981: *Selection, Qualification, and Training of Personnel for Nuclear Power Plants*, 1981 (American Nuclear Society).



## **Element 10**

### **Human Factors Verification and Validation**



V&V

## **Element 10**

### **Human Factors Verification and Validation**

## 11 ELEMENT 10 – HUMAN FACTORS VERIFICATION AND VALIDATION

### 11.1 Background

Verification and validation (V&V) evaluations seek to comprehensively determine that the design conforms to HFE design principles and that it enables plant personnel to successfully perform their tasks to achieve plant safety and other operational goals. This element is made up of the five V&V activities shown in Figure 11.1. Although the applicant should perform these activities in the order shown, it should be recognized that the process is iterative. A major distinction exists between design *process* V&V evaluations and design *implementation* verification. Design process evaluations are conducted to ensure that HFE principles and methods are appropriately incorporated into the design process. They include the following:

- HSI Task Support Verification—a check to ensure that HSI components are provided to address all identified personnel tasks
- HFE Design Verification—a check to determine whether the design of each HSI component reflects HFE principles, standards, and guidelines
- Integrated System Validation—performance-based evaluations of the integrated design to ensure that the HFE/HSI supports safe operation of the plant
- Human Factors Issue Resolution Verification—a check to ensure that the HFE issues identified during the design process have been acceptably addressed and resolved

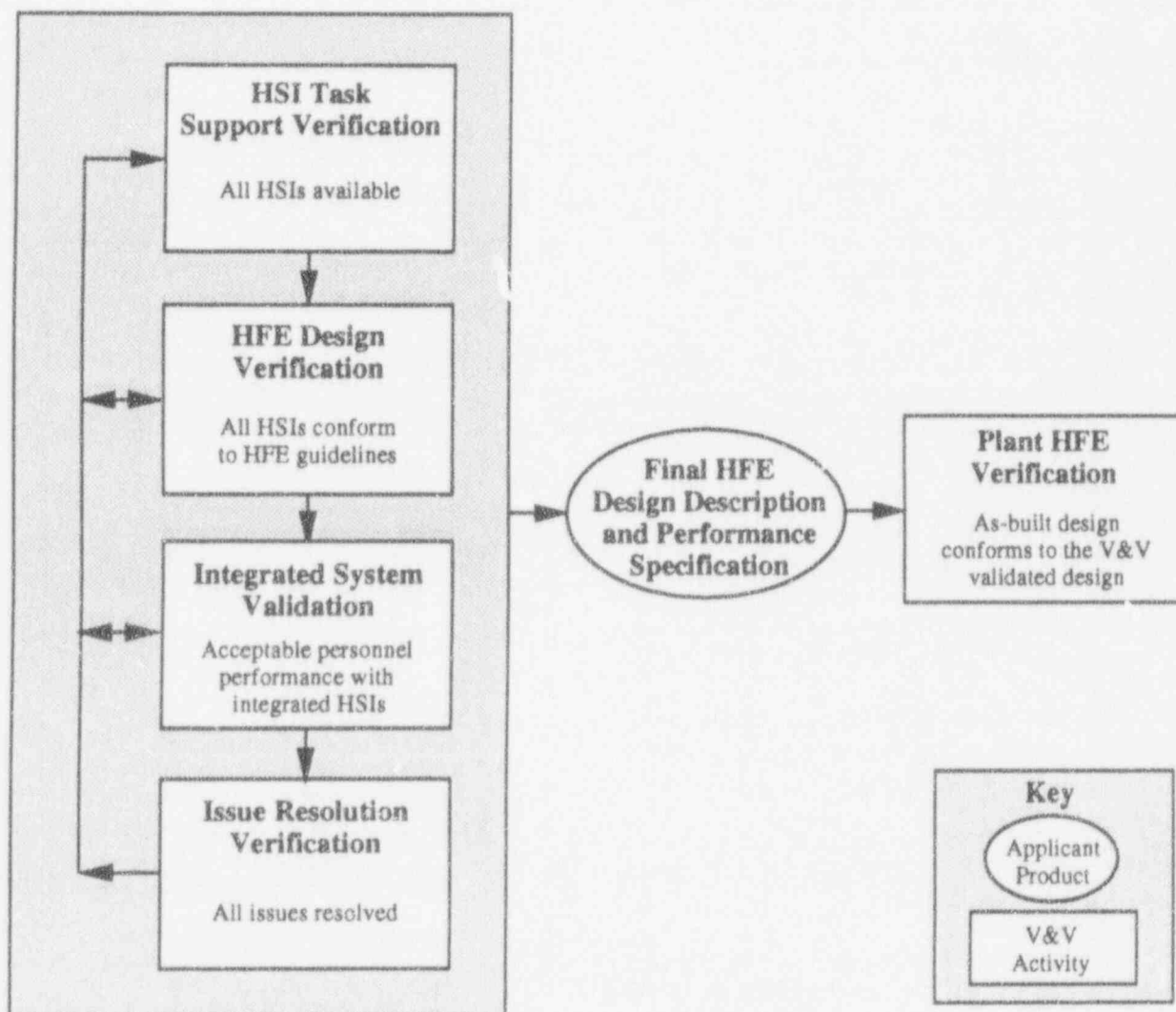


Figure 11.1 Relationship Between Verification and Validation Activities

The process should begin with HSI task support verification to identify missing or potentially unnecessary HSI components. Then the HSIs should undergo HFE design verification to ensure the HSIs are acceptably designed according to HFE principles. Integrated system validation should be performed on a dynamic, high-fidelity representation of the "final" HSI design, that is, after HFE design verification activities have been completed. Modifications to the design may be required after validation. Major changes may require integrated system validation of selected issues. However, relatively minor changes to the design may only require HSI task support verification and HFE design verification. Since issues can arise during validation, issue resolution verification cannot be completed until validation issues have been resolved.

The "final" design should be documented in a design description document that includes the requirements for verification that the "as built" design is the design resulting from the design process V&V evaluations. This document can then be used to conduct a final plant HFE/HSI design verification. The main activity should be a check of the actual HSIs against the description.

V&V, as discussed in this element, is not intended as the activity whereby HSI subsystem design concerns and issues (such as the coding techniques used in the alarm system) are explored and evaluated. These issues should be addressed as part of HFE analyses, tests, and evaluations conducted earlier in the design process and reviewed as part of previous HFE PRM elements.

## 11.2 Objective

The objective of this review is to ensure the following:

- The HFE/HSI design provides all necessary alarms, displays, and controls to support plant personnel tasks (HSI task support verification).
- The HFE/HSI design conforms to HFE principles, guidelines, and standards (HFE design verification).
- The HFE/HSI design can be effectively operated by personnel within all performance requirements (integrated system validation).
- The HFE/HSI design resolves all of the identified HFE issues in the tracking system (human factors issue resolution verification).
- The final product as built conforms to the verified and validated design that resulted from the HFE design process (final plant HFE/HSI design verification).

## 11.3 Applicant Submittals

The applicant should provide the following documents for staff review: implementation plans, analysis results reports, and HFE design team evaluation reports for each V&V activity. For a description of these submittals, see Section 1.4.4. The implementation plans should address all V&V activities including final plant HFE/HSI design verification. For the latter, aspects of the verification that have not been verified in design process V&V activities should be explicitly identified. The HFE issues tracking system should also be reviewed.

A high-fidelity prototype or simulator of the HSI should be available for staff to review and to witness the integrated system validation evaluations.

