SKI Report 2005:15

Research

Human Factors Engineering Plan for Reviewing Nuclear Plant Modernization Programs

John O'Hara
James Higgins

December 2004

ISSN 1104–1374
ISRN SKI-R-05/15-SE

SKI

SKI PERSPECTIVE

Background

Operational experience shows that changes and modifications at Nuclear Power Plants (NPP:s) may lead to safety significant events. On the other hand, modifications are necessary to ensure safety and economy at the NPP:s. It is important to create awareness and understanding of the potential safety impacts of large and small modifications. A modernization influences not only technical aspects but also the layout and design of the control room, teamwork, cognitive demands, procedures and training.

The Swedish Nuclear Power Inspectorate (SKI) reviews aspects of Man-Technology-Organization (MTO) of nuclear power plants involved in modernization of plant systems and control rooms. The purpose of an MTO review is to help ensure personnel and public safety by verifying that accepted MTO practices and guidelines are incorporated into the modernization program and into the nuclear plant design. The need for a generic review plan for the design process was initiated by the large modernization of Oskarshamn 1 as well as plans for large modernizations at other plants.

Purpose

This research was initiated to demonstrate which, and to what depth, MTO aspects should be reviewed during a modernization of an old plant. The purpose of this study was to establish a frame of reference of what MTO aspects are important to review in a modernization program. This review plan was developed for safety reviews of large modernization programs but can be suited to fit modifications that involve any changes to human system interfaces. Depending on the extent of the modernization, the expected depth of the work within the different elements could vary. The depth of the review of a modernization program is decided when SKI makes a review plan of the program.

Even though the purpose of the research was primarily to support SKI in safety reviews of MTO aspects in modernization programs; it could also be used as a brief guide within a modernization program or as a guide in the utilities' own safety review.

Results

The research report *"Human factors engineering plan for reviewing nuclear plant modernization programs"* has been developed. It originates from NUREG-0711 *"Human factors engineering program review model"*, which was modified to incorporate SKI regulatory requirements and to focus on the unique considerations related to plant modifications.

The following report includes eleven different elements that should be included in a modernization program; human factors engineering program management, operating experience review, functional requirements analysis and functional allocation, task analysis, staffing, human reliability analysis, human-system interface design, procedure development,

training program development, human factors verification and validation and design implementation.
The elements include background, objective, expected licensee submittals, review criteria and references.

In the report SKI considers the term *human factors engineering* (HFE) as equal to the Swedish term MTO.

Continued work

SKI is further developing our regulatory strategy for large projects, including modernization programs. The plan is to review modernization programs in phases, starting with the plan of the modernization, ending with follow ups of the issues from the V&V results and of the implementation. Our next step will be to develop review criteria for the different phases.

Effects on SKI regulative work

The results give emphasis to the importance of the field and a better knowledge of the different areas that need to be considered during a modernization. The study will support the present and developing review strategy regarding modernization programs and will be used as a basis for reviews of MTO aspects.

Project information

Responsible for the project at SKI has been Anna Maria Östlund.
SKI reference: 14.3-040139, 14.3-001096/00226

SKI Report 2005:15

Research

Human Factors Engineering Plan for Reviewing Nuclear Plant Modernization Programs

John O'Hara
James Higgins

Brookhaven National Laboratory
Environmental and Systems Engineering Division
Upton, New York 11973
USA

December 2004

ABSTRACT

The Swedish Nuclear Power Inspectorate (SKI) reviews the human factors engineering (HFE) aspects of nuclear power plants (NPPs) involved in the modernization of the plant systems and control rooms.

The purpose of a HFE review is to help ensure personnel and public safety by verifying that accepted HFE practices and guidelines are incorporated into the program and nuclear power plant design. Such a review helps to ensure the HFE aspects of an NPP are developed, designed, and evaluated on the basis of a structured top-down system analysis using accepted HFE principles. The review addresses eleven HFE elements: HFE Program Management, Operating Experience Review, Functional Requirements Analysis and Allocation, Task Analysis, Staffing, Human Reliability Analysis, Human-System Interface Design, Procedure Development, Training Program Development, Human Factors Verification and Validation, and Design Implementation.

ACKNOWLEDGMENTS

Brookhaven National Laboratory would like to thank the following SKI personnel for all their guidance and assistance in developing this report: Anna Maria Ostlund, Pia Jacobsson, Gerd Svensson, and Klas Idehag.

CONTENTS

FIGURES

TABLES

ACRONYMS

ATWS	anticipated transients without scram
CR	control room
EOF	emergency offsite facility
EOP	emergency operating procedure
FSE	functions, systems and equipment
GTG	generic technical guidance
HA	human action
HFE	human factors engineering
HRA	human reliability analysis
HSI	human-system interface
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
LCS	local control station
MMI	man-machine interface (same as HSI)
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission (in the United States)
OER	operating experience review
PIE	postulated initiating event
PSA	probabilistic safety assessment
PSF	performance shaping factor
SKI	Statens Kärnkraftinspektion
TSC	technical support center
V&V	verification and validation

1 INTRODUCTION

1.1 Background

Nuclear power plant (NPP) personnel play a vital role in the productive, efficient, and safe generation of electric power. Operators monitor and control plant systems and components to ensure their proper operation. Test and maintenance personnel help ensure that plant equipment is functioning properly and restore components when malfunctions occur. Personnel interact with the plant's systems and components through the human-system interfaces (HSIs). The HSI may be defined as the technology through which personnel interact with plant systems to perform their tasks. It includes resources such as alarms, displays, support systems, and controls. The HSI is made up of hardware and software components and is characterized in terms of its physical and functional characteristics. Personnel use of the HSI is influenced directly by (1) the organization of HSI components into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into workplaces (e.g., main control room, remote shutdown station, local control stations); and (3) the environmental conditions (e.g., radiation, temperature, humidity, ventilation, illumination, and noise).

Computer-based HSI technology is being integrated into plants as part of plant modernization programs leading to modifications to control rooms, remote shutdown facilities, and local panels. New digital systems often provide personnel with information they did not have with conventional systems. Improved instrumentation and signal validation techniques can help ensure that the information is more accurate, precise, and reliable. In addition, data processing techniques and the flexibility of computer-based information presentation offer designers with the ability to display information in ways that are much better suited to personnel tasks and information processing needs. These developments can result in improved power plant availability and safety through the avoidance of transients, forced outages, and unnecessary shutdowns. However, while advanced HSIs can greatly improve operator and plant performance, it is equally important to recognize that, if poorly designed and implemented, there is the potential to negatively impact human performance, create human errors, and reduce human reliability.

The Swedish Nuclear Power Inspectorate (SKI) reviews the design and operations of nuclear power plants (NPPs) to ensure that they meet regulatory requirements and that they will perform as needed to reliably ensure plant safety. This process is called a "safety evaluation" and includes a review of the human factors engineering (HFE) aspects of plant design and operation.

The Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities (SKIFS) (SKI, 1998) provides the general requirements and guidance for the performing safety reviews. This document supports HFE safety evaluations by providing detailed criteria for conducting safety reviews. An initial version of this plan was developed using the Human Factors Engineering Program Review Model (NUREG-0711: NRC, 2002). The guidance in NUREG-0711 was modified to:

- incorporate SKIFS requirements for HFE
- focus on the unique considerations related to plant modifications

The initial version of the review plan was then used to review of the major instrumentation

and control (I&C) system and control room modernization program at Unit 1 of the Oskarshamn Nuclear Power Station. The plan was then updated based on lessons learned from the O1 review. This review plan does not introduce any new requirements.

1.2 General Description of the HFE Review Methodology

The purpose of a HFE review is to ensure safety by verifying that accepted HFE practices and guidelines are incorporated into the plant design. This review plan uses a top-down approach for the conduct of a safety evaluation of NPP modernization programs. Top-down refers to a review approach starting at the "top" with high-level plant mission goals that are divided into the functions necessary to achieve the mission goals. Functions are allocated to human and system resources and are divided 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 HSIs, procedures, and training are designed to support job task performance. The detailed design of the HSIs, 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.

An underlying principle of the methodology is that the HSIs, procedures, and training should be developed, designed, and evaluated on the basis of a structured top-down systems analysis using accepted HFE principles based on current HFE practices. The review process is organized into 11 elements reflecting five stages of development: planning, analysis, interface design, verification and validation, and design implementation. The review elements associated with each stage are:

Planning

- Element 1 - HFE Program Management
- Element 2 - Operating Experience Review
- Element 3 - Functional Requirements Analysis and Allocation
- Element 4 - Task Analysis
- Element 5 - Staffing and Qualifications
- Element 6 - Human Reliability Analysis

Design

- Element 7 - Human-System Interface Design
- Element 8 - Procedure Development
- Element 9 - Training Program Development

Verification and Validation

- Element 10 - Human Factors Verification and Validation

Implementation

- Element 11 - Design Implementation

Each review element is divided into four sections: Background, Objective, Licensee Submittals, and Review Criteria, and Reference Documents.

(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.

(3) *Licensee Submittals* - Licensees prepare many reports describing their activities related to the areas of review identified above. This review plan will help licensees to identify the most important documents since it more clearly identifies the areas of focus.

In addition to reports, the reviewers may obtain and review sample work products for various elements and implemented designs for the later elements.

(4) *Review Criteria* - This section contains the review criteria for the element, including applicable regulatory requirements from SKIFS.

(5) *Reference Documents* - HFE programs should be conducted and reviewed using accepted HFE practices as specified by applicable regulatory documents and HFE standards, and guidelines. Therefore, each of the 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:

- References include documents that are periodically updated, such as NUREG-0700. The reference contained in this report is to the latest version of the document at the time of its publication. The latest version of the document at the time of usage should be consulted.

- 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 an individual design review.

- There may be inconsistencies or contradictions within and between documents. Such conflicts should 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.

- Alternative approaches to those described in the referenced documents may be acceptable if they have a defensible rationale. Alternative approaches proposed by the licensee should be evaluated.

1.3 Tailoring the Plan

Modernization programs can differ significantly in their scope. Some involve many extensive changes to plant systems and HSIs such that there are changes to:

- the roles and responsibilities of crewmembers
- the means of performing tasks
- task demands (such as changes in time available to perform important tasks)

Other programs are less extensive and may involve only relatively small changes in the I&C such that operator tasks and HSIs are not substantially affected.

Between these two endpoints, is a continuum of the types of changes that licensees can perform.

The review methodology presented in this document is oriented to modernization programs of significant scope, such as the first described above. It thus provides a comprehensive, detailed HFE evaluation.

When this plan is used to review a less extensive modernization program, the level of detail in the plan should be tailored to reflect the unique circumstances of scope of the modification. The reviewer needs to consider the types of changes that are being made and what aspects of human performance they may impact. For example, if only relatively small changes in underlying I&C are planned such that operator tasks and HSIs are not substantially changed, then the elements of function allocation and task analysis may not be applicable.

Table 1-1 provides guidance on how to select the review elements that are relevant to a specific modernization project. The table is in question format. A yes answer to a question means that the HFE review element should be included in the review plan.

Table 1-1 Selection HFE Review Elements for a Specific Review

HFE Element	Review Element is Included if the Plant Modification...
1: HFE Program Management	Is more than a very simple change, such as replacing an analog recorder with a digital recorder
2: Operating Experience Review	Is more than a very simple change, such as replacing an analog recorder with a digital recorder
3: Functional Requirements Analysis and Allocation	Affects the level of automation and the functions and tasks that personnel perform
4: Task Analysis	Changes the way in which tasks are performed or the task demands, e.g., less time is available
5: Staffing and Qualifications	Changes the overall staffing or the qualification requirements for personnel
6: Human Reliability Analysis	Impacts any task that is credited in the SAR or risk-important based on PRA criteria Creates new risk-important tasks as a result of the modification
7: Human-System Interface Design	Changes any HSI characteristics or functions
8: Procedure Development	Requires a change in plant procedures or the development of new procedures
9: Training Program Development	Changes personnel functions or tasks Introduces changes to the knowledge, skills, or abilities or plant personnel Changes teamwork, crew coordination, or supervision

10: HFE V&V • HSI Task Support Verification • HFE Design Verification • Integrated System Validation • Human Factors Issue Resolution Verification • Final Plant HFE/HSI Design Verification	Changes personnel functions or tasks Changes HSIs Is more than a very simple change Created HFE-related issues that have been tracked Changes have been made to HSIs or procedures
11: Design Implementation	Is more than a very simple change, such as replacing an analog recorder with a digital recorder

In addition to scope of the plant changes, risk importance should be taken into account when deciding which particular items to review and the depth of review necessary. If plant modifications do not impact the performance of safety functions, then a more limited, sampling review may be appropriate.

2 ELEMENT 1 - HFE PROGRAM MANAGEMENT

2.1 Background

The overall purpose of the HFE program review is to ensure that the licensee has integrated HFE into the plant modernization program. To accomplish this, a licensee should have an HFE program plan that is implemented by a qualified HFE design team. The term "HFE design team" generically refers to the primary organization or function within the organization that is responsible for HFE within the scope of the staff's review. 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 the HFE program management review is to ensure that:

- The Licensee's modernization program and its products meet the general HFE requirements for facility design and operation described in The Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities.

- The Licensee has integrated HFE into plant modernization development, design, and evaluation.

- The Licensee 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.

2.3 Licensee Submittals

The licensee should provide the following for a safety review: HFE program plan describing the licensee's HFE goals/objectives, technical program to accomplish the objectives, a system to track HFE issues, the HFE design team, and the management and organizational structure to allow the technical program to be accomplished.

2.4 Review Criteria

2.4.1 General HFE Program Goals and Scope

(1) The licensee of a nuclear facility shall:

- "establish documented guidelines for how safety shall be maintained at the facility as well as ensure that the personnel performing duties which are important to safety are well acquainted with the guidelines" (SKIFS 1998: Chapter 2 3§, Point 1, p. 3).

- "ensure that the activity carried out at the facility is controlled and developed with the support of a quality system which covers those activities which are of importance to safety" (SKIFS 1998: Chapter 2 3§, Point 2, p. 3).

- "ensure that decisions on safety-related issues are preceded by adequate investigation and consultation so that the issues are comprehensively examined" (SKIFS 1998: Chapter 2 3§, Point 3, p. 3).

- "ensure that the personnel is provided with the necessary conditions to carry out work in a safe manner" (SKIFS 1998: Chapter 2 3§, Point 6, p. 3).

(2) *Modernization Philosophy* – This philosophy will be reviewed to determine the licensee's approach to the introduction of new technologies and its desired effect on plant personnel.

(3) *HFE Program Goals and Objectives*

- The design solutions shall be adapted to the personnel's ability to manage, in a safe manner, the facility as well as the abnormal events, incidents, and accidents that can occur (SKIFS 1998: Chapter 3 3§, p. 5).

- The general objectives of the program should stem from the philosophy and should be stated in "human- centered" terms. As the HFE program develops, these goals should be defined and used as a basis for HFE test and evaluation activities. "The design solutions should be adapted to the functions and tasks that are to be carried out as well as to the possibilities and limitations of human beings" (SKIFS 1998: On Chapter 3 3§, p. 30).

(4) *Assumptions and Constraints* - 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. The design assumptions and constraints should be clearly identified.

(5) *Applicable Facilities* - The facilities impacted by modernization program should be identified, e.g., the main control room, emergency control room (or remote shutdown facility), technical support center (TSC), emergency operations facility (EOF), and local control stations (LCSs).

(6) *Applicable HSIs* - The HSIs impacted by the modernization program should be identified, including those impacting operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures).

(7) *Effects of Modifications on Personnel Performance* - The goals of the HFE program should address the need to consider the effects that the modification may have on the performance of personnel. The transition from the existing plant configuration to the modification configuration can pose demands on human performance that differ from either the initial or final configurations. Therefore, it should be planned so it places minimal demands for adapting to the change. The considerations should include the following:

- planning the installation to minimize disruptions to work
- coordinating training and procedure modifications with implementing the modification to ensure that both accurately reflect its characteristics.

- conducting training to maximize personnel's knowledge and skill with the new design before its implementation

(8) *Safety Review* - "A safety review shall determine or control that the applicable safety-related aspects of a specific issue have been taken into account and that appropriate safety-related requirements with respect to the design, function, organization and activities of a facility are met. The review shall be carried out systematically and shall be documented. A safety review shall be performed within the parts of a facility's organization which are responsible for the specific issues as well as within a safety review function appointed for this purpose which shall have an independent position relative to the parts of the organization which are responsible for the specific issues" (SKIFS 1998: Chapter 4 3§, pp. 5-6).

2.4.2 Program Management

(1) *Design Team*

- The design team should include HFE expertise (SKIFS 1998: On Chapter 3 §3, p. 31).

- Training needs and plans for addressing the team's familiarity with different human factors principles, techniques and guidelines, and methods should be identified.

- Plant personnel affected by the modernization program should participate in the design activities, including operations, maintenance, and engineering personnel. Specific methods should be identified describing how plant personnel will provide (or have provided) their knowledge and expertise to the design program.

- A major modernization program can involve activities by several vendors, contractors, and consulting organizations. Specific methods should be identified describing how licensee personnel oversee and manage the work of vendors and contractors involved in the modernization program. HFE requirements should be included in each contract and the contractor's compliance with HFE requirements should be periodically verified. The roles and responsibilities for each of the team members responsible for performing human factors work should be identified along with procedures to ensure consistency of the HFE work across HFE organizations.