After the V&V activities, the final design should be described in a detailed design description. This description will serve as the basis for the verification that the actual in-plant HSI conforms to the design that resulted from the HFE design process including the V&V activities. The results of the applicant's final plant HFE/HSI design verification should be documented.

## 11.4 Review Criteria

### 11.4.1 General Criteria

- (1) The general scope of V&V should include the following for all applicable facilities as defined in Element 1 - HFE Program Management:

- HSI hardware
- HSI software
- communications
- procedures
- workstation and console configurations
- design of the overall work environment
- trained personnel

The scope of integrated system validation may be limited to those applicable facilities required for the evaluation of scenarios described in item 4 of Section 11.4.4 below.

- (2) The order of V&V activities should be as follows:

- HSI task support verification
- HFE design verification
- integrated system validation

- human factors issue resolution verification
- final plant HFE/HSI design verification

(3) The following documents may be used as guidance (per Section 1.4.4):

Documents listed for the following HFE PRM elements can be used to support V&V activities:

- Element 7 – HSI Design
- Element 8 – Procedure Development
- Element 9 – Training Program Development

Regulatory Guide 1.33: *Quality Assurance Program Requirements* (NRC).

IEEE Std. 845-1988: *IEEE Guide to Evaluation of Man-Machine Performance in Nuclear Power Generating Station Control Rooms and Other Peripheries*, 1988 (Institute of Electrical and Electronics Engineers).

AR 602-1: *Human Factors Engineering Program*, 1983 (Department of Defense).

TOP 1-2-610: *Test Operating Procedure*, Parts 1 and 2, 1990 (Department of Defense).

#### 11.4.2 Human-System Interface Task Support Verification

- (1) All aspects of the HSI (e.g., controls, displays, procedures, and data processing) that are required to accomplish human tasks and actions [as defined by the task analysis, emergency operating procedure analysis, and the critical actions of the probabilistic risk assessment/human reliability analysis (PRA/HRA)] should be verified as available through the HSI.
- (2) It should be verified that the HSI does not include information, displays, controls, etc., that do not support operator tasks. This includes nonfunctional decorative details such as borders and shadowing on graphical displays.

#### 11.4.3 HFE Design Verification

- (1) All aspects of the HSI (e.g., controls, displays, procedures, and data processing) should be verified as designed to be appropriate to personnel task requirements and operational considerations as defined by design specifications and to be consistent with accepted HFE guidelines, standards, and principles.
- (2) Deviations from accepted HFE guidelines, standards, and principles should be acceptably justified

on the basis of a documented rationale such as trade study results, literature-based evaluations, demonstrated operational experience, and tests and experiments.

#### 11.4.4 Integrated System Validation

(1) The methodology for integrated system validation should address

- general objectives
- personnel performance issues to be addressed (e.g., crew coordination)
- test methodology and procedures
- test participants (operators to participate in the test program)
- test conditions (including plant conditions, operating sequences, and accident scenarios)
- HSI description
- performance measures
- data analysis
- criteria for evaluation of results
- utilization of evaluations

(2) Validation should be performed by evaluating dynamic task performance using tools that are appropriate to the accomplishment of this objective. The primary tool for this purpose is a simulator, that is, a facility that physically represents the HSI configuration and that dynamically represents the operating characteristics and responses of the plant design in real time. The requirement to validate performance at plant HSIs outside the control room (CR) will be dependent on the applicant's design. Human actions at non-CR facilities such as remote shutdown panels and local control stations may be evaluated using mockups, prototypes, or similar tools.

(3) The evaluations should address

- adequacy of entire HSI configuration for achievement of HFE program goals
- confirmation of allocation of function and the structure of tasks assigned to personnel
- adequacy of staffing and the HSI to support staff to accomplish their tasks
- adequacy of procedures
- confirmation of the dynamic aspects of the HSI for task accomplishment



- evaluation and demonstration of error tolerance to human and system failures
- (4) All critical human actions as defined by the task analysis and PRA/HRA should be tested and found to be adequately supported in the design, including the performance of critical actions outside the control room. The design of tests and evaluations to be performed as part of HFE V&V activities should specifically examine these actions.
- (5) Regulatory Guide 1.33, Appendix A, contains several categories of activities that should be covered by procedures. The validation should evaluate selected activities based on procedures developed to address this guide. The evaluation should include appropriate procedures in each relevant category, that is,
- administrative procedures
  - general plant operating procedures
  - procedures for startup, operation, and shutdown of safety-related systems
  - procedures for abnormal, offnormal, and alarm conditions
  - procedures for combating emergencies and other significant events
  - procedures for control of radioactivity
  - procedures for control of measuring and test equipment and for surveillance tests, procedures, and calibration
  - procedures for performing maintenance
  - chemistry and radiochemical control procedures
- (6) Dynamic evaluations should evaluate the HSI under a range of operational conditions and upsets, and should include the following:
- normal plant evolutions (e.g., startup, full-power, and shutdown operations)
  - instrument failures [e.g., safety-related system logic and control unit, fault tolerant controller (nuclear steam supply system), local "field unit" for multiplexer (MUX) system, break in MUX line]
  - HSI equipment and processing failure (e.g., loss of video display units, loss of data processing, loss of large overview display)
  - transients (e.g., turbine trip, loss of offsite power, station blackout, loss of all feedwater, loss of service water, loss of power to selected buses and CR power supplies, safety/relief valve transients)
  - accidents (e.g., main steam line break, positive reactivity addition, control rod insertion at power, control rod ejection, anticipated transient without scram, and various-sized loss-of-coolant accidents)
  - reactor shutdown and cooldown from remote shutdown panel
- (7) The scenarios should be realistic. Selected ones should include environmental conditions such as noise and distractions that may affect human performance in an actual nuclear power plant. For actions outside the CR, the performance impacts of potentially harsh environments (i.e., high radiation) that require additional time should be realistically simulated (i.e., time to don protective clothing and access hot areas).
- (8) Performance measures for dynamic evaluations should be adequate to test the achievement of all objectives, design goals, and performance requirements and should include the following at a minimum:
- system performance measures relevant to plant safety
  - crew primary task performance (e.g., task times, procedure violations)
  - crew errors
  - situation awareness
  - workload
  - crew communications and coordination
  - dynamic anthropometry evaluations
  - physical positioning and interactions

#### 11.4.5 Human Factors Issue Resolution Verification

- (1) All issues documented in the human factors issue tracking system of Element 1 should be verified as adequately addressed.

- (2) Issues that could not be resolved until a plant is built should be specifically identified and incorporated into the final plant HFE/HSI design verification.

#### **11.4.6 Final Plant HFE/HSI Design Verification**

- (1) Following design process V&V activities, a design description should be developed that describes the detailed design and its performance criteria.
- (2) Aspects of the design that were not addressed in design process V&V should be evaluated using an appropriate V&V method. Aspects of the design addressed by this criterion may include design characteristics such as new or modified displays for plant-specific design features and features that cannot be evaluated in a simulator such as CR lighting and noise.
- (3) The in-plant HFE should conform to the design that resulted from the HFE design process and V&V activities.