- The interfaces between the HFE team and the other project groups should be identified.

(2) *HFE Documentation*

- "The quality system shall be kept up-to-date and documented in a quality manual or similar document. The routines and procedures necessary for the control of those activities which are important to safety shall be added to the document" (SKIFS 1998: Chapter 2 4§, Point 8, pp. 3-4).

- HFE documentation items should be identified and briefly described along with the procedures for retention and access. This should include: policies and procedures for human factors, standards and technical guides, and other basis documents. The documentation should also include timelines and milestones for the various HFE activities and any stop-points that may be needed.

(3) *Issues Tracking* - 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 plant modernization program. This tracking system should be maintained throughout the project and should document the resolution of issues. An existing licensee tracking system may be adapted to serve this purpose.

2.4.3 Technical Considerations

(1) The general development of implementation plans, analyses, and evaluation of the following should be identified and described:

- operating experience review
- functional requirements analysis and allocation
- task analysis
- staffing
- human reliability analysis
- HSI design
- procedure design
- training design
- human factors verification and validation
- design implementation

The methods and intended tools for addressing each of the elements should be identified. The criteria used for determining which HFE activities are included or excluded should be identified.

(2) The level of effort for each HFE activity should be identified along with its supporting rationale.

(3) The licensee shall:

- ensure that safety, through these and other measures, is maintained and continuously developed (SKIFS 1998: Chapter 2 3§, Point 8, p. 3)

- "the possibility of improving safety will be taken into account in every measure resulting in modifications to the facility or in the activities carried out. This particularly applies in the case of engineered modifications, modifications to operating conditions, organizational modifications and rationalizations" (SKIFS 1998: On Chapter 2 3§, Point 8, p. 29)

(4) The licensee should identify how "the consequences of a modification will be analyzed, so that an improvement in safety in one respect does not lead to a

deterioration in safety in another respect, in such a way that the level of safety as a whole is degraded" (SKIFS 1998: On Chapter 2 3§, Point 8, p. 29).

(5) The licensee should identify how "the design basis requirements will, to the appropriate extent, be taken into account during all design work, before a facility is taken into operation as well as in connection with later plant modifications" (SKIFS 1998: On Chapter 2 5§, p. 30).

(6) The licensee should identify how the impact of the modernization program on the following will be addressed:

- Safety analysis report
- "The technical specifications shall be kept up-to-date. Safety reviews in accordance with Chapter 4. 3§ shall be carried out for any modification or any planned temporary deviations from the Technical Specifications." (SKIFS 1998: Chapter 5 1§, p. 7)
- Design basis assumptions

(7) The licensee should ensure that defense-in-depth is not compromised (SKIFS 1998: Chapter 2 §2, p. 2). Defense-in-depth is one of the fundamental principles upon which the plant was designed and built. Defense-in-depth uses multiple means to accomplish safety functions and to prevent the release of radioactive materials. Defense-in-depth is important in accounting for uncertainties in equipment and human performance, and for ensuring some protection remains even in the face of significant breakdowns in particular areas. Defense-in-depth may be changed but should be maintained overall. Important aspects of defense-in-depth include:

- Defense in depth shall be achieved by: ensuring that the design, construction, operation, monitoring, and maintenance of a facility is such that abnormal events, incidents, and accidents are prevented (SKIFS 1998: Chapter 2 1§, p. 2)
- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- There is no over-reliance on programmatic activities to compensate for weaknesses in plant design. This may be pertinent to changes in credited human actions (HAs).
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers).
- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed. Caution should be exercised in crediting new HAs to assure that the possibility of significant common cause errors is not created.

- Independence of barriers is not degraded.

- Defenses against human errors are preserved. For example, establish procedures for a second check or independent verification for risk-important HAs to determine that they have been performed correctly.

- Safety margins are often used in deterministic analyses to account for uncertainty and to provide an added margin of assurance that the various limits or criteria important to safety are not violated. Such safety margins are typically not related to HAs, but the reviewer should take note to see if there are any that may apply to the particular case under review. It is also possible to add a safety margin (if desired) to the HA by demonstrating that the action can be performed within some time interval (or margin) that is less than the time identified by the analysis.

(8) Determine if IEC1226, *Nuclear Power Plants Instrumentation and Control Systems Important to Safety: Classification*, (or similar document) was used for the I&C design and whether its implementation should be reviewed for its HFE related implications. (The Appendix at the end of this document identifies some of the HFE implications of IEC 1226).

2.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities.

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

IEC 1226: *Nuclear Power Plants – Instrumentation and Control Systems Important for Safety – Classification,* 1993 [International Electrochemical Commission (Bureau Central de la Commission Electotechnique Internationale)].

International Standards Organization (2000). *Ergonomic Design of Control Centres -- Part 1: Principles for the Design of Control Centres* (ISO 11064-1). Geneva, Switzerland: International Standards Organization.

NRC (2002). *Human System Interface Design Review Guidelines* (NUREG-0700). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (2002). *Human Factors Engineering Program Review Model* (NUREG-0711). Washington, DC: U.S. Nuclear Regulatory Commission.

3 ELEMENT 2 - OPERATING EXPERIENCE REVIEW

3.1 Background

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 similar 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. For plant upgrades, it is important to consider both plant specific and industry-wide operating experience. The issues and positive 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, negative features encountered in previous designs can be identified and analyzed so that they are avoided in the development of the current system and positive features can be retained.

Thus, OER information contributes to other review elements. These inputs are summarized in Table 3-1. As indicated in the table, OER can contribute to review as well as to system design. 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
Task Analysis, Human Reliability Analysis, and Staffing	• Risk-important human actions and errors • Problematic operations and tasks • Staffing shortfalls
Human-System Interface, Procedures, and Training Development	• Trade study evaluations • Potential design solutions • Potential design issues
Verification and Validation	• Tasks to be evaluated • Event and scenario selection • Performance measure selection • Issue resolution verification

The technical basis for including an OER element is founded in international and Swedish nuclear industry regulations, standards, and recommended practices. 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). Thus, OER is widely recognized as an activity important to safe and efficient plant design.

3.2 Objective

The objective of this review is to ensure that the licensee has identified and analyzed HFE-related problems and issues encountered during their history and in previous control rooms that are similar to the current design under review. These identified problems and issues should be addressed in the development of the current design. Positive features should be identified so they may be retained where appropriate.

3.3 Licensee Submittals

Licensee documents addressing operating experience should be identified.

3.4 Review Criteria

(1) "The licensee of a nuclear facility shall... ensure that experience from the facilities own and from similar activities is continuously utilized and communicated to the personnel concerned" (SKIFS 1998: Chapter 2, 3§, Point 7, p. 3).

(2) *Predecessor/Related Plants and Systems* - The review should include information pertaining to the human factors issues related to the licensee's own plant, any other plants with similar control rooms (CRs), and experience pertinent to the new HSI being installed.

(3) *Focus on Plant Modifications* - The scope of the OER should particularly be focused on plant modifications to provide information relevant to the plants' systems or HSIs that are being modified. It should address the operating experience of the plant that will be modified, including experiences with the systems that will be modified and with HSI technologies that are similar to those under consideration. Also, when operators and maintenance personnel are unfamiliar with the proposed technology, attention should be paid to the operating experience of other plants that already have the technology.

(4) *Recognized Industry HFE Issues* - Issues that have been raised by events and accidents at other plants in the industry should be addressed. The issues are organized into the following categories:

- Chernobyl issues (e.g., as described in IAEA Safety Series INSAG-7, The Chernobyl Accident: Updating of INSAG-1).
- TMI issues (e.g., as described in NUREG - 0737 and in 10 CFR 50.34 (f), *Additional TMI related requirements*
- issues related to low power and shutdown operations

(5) Swedish operating plant event reports.

(6) *Operational Event Evaluation:*

- Events which have occurred and conditions which are detected and are important to safety, shall be investigated in a systematic manner in order to determine sequences and causes as well as in order to establish the measures required to restore the safety margins and to prevent reccurance. The results of the investigations shall be disseminated within the organization as well as shall contribute to the development of safety at the facility. The results shall be reported to the Swedish Nuclear Power Inspectorate in accordance with the provisions of Chapter 7.1**§ (**SKIFS 1998: 5 6**§, p. 8**).

- "... all such events and conditions should be systematically investigated so that the entire event sequence is clarified, including the circumstances which could have prevented or stopped the sequence, so that the consequences are determined, so that the root causes are established with a high degree of probability as well as that well-founded measures are specified to prevent similar events or conditions from recurring. .... The investigation methodology should be such that all aspects and circumstances are taken into account, including those relating to the man-technology-organization interaction (human factors)" (SKIFS 1998: On Chapter 5 6§, p. 39).

(7) *Related HSI Technology* - The OER should address related HSI technology. Emphasis should be given to HFE issues associated with the use of new HSI's planned for implementation at the plant such as, large screen displays and advanced alarm systems.

(8) *Issues Identified by Plant Personnel* - "Experience from the facility in question and from the personnel should be taken advantage of at an early stage" (SKIFS 1998: On Chapter 3 3§, pp 30-31). Issues identified by operators should be documented and the disposition/-resolution should be noted. The following topics, as a minimum, should be addressed by operator input:

- Plant Operations
  - normal plant evolutions (e.g., startup, full power, and shutdown)
  - HSI equipment and processing failure (e.g., loss of video display units, and loss of data processing)
  - 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 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 (ATWS), and various-sized loss-of-coolant accidents)

- HFE 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

(9) *Risk-Important Tasks* - The OER should identify, risk-important, human actions that are identified in the Probabilistic Safety Assessment (PSA) and that have been prone to error. These human actions should receive special attention during the design of the user interface to lessen their probability of failure.

(10) *Procedures and documentation* – The licensee should describe their procedures for conducting operating experience review.

- "Efficient procedures should exist for continuous experience feedback within all of the parts of the organization carrying out tasks which are of importance for safety" (SKIFS 1998: On Chapter 2 3§, Point 7, pp 28-29).

- "The possibility of improving safety should be taken into account in every measure resulting in modifications to the facility or in the activities carried out" (SKIFS 1998: On Chapter 2 3§, Point 8, p. 29).

- The OER issues should be analyzed with regard to the identification of human performance issues, and design elements that support and enhance human performance. Each operating experience issue determined to be appropriate for incorporation in the design (but not already addressed in the design) should be documented in an appropriate plant tracking system.

3.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities

SKIFS 2000:1, *Swedish Nuclear Power Inspectorate's Regulations concerning the Competence of Operations Personnel at Reactor Facilities*

10 CFR 50.34 (f), *Additional TMI related requirements*, U.S. Code of Federal Regulations, Part 50

IAEA Safety Series INSAG-7, *The Chernobyl Accident: Updating of INSAG-1*

NUREG-0737, *Clarification of TMI Action Plan Requirements*, November, 1980

NUREG/CR-6400, *Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience*, J. Higgins and K. Nasta, 1996

4 ELEMENT 3—FUNCTIONAL REQUIREMENTS ANALYSIS AND FUNCTIONAL ALLOCATION

4.1 Background

Plant modernization programs can change the way functions and responsibilities are allocated to personnel and system resources. New systems provide the opportunity to automate process functions that previously were the responsibility of plant personnel. In addition, computer-based systems provide the opportunity to automate various cognitive functions, such as with computerized procedures. These changes in automation can impact the role of plant personnel, as well as significantly affect individual and team performance.

The purpose of the Element 3 review is to ensure the changes in the function allocations resulting from new plant systems and new HSIs take advantage of human strengths and avoid allocating functions that would be negatively affected by human limitations. This is examined in two steps: functional requirements analysis and function allocation (assignment of levels of automation such as manual, automatic, or a combination of the two).

4.2 Objective

The objective of this review is to ensure that the licensee has evaluated any changes in safety functions or the allocations of functions to personnel and system resources. If there are changes as the result of new systems or new HSIs, then the review will address whether the licensee has (1) adequately analyzed the changes in the plant's safety functional requirements, and (2) that the functions have been allocated to support an acceptable role for plant personnel; i.e., the allocations take advantage of human strengths and avoid allocating functions that would be negatively affected by human limitations.

4.3 Licensee Submittals

Licensee documents addressing functional requirements analysis and functional allocation should be identified.

4.4 Review Criteria

(1) "The design solutions shall be adapted to the personnel’s ability to, in a safe manner, manage the facility as well as the abnormal events, incidents and accidents which can occur" (SKIFS 1998 Chapter 3 3§, p. 5).

(2) Changes to existing plant safety functions or the introduction of new functions are usually not the case but are important if being implemented and should be identified. For each safety function impacted by the modernization program, the set of plant system configurations or success paths that are responsible for or capable of carrying out the function should be clearly defined.

(3) Modifications that change operator tasks (e.g., they are now automated) or task demands (e.g., less time to perform a task is now available) should be identified.

(4) Function decomposition should start at "top-level" functions where a very general picture of major functions is described, and continue to lower levels until a specific critical end-item requirement emerges (e.g., a piece of equipment, software, or an operator). A description should be provided for each new or changed function that includes:

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

(5) Function allocation should be performed using a structured, documented methodology reflecting HFE principles. An example functional allocation process and considerations is shown in Figure 4-1.

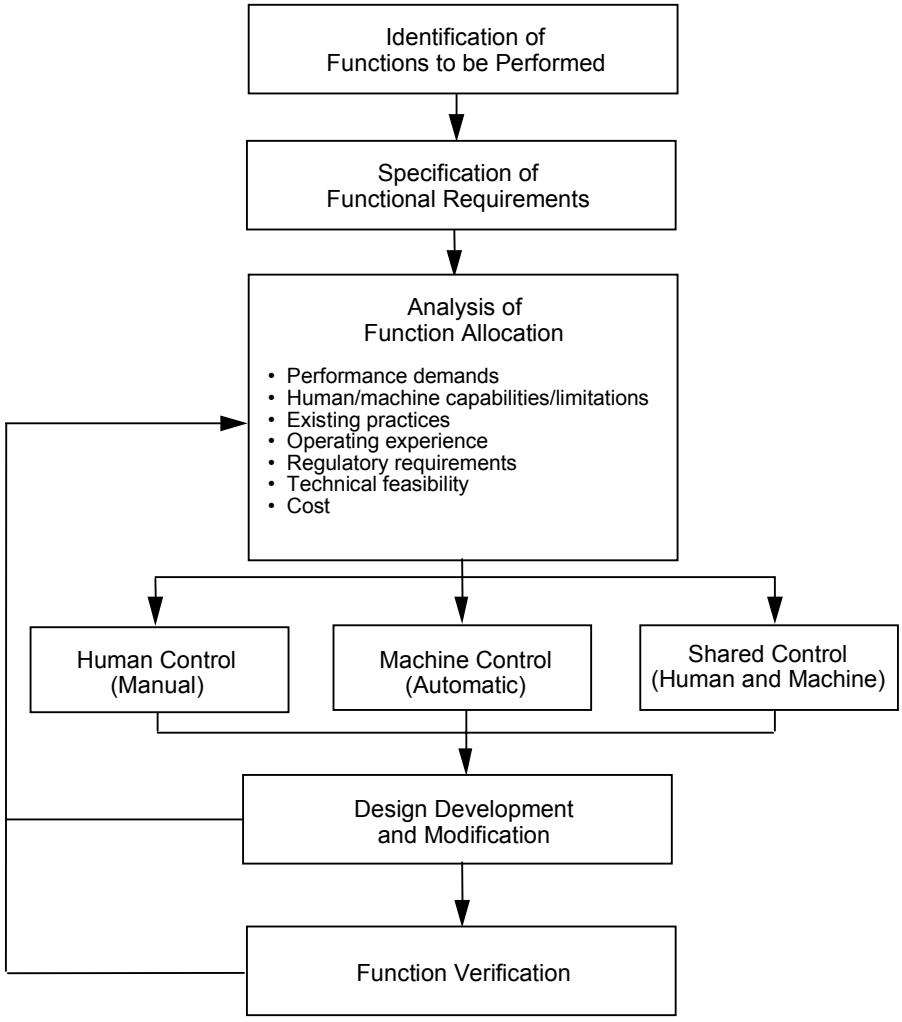

Figure 4-1 Allocation of Functions to Human and Machine Resources

(6) The technical basis for all functional allocations should be documented, including the allocation criteria, rationale, and analyses method. The technical basis for functional allocation can be any one or combination of the evaluation factors.

(7) The licensee should provide a description of how the role of personnel has changed in terms of personnel responsibility and level of automation. It should include the requirement for personnel to monitor automatic functions and to assume manual control in the event of an automatic system failure.

4.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities

IAEA-TECDOC-668: *The Role of Automation and Humans in Nuclear Power Plants*, 1992 (International Atomic Energy Agency - International Working Group on NPP Control and Instrumentation).

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

NASA Technical Memo No. 103885: *Human-Centered Aircraft Automation: A Concept and Guidelines*, 1991 (NASA - C. Billings).

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

5 ELEMENT 4 - TASK ANALYSIS

5.1 Background

Task analysis is the evaluation of the functions to be performed by plant personnel in order to identify the specific tasks that need to be accomplished and defines their information, control and task-support requirements.