## References

## References

## 12 REFERENCES\*

- American National Standards Institute, ANSI HFS-100-1988, "American National Standard for Human Factors Engineering of Visual Display Terminal Workstations," Santa Monica, California, 1988.
- American Nuclear Society, ANSI/ANS 3.1-1981, "Selection, Qualification, and Training of Personnel for Nuclear Power Plants," LaGrange Park, Illinois, 1981.
- ..., ANS 3.2-1988, "Administrative Controls and QA for the Operational Phase of NPPs," LaGrange Park, Illinois, 1988.
- Bailey, R.W., *Human Performance Engineering: A Guide for System Designers*, Prentice-Hall, Inc., New Jersey, 1982.
- Bari, R., et al., "Probabilistic Safety Analysis Procedures Guide," NUREG/CR-2815, U.S. Nuclear Regulatory Commission, Washington, D.C., 1985.
- Barnes, V., et al., "Techniques for Preparing Flowchart Format Emergency Operating Procedures," NUREG/CR-5228, Volumes 1 and 2, U.S. Nuclear Regulatory Commission, Washington, D.C., 1989.
- Bastl, W., et al., "Balance Between Automation and Human Actions in NPP Operation: Results of International Cooperation," *Balancing Automation and Human Actions in Nuclear Power Plants*, 1991, International Atomic Energy Agency, Vienna, Austria, 1991.
- Beattie, J., and J. Malcolm, "Development of a Human Factors Engineering Program for the Canadian Nuclear Industry," *Proceedings of the Human Factors Society - 35th Annual Meeting*, 1991, Human Factors Society, Santa Monica, California, 1991.
- Brown, W., J. Higgins, and J. O'Hara, "Local Control Stations: Human Engineering Issues and Insights," Draft NUREG/CR-6146, Brookhaven National Laboratory, Upton, New York, 1993.
- Burgy, D., et al., "Task Analysis of Nuclear Power Plant Control Room Crews," NUREG/CR-3371, Volumes 1 and 2, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.
- Campbell, D., and D. Fisk, "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin*, 56:81-105, 1959.
- Carter, R., and R. Uhrig, "Human Factors Issues Associated With Advanced Instrumentation and Controls Technologies in Nuclear Plants," NUREG/CR-5439, U.S. Nuclear Regulatory Commission, Washington, D.C., 1990.
- Coblentz, A., *Vigilance and Performance in Automated Systems*, NATO ASI Series D, 49, Kluwer Academic Publishers, Boston, Massachusetts, 1988.
- DeGreene, K.B., *Systems Psychology*, McGraw-Hill Book Company, New York, 1970.
- Drury, C., B. Paramore, H. Van Cott, S. Grey, and E. Corlett, "Task Analysis," *Handbook of Human Factors* (G. Salvendy, ed.), Wiley-Interscience, New York, 1987.
- Edwards, E., "Automation in Civil Transport Aircraft," *Applied Ergonomics*, 8:194-198, 1977.
- El-Bassioni, A., et al., "PRA Review Manual," NUREG/CR-3485, U.S. Nuclear Regulatory Commission, Washington, D.C., 1985.
- Electric Power Research Institute, *Advanced Light Water Reactor Utility Requirements Document*, Volume II, *Evolutionary Plant*, Revision 4, Electric Power Research Institute, Palo Alto, California, 1992.
- ..., "Man-Machine Interface Systems," *Advanced Light Water Reactor Utility Requirements Document*, Volume II, *Evolutionary Plant*, NP-6780-L, Revision 1, Electric Power Research Institute, Palo Alto, California, 1990.
- Ephrath, A., and L. Young, "Monitoring vs. Man-In-The-Loop Detection of Aircraft Control Failures," *Human Detection and Diagnosis of System Failures*, Plenum Press, New York, 1981.
- Frey, R., et al., "Computer-Generated Display System Guidelines," EPRI NP-3701, Volumes 1 and 2, Electric Power Research Institute, Palo Alto, California, 1984.
- Gagne, R.M., and A.W. Melton, *Psychological Principles in System Development*, Holt, Rinehart and Winston, New York, 1988.
- Galletti, G.S., and A.B. Sutthoff, "Lessons Learned From the Special Inspection Program for Emergency Operating Procedures," NUREG-1358, Supplement 1, U.S. Nuclear Regulatory Commission, Washington, D.C., 1992.
- Gertman, D., W. Gilmore, W. Galyean, M. Groh, C. Gentilioni, B. Gilbert, and W. Reece, "Nuclear Computerized Library for Assessing Reactor Reliability: Summary Description," NUREG/CR-4639, Volume 1, U.S. Nuclear Regulatory Commission, Washington, D.C., 1990.

\*The references include those identified in appendix B.