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 HFE activities; e.g., it forms the basis for:

- function allocation evaluation; that is, for examining the capability of plant personnel to accomplish tasks assigned to them
- staffing, qualifications, and job design
- HSIs, procedures, and training program design
- task-support verification criteria (see Element 10, HFE Verification and Validation)

5.2 Objective

The objective of this review is to ensure that the licensee's task analysis identifies (1) the specific tasks that are needed for function accomplishment and (2) the task information, control and task-support requirements.

5.3 Licensee Submittals

Licensee documents addressing task analysis should be identified.

5.4 Review Criteria

(1) "The design solutions shall be adapted to the personnel's ability to, in a safe manner, manage the facility as well as the abnormal events, incidents and accidents which can occur" (SKIFS 1998: Chapter 3 §3, p.5).

(2) Task analysis shall:

- "ensure that the personnel is provided with the necessary conditions to carry out work in a safe manner" (SKIFS 1998: Chapter 2 3§, Point 6, p.3)

- "ensure that adequate personnel is available with the necessary competence and of the suitability otherwise needed for those tasks which are of importance for safety as well as ensure that this is documented" (SKIFS 1998:Chapter 2 3§, Point 4, p. 3)

(3) "In order to analyze the need for personnel and the competence that is needed in the activity, a systematic method should be used. Such a method is normally based on analyses of the tasks which must be carried out in order to ensure that a high level of safety is maintained in the activity" (SKIFS 1998: On Chapter 2 3§, Point 4, p. 27).

(4) The scope of the tasks to be analyzed should include:

- all risk important tasks as identified in PSA & human reliability analysis (HRA) (see also Element 6, HRA)

- new tasks that have to be performed by personnel by the introduction of new systems and new HSIs

- tasks that have been significantly changed by the introduction of new systems and new HSIs

- tasks that have been reallocated from one staff member to another from the pre- to the post-modernization arrangement and which significantly change the responsibilities of the individual crew members.

(5) Any existing task analyses should be revised and updated to reflect requirements of the modification. The tasks analyses to be revised should include tasks involving the modification and its interactions with the rest of the plant. Maintenance, tests, inspections, and surveillances tasks related to the modification should also be included. Attention should be given to risk-important actions that are new or supported by new technologies (e.g., new capabilities for on-line maintenance).

(6) Task analyses should begin with a high-level level description of the task and break the task down into detailed descriptions of what personnel must do. Relationships between tasks should be identified. For each task the requirements for successful task performance should be identified. This includes: information, control, communications, and any other support needed. Where appropriate, the analyses should consider the requirements imposed by environmental factors such as protective clothing. Detailed task descriptions should address the appropriate task elements listed in Table 5-1.

(7) The contribution of the old HSIs (those that will be replaced as part of the modernization program) on task performance should be evaluated to provide a better understanding of how tasks have been performed. The analysis should identify the design characteristics of the existing HSIs that support the performance of experienced personnel (e.g., support high levels of performance during demanding situations). This can help assure that important task support functionality of the existing HSIs can be accommodated in the new HSI design. In addition, the task analysis should identify and examine adjustments made to the HSIs by users, such as notes and external memory-aids, which suggest that the users' needs may not be fully met by its current design.

(8) The task analysis results should provide input to the design of HSIs, procedures, and personnel training programs. It should identify information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls for human task accomplishment.

Table 5-1 Task Considerations

Task Elements	Example
Information Requirements	alarms and alerts parameters (units, precision, and accuracy) feedback needed to indicate adequacy of actions taken
Decision-making Requirements	decisions type (relative, absolute, probabilistic) evaluations to be performed
Response Requirements	type of action to be taken task frequency, tolerance and accuracy time available and temporal constraints (task ordering) physical position (stand, sit, squat, etc.) biomechanics - movements (lift, push, turn, pull, crank, etc.) - forces needed
Communication Requirements	personnel communication for monitoring information or control
Workload	cognitive physical overlap of task requirements (serial vs. parallel task elements)
Task Support Requirements	special and protective clothing job aids or reference materials needed tools and equipment needed
Workplace Factors	ingress and egress paths to the worksite workspace envelope needed by action taken typical and extreme environmental conditions, such as lighting, temp, noise
Situational and Performance Shaping Factors	stress reduced manning
Hazard Identification	identification of hazards involved, e.g., potential personal injury

5.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities

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

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

A Guide to Task Analysis (Kirwan and Ainsworth, 1992).

Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work (Vicente, 1999).

6 ELEMENT 5 - STAFFING

6.1 Background

Plant staffing and the assurance of qualified personnel is an important consideration throughout the design and validation process. Normal and minimum staffing levels should be clearly established as design goals early in the design process on the basis of experience with the previous operation of the plant being modified, and Government regulations.

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 licensee has analyzed the requirements for the normal and minimum number of personnel in a systematic manner that includes a thorough understanding of task requirements and applicable regulatory requirements.

6.3 Licensee Submittals

Licensee documents addressing staffing should be identified.

6.4 Review Criteria

(1) "The Licensee of a nuclear facility shall ensure that adequate personnel is available with the necessary competence and the suitability otherwise needed for those tasks which are of importance for safety as well as ensure that this is documented" (SKIFS 1998: Chapter 2 3§, Point 4, p. 3).

(2) "The Licensee of a nuclear facility shall ensure that responsibilities and authority are defined and documented with respect to personnel carrying out work which is important to safety" (SKIFS 1998: Chapter 2 3§, Point 5, p. 3)

(3) The staffing analysis should determine the impact of plant modifications on the number and qualifications 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.

(4) The staffing analysis should be iterative; that is, initial staffing goals should be reviewed and modified as the analyses associated with other elements are completed.

(5) Staffing should be modified, if necessary, to address the following issues:

- operational problems that resulted from staffing levels at prior to the modifications
- significant differences between the original and the new modified systems and CR
- changes to the roles of operators, as determined by the function analysis

- changes to operator response time and workload
- changes to operator communication and coordination
- 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 effect the use of advanced HSI technology
- demands resulting from the locations and use (especially concurrent use) of controls and displays, including the availability of plant information from individual operator workstations and group-view interfaces
- the requirements for coordinated actions between individual operators
- the physical configuration of the control room and control consoles

(6) The staffing for operations personnel should meet the requirements and guidance of SKIFS 2000 and plant specific STFs, as follows.

- In order to hold a specific position, operations personnel must be authorized for that position. Authorizations are issued by the licensee (SKIFS 2000: 5§, p. 2).
- An employee may, at the same time, be authorized for a maximum of two different positions involving control room duties (SKIFS 2000: 6§, p. 3). When applying the provision concerning two positions, assistant shift supervisor or equivalent and shift supervisor may be counted as one position. - For example, within the framework of the authorization, a turbine operator should be able to carry out certain maneuvers in the reactor systems and a reactor operator should be authorized to conduct some of the shift supervisor's tasks if the supervisor is temporarily absent.
- Plant specific STF sections related to staffing.

(7) In the event that a formal staffing analysis has not been performed, the licensee and SKI should nonetheless verify certain aspects of shift staffing. This may occur when the plant has designed the new CR for the same staffing level as previously used. The plant should perform suitable testing verify that the numbers and the skills of the staff are adequate. This can be an acceptable alternative approach, provided that the licensee formally evaluates the staffing level as part of their V&V program and finds it acceptable.

Regarding the background of the personnel, the licensee should establish a plan for re-education and then evaluate the acceptability of training for the various new tasks (e.g., operations, maintenance, and surveillance testing) required of personnel in the modified control room.

6.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities

SKIFS 2000:1, Swedish Nuclear Power Inspectorate's Regulations concerning the Competence of Operations Personnel at Reactor Facilities

10 CFR 50.54, *Conditions of license*, (j) through (m), that address operations staffing, U.S. Code of Federal Regulations, Part 50, "Domestic Licensing of Production and Utilization Facilities."

10 CFR 50.47, *Emergency Plans, U.S. Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy."

ANSI/ANS 3.1-1993: *Selection, Qualification, and Training of Personnel for Nuclear Power Plants*, 1993 (American Nuclear Society).

Information Notice 95-48: Results of Shift Staffing Study, 1995 (NRC).

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).

7 ELEMENT 6 - HUMAN RELIABILITY ANALYSIS

7.1 Background

Human reliability analysis (HRA), as part of Probabilistic Safety Assessment (PSA), 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 qualitative and quantitative aspects, both of which are useful for HFE purposes. HRA should be conducted as an integrated activity in support of both HFE design activities and PSA activities. The PSA/HRA should be initially performed early in the design process to provide design insights and guidance both for systems design and for HFE purposes. HRA should be conducted as an integrated activity in support of both HFE design activities and PSA activities. Figure 7-1 illustrates the relationship between the PSA/HRA and the rest of the HFE program, including the concept of an initial PSA/HRA and then a final one at completion of design. 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.

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

Thus, there are important interfaces between the HFE program and risk analyses. A quality HRA is essential to both risk analysis and HFE design activities. The objective and criteria associated with this element are intended to ensure the acceptability of this activity.

7.2 Objective

The objective of this review are to ensure that (1) the licensee has addressed human error mechanisms in the design of 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, and (2) the HRA activity effectively integrates the HFE program activities and PSA/risk analysis activities.

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

7.3 Licensee Submittals

Licensee documents addressing HRA should be identified.

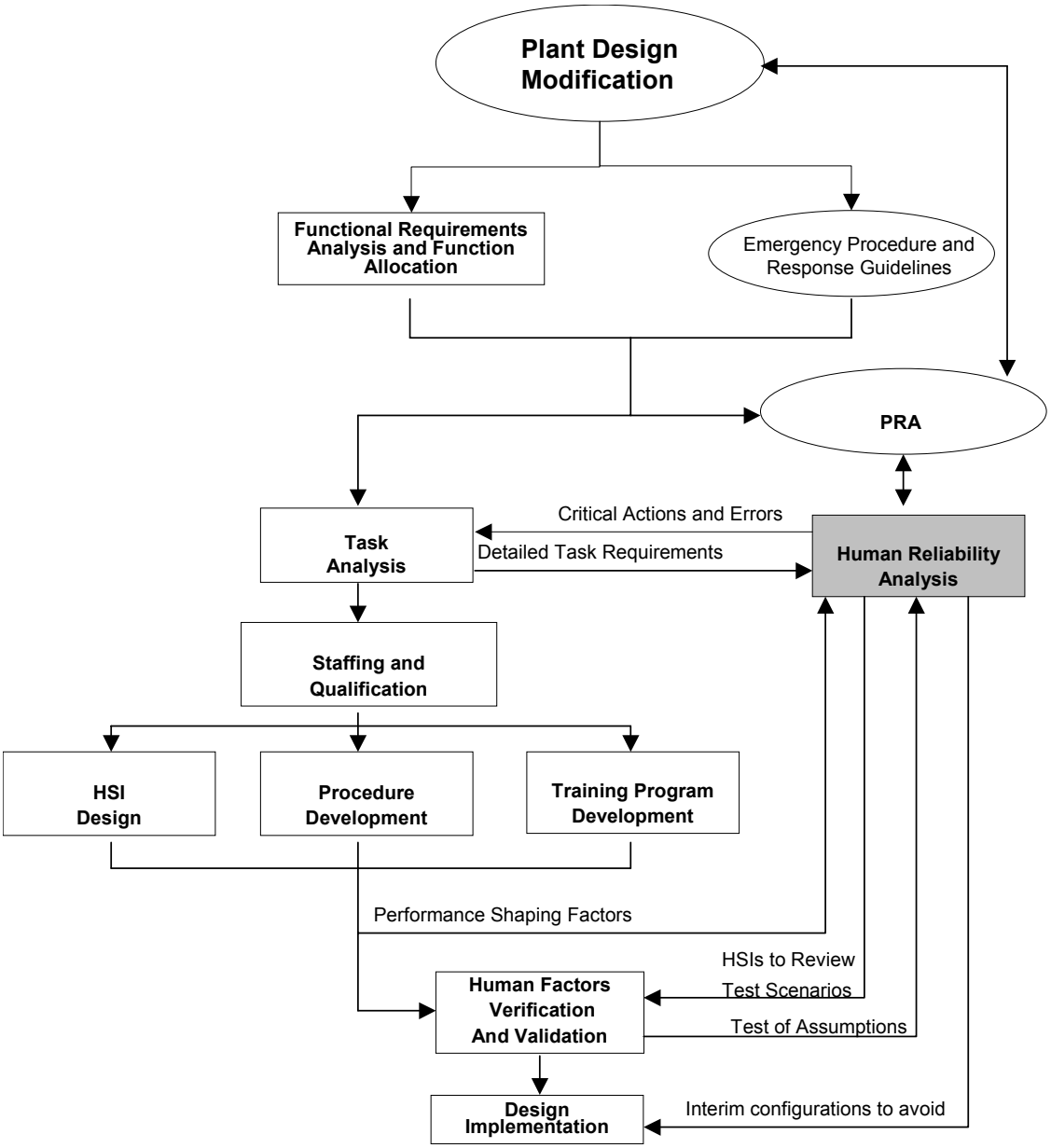

Figure 7-1 The Role of Human Reliability Analysis in the HFE Program

7.4 Review Criteria

(1) "Analyses of conditions which are of importance for the safety of a facility shall be carried out before a facility is constructed and taken into operation. The analyses shall subsequently be kept up-to-date. The safety analyses shall be based on a systematic inventory of such events, event sequences and conditions which can lead to a radiological accident" (SKIFS 1998: Chapter 4 1§, p. 5).

(2) "Both deterministic and probabilistic analyses should be used since they supplement each other and, in this way, provide as comprehensive a view as possible of risk and safety" (SKIFS 1998: On Chapter 4 1§, p. 31). The analyses should include operator error.

(3) If necessary, the PSA should be remodeled at account for plant/system/function changes created by the modernization program. This remodeling should incorporate new and changed human actions.

- The scope of the human-reliability analysis should address personnel actions resulting from the modification and its interactions with the rest of the plant.

- When upgrading plant systems or the HSIs and procedures, consideration should be given to the following effects of these modifications on the existing HRA:

  - Whether the original HRA assumptions are valid for the modified design
  - whether the human errors analyzed in the existing HRA are still relevant
  - whether the probability of errors by operators and maintenance personnel may change
  - whether errors may be introduced that are not modeled by the existing HRA and PSA
  - whether the consequences of errors, established in the existing HRA, may change

(4) Human actions should be quantified taking into account the new technology, teamwork, etc. that act as performance shaping factors (PSFs).

(5) Risk-important human actions should be identified from the PSA/HRA and used as input to the HFE design effort. These actions should be developed from both the Level 1 (core damage) PSA and Level 2 (release from containment) PSA including both internal and external events, as recommended by SKI (1998, p.33). The actions 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. If the modification involves new or existing human actions that are risk-important, then these actions should be re-examined as described in criterion (3), above, and addressed accordingly.

(6) Risk-important human actions that are identified by means of PSA/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.

(7) The use of PSA/HRA results by the HFE design team should be specifically addressed; that is, how are risk-important 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.

(8) HRA assumptions such as decision making and diagnosis strategies for dominant sequences should be validated by walkthrough analyses with personnel with operational experience using a plant-specific control room mockup or simulator. Reviews should be conducted before the final quantification stage of the PSA.

7.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities

IEEE Std. 1082-1997, "IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations."

NUREG/CR-6689: "Proposed Approach for Reviewing Changes to Risk-Important Human Actions," 2000 (Higgins, J. and O'Hara, J).

NUREG/CR-5319, *Risk Sensitivity to Human Error*, P. Samanta, S. Wong, S. Haber, W. Luckas, J. Higgins, and D. Crouch, April, 1989.

8 ELEMENT 7 - HUMAN-SYSTEM INTERFACE DESIGN

8.1 Background

The HSI design process represents the translation of function, task, and staffing requirements into HSI characteristics and functionality. HSIs should be designed using a structured methodology that guides designers in the identification of what how HSIs should be laid out in the control room (based on staffing and crew member responsibilities), how HSIs should be organized at workstations and other control room resources, and how to design the detailed characteristics and functions of the alarms, displays, controls, and support aids. The process should ensure standardization and consistency in the application of HFE principles.

8.2 Objective

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

8.3 Licensee Submittals

Licensee documents addressing HSI design should be identified. In addition to licensee documentation, an upgraded plant simulator may be used for the review of the HSI design characteristics and functions.

8.4 Review Criteria

8.4.1 HSI Design Inputs

(1) The following sources of information should provide input to the HSI design process:

- *Function analyses* - Levels of automation and manual control
- *Task analysis* - The set of requirements to support the role of personnel is provided by task analysis.
- *Staffing analyses* - The results of the staffing/qualifications and job analyses provide input for the layout of the HSIs between and within consoles, panels, and workstations.
- *Operational experience* - Lessons learned from other complex human-machine systems, especially predecessor designs and designs involving similar HSI technology should be used as an input to HSI design.
- *Other requirements* - The licensee should identify any other source of requirements such as those provided by a contractor or vendor, or those identified in appropriate standards and guidance documents as inputs to the HSI design.

(2) A concept of operations should be developed that reflects the modernization philosophy. It should address:

- The relationship between crew members and plant automation specifying the specific responsibilities of the crew for monitoring, interacting with, and overriding automatic systems.