- Gould, J., "How To Design Usable Systems," *Handbook of Human Computer Interaction*, Elsevier Science Publishers, Amsterdam, Netherlands, 1988.
- Hannaman, G., A. Spurgin, V. Joksimovich, J. Wreathall, and D. Orvis, "Systematic Human Action Reliability Procedure (SHARP)," NP-3583, Interim Report, Electric Power Research Institute, Palo Alto, California, June 1984.
- Institute of Electrical and Electronics Engineers, IEEE Std. 845-1988, "IEEE Guide to Evaluation of Man-Machine Performance in Nuclear Power Generating Station Control Rooms and Other Peripheries," New York, 1988.
- ..., IEEE Std. 1023-1988, "IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations," New York, 1988.
- ..., IEEE Std. P1082/D8-1990, "A Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations," New York, 1990.
- International Atomic Energy Agency (IAEA), International Nuclear Safety Advisory Group, Safety Series No. 75-INSAG-3, "Basic Safety Principles for Nuclear Power Plants," Vienna, Austria, 1988.
- International Atomic Energy Agency, International Working Group on NPP Control and Instrumentation, IAEA-TECDOC-668, "The Role of Automation and Humans in Nuclear Power Plants," Vienna, Austria, 1992.
- International Electrotechnical Commission (IEC), "Design for Control Rooms of Nuclear Power Plants," IEC-964, Bureau Central de la Commission Electrotechnique Internationale, Geneva, Switzerland, 1989.
- Karat, J., "The Relation of Psychological Theory to Human-Computer Interaction Standards," *Designing and Using Human-Computer Interfaces and Knowledge Based Systems*, Elsevier Science Publishers, Amsterdam, Netherlands, 1989.
- Kaufman, J., G. Lanik, R. Spence, and E. Trager, "Operating Experience Feedback Report—Human Performance in Operating Events," NUREG-1275, Volume 8, U.S. Nuclear Regulatory Commission, Washington, D.C., 1992.
- Kennedy, W., "Survey of OECD Members on the Use of Computers in Control Rooms of Nuclear Power Plants," *Man-Machine Interface in the Nuclear Industry*, International Atomic Energy Agency, Vienna, Austria, 1988.
- Kibble, M., "Information Transfer From Intelligent EW Displays," *Proceedings of the Human Factors Society—32nd Annual Meeting, 1988*, Human Factors Society, Santa Monica, California, 1988.
- Kinkade, R.G., and J. Anderson, "Human Factors Guide for Nuclear Power Plant Control Room Development," EPRI NP-3659, Electric Power Research Institute, Palo Alto, California, 1984.
- Kockler, F., T. Withers, J. Podiack, and M. Gierman, *Systems Engineering Management Guide*, Department of Defense AD/A223 168, Defense Systems Management College, Fort Belvoir, Virginia, 1990.
- Lapinsky, G., "Lessons Learned From the Special Inspection Program for Emergency Operating Procedures," NUREG-1358, U.S. Nuclear Regulatory Commission, Washington, D.C., 1989.
- Moray, N., and B. Huey, *Human Factors Research and Nuclear Safety*, National Research Council, National Academy of Sciences, Washington, D.C., 1988.
- Moray, N., P. Lootsteen, and J. Pajak, "Acquisition of Process Control Skills," *IEEE Transactions on Systems, Man, and Cybernetics*, 16:497-504, 1986.
- Neboyan, V., and A. Kossilov, *Control Rooms and Man-Machine Interface in Nuclear Power Plants*, IAEA-TECDOC-565, International Atomic Energy Agency, Vienna, Austria, 1990.
- O'Hara, J., et al., "Advanced Human System Interface Design Review Guideline," NUREG/CR-5908, U.S. Nuclear Regulatory Commission, Washington, D.C., 1994.
- O'Hara, J., and R. Hall, "Human-Computer Interface and Human Reliability," *Proceedings on Advances in Human Factors Research on Man/Computer Interactions*, 1990, American Nuclear Society, Nashville, Tennessee, 1990.
- O'Hara, J., W. Brown, and J. Higgins, "Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems," Draft NUREG/CR-6105, Brookhaven National Laboratory, Upton, N.Y., 1993.
- Pack R., et al., "Human Engineering Design Guidelines for Maintainability," EPRI NP-4350, Electric Power Research Institute, Palo Alto, California, 1985.
- Pew, R., and the Committee on Human Factors, "Research Needs for Human Factors," National Research Council, National Academy of Sciences, Washington, D.C., 1983.
- Potter, S., R. Cook, D. Woods, and J. McDonald, "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*, Human Factors Society, Santa Monica, California, 1990.
- Price, H., "The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review," NUREG/CR-2623, U.S. Nuclear Regulatory Commission, Washington, D.C., 1982.
- Pulliam, R., et al., "A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control," NUREG/CR-3331, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.
- Rasmussen, J., K. Duncan, and J. Leplat, *New Technology and Human Error*, J. Wiley and Sons, New York, 1987.
- Reaux, R., and R. Williges, "Effects of Level of Abstraction and Presentation Media on Usability of User-System Interface Guidelines," *Proceedings of the Human Factors Society—32nd Annual Meeting*, Human Factors Society, Santa Monica, California, 1988.
- Sexton, G., "Cockpit-Crew Systems Design and Integration," *Human Factors in Aviation*, Academic Press, New York, 1988.
- Smith, S., "Standards Versus Guidelines for Designing User Interface Software," *Handbook of Human-Computer Interaction*, Elsevier Science Publishers, Amsterdam, Netherlands, 1988.
- Stubler, W., E. Roth, and R. Mumaw, "Evaluation Issues for Computer-Based Control Rooms," *Proceedings of the Human Factors Society—35th Annual Meeting, 1991*, Human Factors Society, Santa Monica, California, 1991.
- Swain, A., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Washington, D.C., 1987.
- ..., and H. Guttmann, "Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Applications—Final Report," NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.
- U.S. Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy," U.S. Government Printing Office, Washington, D.C., revised periodically.
- ..., Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," Title 10, "Energy," U.S. Government Printing Office, Washington, D.C., revised periodically.
- ..., Part 55, "Operator's Licenses," Title 10, "Energy," U.S. Government Printing Office, Washington, D.C., revised periodically.
- U.S. Department of Defense (DOD), "System Safety Program Plan," 882C, Department of the Navy, Philadelphia, Pennsylvania, 1993.
- ..., "Human-Computer Interface Style Guide (Version 1)," Office of Management and Budget, Washington, D.C., 1992.
- ..., "Defense Acquisition," DODD 5000.1, Office of Management and Budget, Washington, D.C., 1991a.
- ..., "Defense Acquisition Management Policies and Procedures," DODI 5000.2, Office of Management and Budget, Washington, D.C., 1991b.
- ..., "Human Engineering Procedures Guide," DOD-HDBK-763, Office of Management and Budget, Washington, D.C., 1991c.
- ..., "Task Performance Analysis," MIL-STD-1478, Department of the Army, Washington, D.C., 1991d.
- ..., "Human Engineering Guidelines for Management Information Systems," DOD-HDBK-761A, Office of Management and Budget, Washington, D.C., 1990a.
- ..., "Manpower and Personnel Integration (MANPRINT) in the Material Acquisition Process," AR 602-2, Department of the Army, Washington, D.C., 1990b.
- ..., "System Engineering Management Plan," DI-MGMT-81024, Office of Management and Budget, Washington, D.C., 1990c.
- ..., "Test Operating Procedure," TOP 1-2-610, Parts 1 and 2, Office of Management and Budget, Washington, D.C., 1990d.
- ..., "Human Engineering Design Criteria for Military Systems, Equipment and Facilities," MIL-STD-1472D, Office of Management and Budget, Washington, D.C., 1989a.
- ..., "Human Engineering Program Plan," DI-HFAC-80740, Office of Management and Budget, Washington, D.C., 1989b.
- ..., "Guidelines for Designing User Interface Software," ESD-TR-86-278, Washington, D.C., 1986.
- ..., "Technical Reviews and Audits for Systems, Equipment, and Computer Software," MIL-STD-1521B, Department of the Air Force, Washington, D.C., 1985.
- ..., "Human Factors Engineering Program," AR 602-1, Department of the Army, Washington, D.C., 1983.

- ..., "Human Factors Engineering Design for Army Material," MIL-HDBK-759A (MI), Department of the Army, Washington, D.C., 1981.
- ..., "Critical Task Analysis Report," DI-H-7055, Office of Management and Budget, Washington, D.C., 1979a.
- ..., "Human Engineering Requirements for Military Systems, Equipment and Facilities," MIL-H-46855B, Office of Management and Budget, Washington, D.C., 1979b.
- U.S. Nuclear Regulatory Commission, Generic Letter 91-06, "Adequacy of Safety-Related DC Power Supplies," Resolution of Generic Issue A-30, Washington, D.C., 1991.
- ..., Generic Letter 91-07, "Reactor Coolant Pump Seal Failures," Generic Letter 91-07, Generic Issue 23, Washington, D.C., 1991.
- ..., Generic Letter 91-11, "LCOs for Class 1E Vital Instrument Buses and Interlocks and LCOs for Class 1E Tie Breakers," Resolution of Generic Issues 48 and 49, Washington, D.C., 1991.
- ..., Information Notice 93-8, "Importance of Engineering Expertise on Shift," Washington, D.C., 1993.
- ..., Information Notice 93-47, "Unrecognized Loss of Control Room Annunciators," Washington, D.C., 1993.
- ..., NUREG-0654, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," Washington, D.C., 1980.
- ..., NUREG-0696, "Functional Criteria for Emergency Response Facilities," Washington, D.C., 1980.
- ..., NUREG-0700, "Guidelines for Control Room Design Reviews," Washington, D.C., 1981.
- ..., NUREG-0737 and supplements, "Clarification of TMI Action Plan Requirements," Washington, D.C., 1980.
- ..., NUREG-0800, "Standard Review Plan," Revision 1, Washington, D.C., 1984.
- ..., NUREG-0899, "Guidelines for the Preparation of Emergency Operating Procedures," Washington, D.C., 1982.
- ..., NUREG-0933 and Supplements 1-12, "A Prioritization of Generic Safety Issues," Washington, D.C., 1991.
- ..., NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," Washington, D.C., draft, 1992.
- ..., NUREG/CR-2300, "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," Washington, D.C., 1983.
- ..., Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," Washington, D.C.
- ..., Regulatory Guide 1.33, "Quality Assurance Program Requirements," Revision 2, Washington, D.C..
- ..., Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for NPP Safety Systems," Washington, D.C.
- ..., Regulatory Guide 1.62, "Manual Initiation of Protective Actions," Washington, D.C.
- ..., Regulatory Guide 1.81, "Shared Emergency and Shutdown Electrical Systems for Multi-Unit NPPs," Washington, D.C.
- ..., Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environmental Conditions During and Following an Accident," Washington, D.C.
- ..., Regulatory Guide 1.105, "Instrumentation Setpoints," Washington, D.C.
- ..., Regulatory Guide 1.108, "Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at NPPs," Washington, D.C.
- ..., Regulatory Guide 1.114, "Guidance to Operators at the Controls and to Senior Operators in the Control Room of a Nuclear Power Unit," Washington, D.C.
- Van Cott, H.P., and R.G. Kinkade, *Human Engineering Guide to Equipment Design*, U.S. Government Printing Office, Washington, D.C., 1972.
- Warm, J., and R. Parasuraman, "Vigilance: Basic and Applied Research," *Human Factors*, Special Issue, 29:623-740, 1987.
- White, J., and D. Lanning, (eds.), "European Nuclear Instrumentation and Controls," NTIS Report No. PB92-100197, World Technology Evaluation Center, Loyola College, Baltimore, Maryland, 1991.
- Wickens, C., and C. Kessel, "The Detection of Dynamic System Failures," *Human Detection and Diagnosis of System Failures*, Plenum Press, New York, 1981.
- Wiener, E., and R. Curry, "Flight-Deck Automation: Promises and Problems," *Ergonomics*, 23:995-1011, 1980.