- How crew members will work with HSI resources. Examples of information that should be identified are: the allocation of tasks to the main control room or local control stations, whether operators will work at a single large workstation or individual workstations, what types of information each crew member will have access to, and what types of information should be displayed to the entire crew.

- Coordination of crew member activities that impact plant operations, such as the interaction with auxiliary operators and coordination of maintenance and operations should be addressed.

(3) "The design solutions shall be adapted to the personnel's ability to, in a safe manner, manage the facility as well as the abnormal events, incidents and accidents which can occur" (SKIFS 1998: Chapter 3 3§, p.5).

- "Safety systems are designed so that there is enough time for consideration and time for executing the operator actions that affect the safety functions. Particular attention should be paid to the information and alarm systems of the control rooms." (SKIFS 1998: On Chapter 3 3§, p. 31)

- "The personnel should have access to the information that is necessary at different operating states without becoming overloaded by information during abnormal events, incidents, accidents or refueling outages." (SKIFS 1998: On Chapter 3 3§, p. 31)

- "The man-machine interface is designed in accordance with accepted ergonomic practice, so that the interface is compatible with human conditions as well as satisfy the need for interaction and communication during work." (SKIFS 1998: On Chapter 3 3§, p. 31)

- "The solutions that are developed should be evaluated in the context where they will be used." (SKIFS 1998: On Chapter 3 3§, p. 31)

(4) Functional requirements should be established for individual HSI types such as alarms, displays, controls, and operator aids.

(5) HFE guidelines should be utilized in the design of the general HSI features, layout, detailed design, and environment. The guidance should be tailored to reflect design decisions by the licensee to address specific goals and needs of the HSI design. This guidance should be documented in a Style Guide. The Style Guide should address consistency in design across old and new HSIs. Consistency with existing strategies can reduce the learning required for personnel to become proficient in using the modification. For example, introducing designs that require personnel to develop new strategies should be avoided, unless the new HSIs have significant benefits (i.e., the users should not be required to abandon existing skills and acquire new ones unless

the new methods provide distinct benefits, such as allowing the user to reach a higher level of performance).

8.4.2 HSI Detailed Design and Integration

(1) The HSI detailed design should support personnel in their primary role of monitoring and controlling the plant while minimizing personnel demands associated with use of the HSIs (e.g., window manipulation, display selection, and display system navigation).

(2) For risk-important actions, the design should seek to minimize the probability that errors will occur and maximize the probability that an error will be detected if one should be made.

(3) The layout of HSIs within consoles, panels, and workstations should be based upon (1) analyses of operator roles (job analysis) and (2) systematic strategies for organization such as arrangement by importance, frequency of use, and sequence of use.

(4) Personnel and task performance should be supported during minimal, nominal, and high-level staffing.

(5) The design process should take into account the use of the HSIs over the duration of a shift where decrements in performance due to fatigue may be a concern.

(6) HSI characteristics should support human performance under the full range of environmental conditions, e.g., normal as well as credible extreme conditions. For the main control room requirements should address conditions such as loss of lighting, loss of ventilation, and main control room evacuation. For the emergency control room (or remote shutdown facility) and for local control stations, requirements should address constraints imposed by the ambient environment (e.g., noise, temperature, and contamination) and by protective clothing (if necessary).

(7) The HSIs should be designed to support inspection, maintenance, test, and repair of plant equipment and the HSIs. The HSIs should be designed so that inspection, maintenance, test, and repair of the HSIs does not interfere with other plant control activities (e.g., maintenance tags should not block the operators' views of plant indications).

(8) Resolution of design conflicts should be documented to provide a reference for future modifications of the HSI design.

(9) Design requirements for computer-based HSI modifications should include requirements for crew coordination and define design characteristics for supporting coordination. These requirements should be derived from function and task analyses and should include communication and flexible allocation of tasks between crew members. If the proposed design may limit crew coordination, the design requirements should include features for overcoming these potential problems. Design characteristics that may limit crew coordination include features that limit the ability of personnel to have a shared view of plant information (e.g., decision-aids and

display devices that can only be accessed by one individual), maintain an awareness of others' actions, and communicate effectively with others from anticipated work locations. The design requirements should ensure that the HSIs are compatible with the organizational structure of the crew, and produces manageable levels of workload while ensuring plant safety.

(10) If the degree of integration between plant systems is changed, then design requirements should be developed to ensure that the HSIs support personnel in controlling these systems. For example, higher-level automation may bring together, under a single controller, systems that were formerly controlled separately.

(11) The following considerations should be addressed in the review of facilities supporting emergency preparedness:

- "Premises which are suitable for the purpose are premises which are equipped with the necessary communication equipment and other necessary aids, access routes, radiation protection and protection ventilation." (SKIFS 1998: On Chapter 5 5§, p. 38).

- "A reactor should also be equipped with a remote emergency control room from which it should be possible to monitor the critical parameters for safety, and from where it is possible to bring the facility to a safe and stable condition." (SKIFS 1998: On Chapter 5 5§, p. 38).

- "Technical systems are communication systems and a monitoring and sampling system that allows the state of the facility to be evaluated also during severe conditions. For example, this means that sampling can be carried out from radiation protected areas. The sampling equipment should be easy to maneuver and accessible also during severe conditions." (SKIFS 1998: On Chapter 5 5§, p. 38).

8.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities.

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

ANSI/AIAA G-035-1992: *Guide to Human Performance Measurements*, 1993 (ANSI).

BNL TR E2090-T4-4-12/94, Rev. 1: *Group-View Displays*, 1996 (W. Stubler and J. O'Hara).

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

ISO 11064-1: *Ergonomic Design of Control Centres -- Part 1: Principles for the Design of Control Centres,*2000 (International Standards Organization).

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

NUREG-0700: *Human-System Interface Design Review Guideline*, revised periodically (NRC).

NUREG/CR-6633: *Advanced Information Systems: Technical Basis and Human Factors Review Guidance*, 2000 (J. O'Hara, et al.).

NUREG/CR-6634: *Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance*, 2000 (J. O'Hara, et al.).

NUREG/CR-6635: *Soft Controls: Technical Basis and Human Factors Review Guidance*, 2000 (W. Stubler, et al.).

NUREG/CR-6636: *Maintenance of Digital Systems: Technical Basis and Human Factors Review Guidance*, 2000 (W. Stubler, et al.).

NUREG/CR-6637: *Human-System Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance*, 2000 (W. Stubler, et al.).

NUREG/CR-6684: *Advance alarm systems: Guidance development and technical basis*, 2000 (Brown, et al.)

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

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

9 ELEMENT 8 - PROCEDURE DEVELOPMENT

9.1 Background

Technically accurate and human-factored procedures are essential for safe plant operations should be derived from the same design process and analyses as the other aspects of the HSI (e.g., displays, controls, operator aids) and subject to the same evaluation processes. For modernization programs, procedure development should address all personnel tasks that are affected by the modification or its interactions with the rest of the plant. Procedures should be developed or modified to reflect the characteristics and functions of the modification. The same human factors analyses, such as task analysis, 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 HSIs during the Test and Evaluation stage and during the V & V stage. 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 procedure development program will result in procedures that support and guide human interaction with the new plant systems and the new CR in order to control plant-related events and accidents. 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 Licensee Submittals

Licensee documents addressing procedure development should be identified.

9.4 Review Criteria

(1) "A facility shall have suitable and documented procedures which shall state which measures shall be adopted during normal operation as well as during abnormal events, incidents and accidents. ... Safety review of these procedures shall be carried out in accordance with Chapter 4.3. The procedures shall be kept up-to-date. The personnel shall be well acquainted with the procedures." (SKIFS 1998: Chapter 5 2§, p. 7)

(2) The scope of the procedures addressed in this review is:

- generic technical guidance (GTG) for emergency operating procedures (EOPs)
- plant and system operations (including startup, power, and shutdown operations for modified/new systems)
- maintenance of modified/new systems and of CR equipment
- abnormal and emergency operations
- alarm response, both written hard-copy procedures and as part of the CR alarm system computer interface

- the maintenance work on systems and components should also be controlled by suitable procedures to the extent that it is important for safety. (SKIFS 1998: On Chapter 5 2§, p. 37).

(3) The basis for procedure changes should include

- plant design bases
- system-based technical requirements and specifications
- task analyses results
- risk-important human actions identified in the HRA/PSA
- initiating events to be considered in the EOPs, including those events in the design bases
- GTG for EOPs

(4) A procedure writer's 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 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. The guide should also note that users (operators) should participate in preparing and revising the procedures (SKIFS 1998: On Chapter 5 2§, p. 37).