Wiener, E., and D. Nagel, *Human Factors in Aviation*, Academic Press, New York, 1988.

Woods, D., E. Roth, W. Stubler, and R. Mumaw, "Navigating Through Large Display Networks in Dynamic Control Applications," *Proceedings of the Human Factors*

*Society—34th Annual Meeting, 1990*, Human Factors Society, Santa Monica, California, 1990.

Woodson, W.E., *Human Factors Design Handbook*, McGraw-Hill Book Company, New York, New York, 1981.



**Appendix A**  
**HFE Design Team Composition**

## APPENDIX A

### HFE DESIGN TEAM COMPOSITION

The term "HFE design team" is used in a generic sense in the HFE PRM to refer to the personnel who are responsible for HFE within the scope of this report. There is no intent to prescribe any particular organizational structure for an applicant, nor is it assumed that HFE is the responsibility of a single organization or that there is necessarily an organizational unit called the HFE design team.

The following is a listing of the required areas of expertise for the HFE design team. Associated with each area of expertise is a listing of minimum qualifications and descriptions of typical contributions to the HFE design and implementation process. The descriptions of typical contributions are provided as examples to further describe the potential value of the various areas of expertise to the HFE design and implementation process. This is not intended to define the total role of each area of expertise.

#### (1) Technical Project Management

- Minimum qualifications:
  - Bachelor's degree
  - 5 years of experience in nuclear power plant design or operations
  - 3 years of management experience
- Typical contributions:
  - develop and maintain the schedule for the HFE design process
  - provide a central point of contact for management of the HFE design and implementation process

#### (2) Systems Engineering

- Minimum qualifications:
  - Bachelor of Science degree
  - 4 years of cumulative experience in at least three of the following areas of systems engineering: design, development, integration, operation, and test and evaluation
- Typical contributions:

- provide knowledge of the purpose, operating characteristics, and technical specifications of major plant systems
- provide input to HFE analyses, especially function analysis and task analysis
- participate in the development of procedures and scenarios for task analysis, validation, and other analyses

#### (3) Nuclear Engineering

- Minimum qualifications:
  - Bachelor of Science degree
  - 4 years of nuclear design, development, test, or operations experience.
- Typical contributions:
  - provide knowledge of the processes involved in reactivity control and power generation
  - provide input to HFE analyses, especially function analysis and task analysis
  - participate in the development of scenarios for task analysis, validation, and other analyses

#### (4) Instrumentation and Control (I&C) Engineering

- Minimum qualifications:
  - Bachelor of Science degree
  - 4 years of experience in design of hardware and software aspects of process control systems
  - experience in at least one of the following areas of I&C engineering: development, power plant operations, and test and evaluation
  - familiarity with the theory and practice of software quality assurance and control
- Typical contributions:
  - provide detailed knowledge of the human-system interface (HSI) design, including



control and display hardware selection, design, functionality, and installation

- provide knowledge of information display design, content, and functionality
- participate in the design, development, test, and evaluation of the HSI
- participate in the development of scenarios for human reliability analysis (HRA), validation, and other analyses involving failures of the HSI data processing systems
- provide input to software quality assurance programs

#### (5) Architect Engineering

- Minimum qualifications:
  - Bachelor of Science degree
  - 4 years of experience in design of power plant control rooms
- Typical contributions:
  - provide knowledge of the overall structure of the plant including performance requirements, design constraints, and design characteristics of the following: containment building, control room, remote shutdown area, and local control stations
  - provide knowledge of the configuration of plant components within the plant
  - provide input to plant analyses, especially function analysis, task analysis, and the development of scenarios for task analysis and validation

#### (6) Human Factors Engineering

- Minimum qualifications:
  - Bachelor's degree in Human Factors Engineering, Engineering Psychology, or related science
  - 4 years of cumulative experience related to the human factors aspects of human-computer interfaces. Qualifying experience should include at least the following activities within the context of large-scale human-machine systems (e.g., process

control): design, development, and test and evaluation

- 4 years of cumulative experience related to the human factors aspects of workplace design. Qualifying experience should include at least two of the following activities: design, development, and test and evaluation.
- Typical contributions:
  - provide knowledge of human performance capabilities and limitations, applicable human factors design and evaluation practices, and human factors principles, guidelines, and standards
  - develop and perform human factors analyses and participate in the resolution of identified human factors problems

#### (7) Plant Operations

- Minimum qualifications:
  - has or has held a senior reactor operator license
  - 2 years of experience in relevant nuclear power plant operations
- Typical contributions:
  - provide knowledge of operational activities including task characteristics, HSI characteristics, environmental characteristics, and technical requirements related to operational activities
  - provide knowledge of operational activities in support of HSI activities such as development of HSI components, procedures, and training programs
  - participate in the development of scenarios for HRA evaluations, task analyses, HSI tests and evaluations, validation, and other evaluations

#### (8) Computer System Engineering

- Minimum qualifications:
  - Bachelor's degree in Electrical Engineering or Computer Science, or graduate degree in other engineering discipline (e.g., Mechanical Engineering or Chemical Engineering)

- 4 years of experience in the design of digital computer systems and real-time systems applications
- familiarity with the theory and practice of software quality assurance and control

- Typical contributions:

- provide knowledge of data processing associated with HSI displays and controls
- participate in the design and selection of computer-based equipment such as controls and displays
- participate in the development of scenarios for HRA, validation, and other analyses involving failures of the HSI data processing systems

#### (9) Plant Procedure Development

- Minimum qualifications:

- Bachelor's degree
- 4 years of experience in developing nuclear power plant operating procedures

- Typical contributions:

- provide knowledge of operational tasks and procedure formats, especially as presented in emergency procedure guidelines and operational procedures of current and predecessor plants
- participate in the development of scenarios for HRA evaluations, task analyses, HSI tests and evaluations, validation, and other evaluations
- provide input for the development of emergency operating procedures, procedure aids, computer-based procedures, and training systems

#### (10) Personnel Training

- Minimum qualifications:

- Bachelor's degree
- 4 years of experience in the development of personnel training programs for power plants

- experience in the application of systematic training development methods

- Typical contributions:

- develop content and format of personnel training programs for licensed and non-licensed plant personnel
- coordinate training issues arising from activities such as HRA, HSI design, and procedure design with the training program
- participate in the development of scenarios for HRA evaluations, task analyses, HSI tests and evaluations, validation, and other evaluations

#### (11) Systems Safety Engineering

- Minimum qualifications:

- Bachelor's degree in Science
- certification by the Board of Certified Safety Professionals in System Safety
- 4 years of experience in system safety engineering

- Typical contributions:

- identify safety concerns and perform a system safety hazard analysis
- provide results of system safety hazard analysis to probabilistic risk assessment/HRA and human factors analyses

#### (12) Maintainability/Inspectability Engineering

- Minimum qualifications:

- Bachelor's degree in Science
- 4 years of cumulative experience in at least two of the following areas of power plant maintainability and inspectability engineering activity: design, development, integration, and test and evaluation
- experience in analyzing and resolving plant system and/or equipment-related maintenance problems

- Typical contributions:

- provide knowledge of maintenance, inspection, and surveillance activities including task characteristics, HSI

characteristics, human performance demands, environmental characteristics, and technical requirements related to the conduct of these activities

- support the design, development, and evaluation of the control room and other HSI components throughout the plant to ensure that they can be inspected and maintained to the required level of reliability
- provide input in the areas of maintainability and inspectability to the development of procedures and training
- participate in the development of scenarios for HSI evaluations including task analyses, HSI design tests and evaluations, and validation

### (13) Reliability/Availability Engineering

- Minimum qualifications:
  - Bachelor's degree
  - 4 years of cumulative experience in at least two of the following areas of power plant reliability engineering activity: design, development, integration, and test and evaluation
  - knowledge of computer-based, human-interface systems
- Typical contributions:
  - provide knowledge of plant component and system reliability and availability and assessment methodologies to the HSI development activities
  - participate in human reliability analyses
  - participate in the development of scenarios for HSI evaluations, especially validation
  - provide input to the design of HSI equipment to ensure that it meets reliability goals during operation and maintains the required level of availability

The education and related professional experience of the HFE design team personnel should satisfy the minimum

qualification requirements specified above for each of the areas of expertise. Qualifying professional experience (e.g., design, development, analysis) for each area of expertise should be directly related to those technologies and techniques that will be used in the HFE design and implementation process.

The required professional experience is to be satisfied by the HFE design team as a collective whole. Therefore, satisfaction of the professional experience requirements associated with a particular skill area may be realized through the combination of the professional experience of two or more members of the HFE design team who each, individually, satisfy the other defined credentials of the particular skill area but who do not possess all of the specified professional experience. It is recognized that one person may possess multiple skills and that people may have additional responsibilities beyond the HFE design team.

Alternative personal credentials may be accepted as the basis for satisfying the minimum personal qualification requirements specified above. Acceptance of such alternative personal credentials should be evaluated on a case-by-case basis and approved, documented, and retained in auditable plant files by the combined operating license applicant. The following factors are examples of alternative credentials that may be considered acceptable:

- A Professional Engineer's license in the required skill area may be substituted for the required Bachelor's degree.
- Successful completion of all technical portions of an engineering, technology or related science baccalaureate program may be substituted for the Bachelor's degree. The successful completion will be determined by a transcript or other certification by an accredited institution. For example, completion of 80 semester credit hours may be substituted for the baccalaureate requirement. The courses should be in appropriate technical subjects relevant to the required skill areas of the HFE design team for which the individual will be responsible.
- Related experience may substitute for education at the rate of 6 semester credit hours for each year of experience up to a maximum of 60 credit hours.
- Where course work is related to job assignments, post-secondary education may be substituted for experience at the rate of 2 years of education for 1 year of experience. Total credit for post-secondary education should not exceed 2 years experience credit.



**Appendix B**

**Operating Experience Review Issues**

## APPENDIX B

### OPERATING EXPERIENCE REVIEW ISSUES\*

Many of the issues identified below are broad and involve system design considerations that are broader than human factors alone. However, each has a human factors component that should not be overlooked by the applicant during the design and implementation process. Thus, for each issue identified below, a brief explanation of the HFE aspects of the issue is provided. These explanations are examples only and are not intended to be a complete specification of the HFE components of the issue (which should be addressed by the applicant in the design-specific treatment of the issue). Each of the issues listed below should be addressed in the operating experience review (OER) as part of the applicant's design and implementation process.

The issues are organized into the following categories, based on the issue's source:

- (1) unresolved safety issues/generic safety issues (USIs/GSIs)
- (2) Three Mile Island (TMI) issues
- (3) NRC generic letters and information notices
- (4) Office for Analysis and Evaluation of Operational Data (AEOD) studies
- (5) low-power and shutdown issues
- (6) applicable operating plant event reports

#### B.1 USIs/GSIs

- (1) A-44, Station blackout—This is a large and significant issue with many human factors-related aspects, including controls, displays, training, and procedures.
- (2) A-47, Safety implications of control systems—This issue relates to the implications of failures of non-safety-related control systems and their interaction with control room operators.
- (3) B-17, Criteria for safety-related operator actions—This issue involves the development of a time criterion for safety-related operator actions including a determination of whether automatic actuation is required. This issue also concerns some current pressurized water reactor designs requiring manual operations to accomplish the switchover from the injection mode to the recirculation mode, after a loss-of-coolant accident (LOCA).
- (4) B-32, Ice effects on safety-related water supplies—The buildup of ice on service water intakes can occur gradually and can require improved instrumentation to allow operators to detect its occurrence before it causes system inoperability.
- (5) GI-2, Failure of protective devices on essential equipment—A large number of licensee event reports have noted the incapacitation of safety-related equipment because of the failure of protective devices such as fuses and circuit breakers. Operators are not always aware of the failure of the equipment because of the design of the instrumentation.
- (6) GI-23, Reactor coolant pump seal failures—This is a multifaceted issue, which includes a number of proposed resolutions. One subissue is the provision of adequate seal instrumentation to allow the operators to take corrective actions to prevent catastrophic failure of seals.
- (7) GI-51, Improving the reliability of open cycle service water (SW) systems—The buildup of clams, mussels, and corrosion products can cause the degradation of open cycle SW systems. Added instrumentation is one means of providing operators with the capability to monitor this buildup and take corrective action before loss of system functionality occurs.
- (8) GI-57, Effects of fire protection system actuation on safety-related equipment—This issue resulted from spurious and inadvertent actuations of fire protection systems, often caused by operator errors during testing or maintenance. Design of systems should prevent such errors to the extent possible.
- (9) GI-75, Generic implications of ATWS [anticipated transient without scram] events at the Salem Nuclear Power Plant—This issue has many subissues, several of which are related to human factors, for example, scram data for post-scram analysis, capability for post-maintenance testing of reactor protection system, and a specific subissue titled "Review of human factors issues."
- (10) GI-76, Instrumentation and control power interactions—This issue raises several concerns, including control and instrumentation faults that could blind or partially blind the operators to the status of the plant.

\*Full citations for referenced material are contained in Section 12.



- (11) GI-96, Residual heat removal (RHR) suction valve testing—The design of the RHR suction valves with respect to valve position indication and instrumentation to detect potential leakage from high-to-low pressure areas is important to the prevention of interfacing system loss-of-coolant accidents (ISLOCAs). This is important for normal operations and for testing.
- (12) GI-101, Break plus single failure in boiling water reactor (BWR) water level instrumentation—This issue attempts to ensure that robust information is available to the operators for both reactor water level and for plant status during the progression of an accident.
- (13) GI-105, Interfacing system LOCA at BWRs—This issue relates to pressure isolation valves for BWRs. Many failures in this area were due to personnel errors. The design should address human factors considerations to correct these potential errors. (NRC work in the ISLOCA area has generally shown that human factors is an area needing considerable attention and one that has contributed to a number of the ISLOCA precursor events.)
- (14) GI-110, Equipment protective devices of engineered safety features (ESFs)—Failures and incapacitation of ESF equipment have occurred because of the failure or intentional bypass of protective devices. Both the design of these protective devices and the appropriate indication to control room operators are important.
- (15) GI-116, Accident management—This issue relates to improved operator training and procedures for managing accidents beyond the design basis of the plant.
- (16) GI-117, Allowable equipment outage times for diverse, simultaneous equipment outages—A key aspect of this item is providing operators with needed assistance in identifying risk-significant combinations of equipment outages. The information needed would include valve alignments, switch settings, as well as components declared inoperable.
- (17) GI-120, Online testability of protection systems—The designs for online testability should include appropriate human factors to ensure safe testing.
- (18) GI-125.I.3, Safety parameter display system (SPDS) availability—This issue addresses SPDS availability and the reliability of the information it displays.
- (19) GI-128, Electrical power reliability—This issue includes power to vital instrument buses, dc power supplies, and electrical interlocks. All of these issues are strongly dependent on proper indication and operator action for high reliability.
- (20) GI-130, Essential service water pump failures at multiplant sites—This issue relates to the arrangement of SW pumps and piping, including cross-ties at multiunit sites. Both the arrangement and the operators' ability to monitor the status of cross ties are important. This item mentions potential applicability to single-unit sites also.
- (21) HF1.1, Shift staffing—This issue is similar to Item I.A.1.4. in Section B.2.
- (22) HF4.4, Guidelines for upgrading other procedures—This issue addresses normal and abnormal procedures in the same manner as emergency procedures.
- (23) HF4.5, Man-machine interface (MMI)—automation and artificial intelligence—See HF5.2 below.
- (24) HF5.1, Local control stations—This issue addresses the MMI of local control stations and auxiliary operator interfaces.
- (25) HF5.2, Review criteria for human factors aspects of advanced controls and instrumentation—This concern is a combination of HF 4.5, the original HF5.2 on annunciators, HF 5.3, and HF5.4.
- (26) HF5.3, MMI—evaluation of operational aids—This issue involves guidance on MMI for new display and control technologies.
- (27) HF5.4, MMI—computers and computer displays—See HF5.2 above.

## B.2 TMI Issues

The following issues come from two sources. Items 1-18 are from 10 CFR 50.34 and are identified by the item numbers from that source. The rest of the items are from NUREG-0933 (and its predecessor NUREG-0737) and are identified by the item numbers from the NUREG report. It should be noted that there is duplication in the content of some items; that is, a single OER item may address several of the TMI issues described below. The items are listed by number and not the technical issue that is addressed.

- (1) 1v, High-pressure coolant injection and reactor core isolation cooling separation—The design should consider control room alarm and indication of the initiation levels and low-level restart values.
- (2) 1vi, Reduction of challenges to safety/relief valves (SRVs)—The design should consider control room

- alarm and indication of SRV status and important parameters.
- (3) 1vii, Automatic depressurization system (ADS) study—Determination of the "optimum" ADS for elimination of manual activation should include consideration of the operator's need to monitor the system and an analysis of the time required for operators to perform manual backup if required.
  - (4) 1viii, Automatic restart of core spray and low-pressure coolant injection—This issue involves allocation-of-function considerations in terms of automatic restart of a system after manual stoppage by the operators. Considerations of whether automatic restart should be available, how it should be implemented, and what alarm and indications are needed in the control room are required.
  - (5) 1xi, Depressurization by means other than ADS—Consideration of depressurization will involve the provision of alarms and indication in the control room. Some methods may also require operator actions that should be subject to the full design and implementation process.
  - (6) 1xii, Alternate hydrogen control systems—The evaluation of design alternatives for hydrogen control systems should include the information needs of the operators to assess the conditions that would require system initiation and the degree of automation of the systems.
  - (7) 2iv, SPDS—The selection and display of important safety parameters and their integration into the overall design of the control room is a primary HFE issue.
  - (8) 2v, Automatic indication of bypassed and inoperable systems—Providing operators with the capability to monitor the status of automatic systems is an important function of the control room information display system and a component important to the maintenance of the operators' situation awareness.
  - (9) 2vi, Venting of noncondensable gases—Operator monitoring of the status of noncondensable gases in the reactor coolant system and having clear, unambiguous indication of the conditions under which gas release must be initiated should be evaluated for HFE design implications.
  - (10) 2xi, Direct indication of SRVs in control room—The alarming and indication of SRV status should be clear and unambiguous and should be evaluated for HFE design implications.
  - (11) 2xii, Auxiliary feedwater indication and initiation—The HFE aspects of providing indication and initiative for auxiliary feedwater should be evaluated.
  - (12) 2xvi, Number of actuation cycles for emergency core cooling system and reactor protection system—As part of the specification, allowable actuation cycles, the method by which cycles will be defined, recorded, and tracked by the operating crew, should be evaluated for HFE design implications.
  - (13) 2xvii, Control room instrumentation for various parameters—The selection and display of important parameters and their integration into the overall design of the control room is a primary HFE issue.
  - (14) 2xviii, Control room instrumentation for inadequate core cooling—The selection and display of important parameters and their integration into the overall design of the control room is a primary HFE issue.
  - (15) 2xix, Instrumentation for postaccident monitoring—The selection and display of important parameters and their integration into the overall design of the control room is a primary HFE issue.
  - (16) 2xxi, Auxiliary heat removal systems design to facilitate manual/automatic actions—The specification and evaluation of manual and automatic actions should be subject to the function allocation analyses performed as part of the design and implementation process.
  - (17) 2xxiv, Recording of reactor vessel level—The selection and display of important parameters and their integration into the overall design of the control room is a primary HFE issue.
  - (18) 2xxv, Technical support center (TSC), operational support center (OSC), and emergency offsite facility (EOF)—The design of the TSC, OSC, and EOF should include HFE considerations to ensure that the personnel located in these facilities can most effectively perform their safety-related functions. Poor HFE design of these facilities may interfere with the performance of operators in a well-designed control room.
  - (19) 2xxvii, Monitoring of implant and airborne radiation—The selection and display of important parameters and their integration into the overall design of the control room is a primary HFE issue.
  - (20) 2xxviii, Control room habitability—While potential pathways for radioactivity to affect control room habitability may be identified and design solutions to preclude such problems may be developed, the control room operating crew should be aware of potential pathways. If warranted, evaluations of methods

to monitor in the control room the integrity of the design solutions and the presence of radiation in the pathways should be considered.

- (21) I.A.1.4, Long-term upgrading of operating personnel and staffing—This issue concerns shift staffing with licensed operators, and working hours of licensed operators. Updates to 10 CFR 50.54 were approved.
- (22) I.A.4.2, Simulator capabilities—This issue involves the improvement of the use of simulators in the training of operators.
- (23) I.C.1, Guidance for evaluation and development of procedures—This issue addresses normal, transient, and accident conditions to ensure that procedures are technically correct, explicit, and easily understood.
- (24) I.C.9, Long-term program for upgrading procedures—This issue includes emergency operating procedures with particular emphasis on diagnostic aids for off-normal conditions.
- (25) I.D.1, Control room design reviews—This issue addresses general control room design issues.
- (26) I.D.2, Plant safety parameter display system console—This issue addresses the need for the provision of an SPDS that displays a minimum set of parameters that define the safety status of the plant.
- (27) I.D.4, Control room design standard—This issue addresses the need for guidance on the design of control rooms to incorporate human factors considerations.
- (28) I.D.5.1, Control room design—improved instrumentation research alarms and displays—This issue involves the man-machine interface in the control room with regard to the use of lights, alarms, and annunciators to reduce the potential for operator error, information overload, unwanted distractions, and insufficient organization of information.
- (29) II.F.1 and II.F.2—These issues address detailed control room design issues related to instrumentation (II.F.1, "Additional accident monitoring instrumentation," and II.F.2, "Instrumentation for detection of inadequate corecooling").
- (30) II.K.1.5, Safety-related valve position description—This issue addresses direct indication of relief and safety valve position in the control room so that the alarming and indication valve status is clear and unambiguous should be evaluated for HFE design considerations.

- (31) II.K.1.10, Review and modify procedures for removing safety-related systems from service—This issue addresses procedures for ensuring that the operability status of safety-related systems is known.

### B.3 NRC Generic Letters and Information Notices

- (1) Generic Letter 91-06, Resolution of Generic Issue (GI) A-30, "Adequacy of Safety-Related DC Power Supplies," pursuant to 10 CFR 50.54(f). In this generic letter, NRC proposes certain monitoring, surveillance, and maintenance provisions for safety-related dc systems.
- (2) Generic Letter 91-07 GI-23, "Reactor Coolant Pump Seal Failures," and its possible effect on station blackout. This generic letter discusses the interaction between GI-23 and A-44, both of which have human factors aspects.
- (3) Generic Letter 91-11 Resolution of Generic Issues 48, "LCOs [Limiting Conditions for Operation] for Class 1E Vital Instrument Buses," and 49, "Interlocks and LCOs for Class 1E Tie Breakers," pursuant to 10 CFR 50.54(f). This generic letter addresses several issues related to electrical systems, including the reduction of human errors, control of equipment status, and testing.
- (4) Information Notice 93-47: Unrecognized Loss of Control Room Annunciators.
- (5) Information Notice 93-81: Implications of Engineering Expertise on Shift.

### B.4 AEOD Studies

The NRC's Office for Analysis and Evaluation of Operational Data (AEOD) conducted a program to identify human factors and human performance issues associated with operating events at nuclear power plants. The resulting reports have been summarized in NUREG-1275, Vol. 8, "Operating Experience Feedback Report - Human Performance in Operating Events" (J. Kaufman, G. Lanik, R. Spence, and E. Trager, 1992).

### B.5 Low-Power and Shutdown Issues

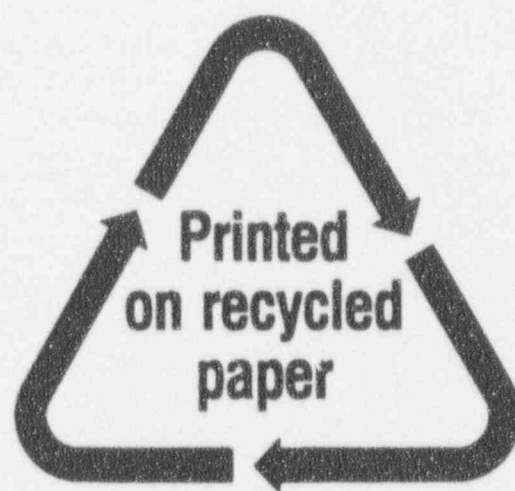
A current area of active NRC work is that of the risk associated with operation during low power and shutdown. The NRC has identified the operator-centered and human factors issues as particularly important in this area. The most current status of these issues is contained in NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," 1992.

## **B.6 Operating Plant Event Reports**

Reports of operating plants, such as licensee event reports (LERs) should be reviewed for operating experience issues applicable to advanced light water reactors.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202		U.S. NUCLEAR REGULATORY COMMISSION		1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Num- bers, if any.) <b>NUREG-0711</b>	
<b>BIBLIOGRAPHIC DATA SHEET</b> (See instructions on the reverse)					
2. TITLE AND SUBTITLE  Human Factors Engineering Program Review Model				3. DATE REPORT PUBLISHED	
				MONTH July	YEAR 1994
				4. FIN OR GRANT NUMBER	
5. AUTHOR(S)  John M. O'Hara, BNL, James C. Higgins, BNL, William F. Stubler, BNL, Clare Goodman, NRC, Richard J. Eckenrode, NRC, James P. Bongarra, NRC and Greg S. Galletti, NRC.				6. TYPE OF REPORT Human Factors Review Criteria	
7. PERIOD COVERED (Inclusive Dates)					
8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)  <div style="display: flex; justify-content: space-between;"> <div>           Division of Reactor Controls and Human Factors            Office of Nuclear Reactor Regulation            U.S. Nuclear Regulatory Commission            Washington, D.C. 20555-0001         </div> <div>           Brookhaven National Laboratory            Department of Advanced Technology            Upton, NY 11973-5000         </div> </div>					
9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)  Same as 8 above.					
10. SUPPLEMENTARY NOTES					
11. ABSTRACT (200 words or less)  The staff of the Nuclear Regulatory Commission is performing nuclear power plant design certification reviews based on a design process plan that describes the human factors engineering (HFE) program elements that are necessary and sufficient to develop an acceptable detailed design specification and an acceptable implemented design. There are two principal reasons for this approach. First, the initial design certification applications submitted for staff review did not include detailed design information. Second, since human performance literature and industry experiences have shown that many significant human factors issues arise early in the design process, review of the design process activities and results is important to the evaluation of an overall design. However, current regulations and guidance documents do not address the criteria for design process review. Therefore, the HFE Program Review Model (HFE PRM) was developed as a basis for performing design certification reviews that include design process evaluations as well as review of the final design. A central tenet of the HFE PRM is that the HFE aspects of the plant should be developed, designed, and evaluated on the basis of a structured top-down system analysis using accepted HFE principles. The HFE PRM consists of ten component elements. Each element is divided into four sections: Background, Objective, Applicant Submittals, and Review Criteria. This report describes the development of the HFE PRM and gives a detailed description of each HFE review element.					
12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)  Human factors, Human factors engineering, Human factors evaluation, Human factors review criteria, Nuclear safety, Safety review, Design certification, Design review, Design process, Human-system interface, Man-machine interface, Verification and validation				13. AVAILABILITY STATEMENT Unlimited	
				14. SECURITY CLASSIFICATION (This Page) Unclassified (This Report) Unlimited	
				15. NUMBER OF PAGES	
				16. PRICE	





Federal Recycling Program



UNITED STATES  
NUCLEAR REGULATORY COMMISSION  
WASHINGTON, D.C. 20555-0001

OFFICIAL BUSINESS  
PENALTY FOR PRIVATE USE, \$300

SPECIAL FOURTH-CLASS RATE  
POSTAGE AND FEES PAID  
USNRC  
PERMIT NO. G-67

120555139531 1 1AN1RX19L11V  
US NRC-OADM  
DIV FOIA & PUBLICATIONS SVCS  
TPS-PDR-NUREG  
2WFN-6E7  
WASHINGTON DC 20555

Introduction

HFE Management

OER

Function Analysis

Task Analysis

Staffing

Human Reliability

HSI Design

Procedures

Training

V&V

References

Appendix A

Appendix B