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

- title and identifying information, such as number, revision, and date
- statement of applicability and purpose
- prerequisites
- precautions (including warnings, cautions, and notes)
- required human actions
- limitations and action statements
- acceptance criteria
- check-off lists
- reference material

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

(7) "In order to ensure that alarm and other initial measures in an accident situation can be implemented without delay, there should be adequate co-ordination between the emergency operating procedures of a facility and the alarm criteria which are established by the Swedish Radiation Protection Institute." (SKIFS 1998: On Chapter 5 4§, p. 37).

(8) "Efficient, in-house procedures should exist for decision-making concerning the summoning of emergency preparedness personnel and, to an adequate extent, checklists and procedures should be available as support to decision makers" (SKIFS 1998: On Chapter 5 4§, pp. 37-38).

(9) All procedures should be verified and validated. "The procedures should be technically correct and easy to use, even under the stressful conditions which can arise in reactor facilities. Thus, if possible and to the extent suitable, a simulator should be used to check the technical content of the procedures and whether they are suited to their purpose." (SKIFS 1998: On Chapter 5 2§, pp. 36-37). Thus, a review should be conducted to ensure they are correct and can be carried out. And, their final validation should be performed in a simulation of the integrated system as part of the verification and validation activities described in Element 10. Procedures should also be developed for temporary configurations of HSIs and plant systems that are used by operations or maintenance personnel. Temporary configurations sometimes occur when an extended period of time is needed for the completion of modifications to the HSIs or to plant systems.

(10) A plan for procedure maintenance and control of procedure updates should be verified to exist. Procedural modifications should be integrated across the full set of procedures; alterations in particular parts of the procedures should not conflict with each other or be inconsistent between the parts.

(11) The physical means by which operators access and use procedures, especially during operational events, should be evaluated as part of the CR and Emergency CR 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. It also applies to procedure use in the emergency CR. 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 CR, emergency CR and at local control stations.

9.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities.

NRC Regulatory Guide 1.33 (Rev. 2): *Quality Assurance Program Requirements*, 1978 (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, 1992 (NRC).

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

NUREG/CR-6634: *Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance*, 2000 (J. O'Hara, et al.).

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. NPPs modernizing with digital I&C and computer-based HSIs may impose demands on the knowledge, skills, and abilities of operations and maintenance personnel that are different from those posed by the old analog technology. These demands stem from differences in operator roles and responsibilities and differences in operator task characteristics resulting from advances in HSI and procedure technologies.

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 licensee has a systematic approach for the development of personnel training related to the changes in operations and maintenance tasks resulting from the modernization project. The development of training to address the new systems and HSIs should include the following five activities:

- a systematic analysis of tasks and jobs to be performed
- development of learning objectives derived from an analysis of desired performance following training
- design and implementation of training 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

10.3 Licensee Submittals

Licensee documents addressing training development should be identified.

10.4 Review Criteria

The review criteria are organized into the following general criteria: Organizational Aspects of Training, Scope, Learning Objectives, Content of Training Program, Evaluation of Training, and Periodic Re-training.

10.4.1 General

(1) The Licensee of a nuclear facility shall... "ensure that adequate personnel is (are) available with the necessary competence and the suitability otherwise needed for those tasks which are of importance for safety as well as ensure that this is documented" (SKIFS 1998: Chapter 2, 3§, Point 4, p.3).

(2) "In order to ensure the availability of personnel with adequate competence, competence and staffing plans should be prepared for several years in advance... In the

light of such analyses, staffing and competence requirements as well as training needs are analyzed. The training needs determine the preparation of training programmes and training materials" (SKIFS 1998: On Chapter 2 3§, Point 4, p. 27).

10.4.2 Organizational Aspects of Training

(1) The roles of all organizations, especially the plant and the 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. The qualifications of organizations and personnel involved in the development and conduct of training should be defined.

(2) Facilities and resources such as plant-referenced simulator and part-task training simulators required to satisfy training design requirements should be defined.

10.4.3 Scope

(1) 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)
- HSIs (e.g., in the main CR, emergency CR, emergency operations facility, and local control stations)

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

10.4.4 Learning Objectives

(1) The training program should be developed 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 all personnel whose actions may affect plant safety
- the full range of plant functions and systems including those that may be different from the old design
- the full range of plant conditions
- the full range of relevant HSIs (e.g., main CR, emergency CR, and local control stations) especially those that are modified

(2) Learning objectives for personnel training should address the changes, resulting from the plant modifications, to the knowledge and skill requirements associated with all relevant dimensions of the jobs of the plant personnel, such as interactions with the plant, the HSIs, and with other personnel. Table 10-1, below, illustrates how these basic dimensions can be addressed.

Table 10-1 Addressing Various Dimensions in a Training-Needs Assessment

Topic	Knowledge	Skill
Plant Interactions	Understanding of plant processes, systems, operational constraints, and failure modes.	Skills associated with monitoring and detection, situation awareness, response planning and implementation.
HSI Interactions	Understanding of HSI structure, functions, failure modes, and interface management tasks (actions, errors, and recovery strategies).	Skills associated with interface-management tasks.
Personnel Interactions (In the CR and in the plant)	Understanding information requirements of others, how actions must be coordinated with others, policies and constraints on crews' interaction.	Skills associated with crew's interactions (i.e., teamwork)

(3) The learning objectives should be derived from descriptions of desired performance after training. These analyses should include but not be limited to training issues identified in the following areas and elements:

- *Licensing Basis* - Learning objectives should be based on knowledge and skill requirements derived from the Final Safety Analysis Report, system description manuals, operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the staff as being important to training.

- *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, Task Analyses, and Staffing Analyses* - tasks identified during task analysis as posing unusual demands including risk-important tasks identified by PSA/HRA, new or different tasks, and tasks requiring high coordination, high workload, or special skills. The development of the training program should address all personnel tasks described above that are affected by the modification or its interactions with the rest of the plant. Any changes to personnel roles and responsibilities resulting from changes in staffing should also be addressed.

- *Human Reliability Assessment* - requirements for coordinating individual roles to reduce the likelihood and/or consequences of human error associated with risk-important human actions and the use of advanced technology

- *HSI Design* - design features whose purpose or operation may be different from past experience or past 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 for suitability verification validation
  - Operator performance concerns (e.g., misdiagnoses of plant event) identified during validation trials.

10.4.5 Content of Training Program

(1) Training design and implementation should be based on the learning objectives

(2) Operators should be trained in the use of effective strategies for: accessing and processing information provided by new HSIs; the presence of both new and old HSIs together; and rules for interpreting symptoms of failures of systems or the HSIs. This training should support personnel in acquiring new strategies, modifying existing ones, and eliminating inappropriate strategies. Additionally, "the procedures should be used on a regular basis in operator training" (SKIFS 1998: On Chapter 5 2§, p. 37).

(3) Team training should be addressed. This training should cover changes to teamwork skills that may result from the plant modifications. Groups of people who work together should be specifically trained in team-related tasks, including how individual roles are related, how the team's performance depends upon individual performances, and what makes the team's task different from the sum of individual ones.

(4) Since older HSIs are to be maintained along with new HSIs, which require different skills, the training program should ensure that personnel can maintain adequate levels of skill for both. This training should also provide skills for transitioning between the old and new components.

10.4.6 Evaluation of Training

(1) "In order to ensure that the personnel has adequate competence, a systematic competence follow-up should also be carried out ... In order to fulfill these aims, the follow-up should be conducted with explicit criteria regarding acceptable performance. " Therefore, methods for evaluating 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." (SKIFS 1998: On Chapter 2 3§, Point 4, p. 27)

(2) Methods for assessing overall proficiency should be defined and coordinated with regulations, where applicable.

- "The competence follow-up should, with regard to tasks of importance for safety, be carried out on an annual basis" (SKIFS 1998: On Chapter 2 3§, Point 4, p. 27).

- Ensure that the Training Program includes an evaluation of trainee mastery of the objectives during training.

(3) "The application, effectiveness and suitability of the system for training and competence evaluation of the operations personnel shall continuously be investigated by the licensee's quality assurance function in accordance with SKIFS 1998: 1 Chapter 2.4 § second paragraph" (SKIFS 2000: 9§, p. 3). This should be verified. Further the evaluation and revision of the training program should also be partially based on the performance of trained personnel in the job setting.

10.4.7 Periodic Re-training

(1) "Operations personnel undergo retraining every year for each position" (SKIFS 2000: 12§, p. 3). For control room personnel, "this should involve a minimum of ten days per year, of which five days using a full-scale simulator (SKIFS 2000: On 12§, p. 10). The following topics should be evaluated with respect to whether modifications to the periodic retraining program are warranted based on the plant changes resulting from the modernization program:

- handling of abnormal operating events and accidents

- co-operation, management and communication within the shift team and with other facility functions when handling various operational scenarios (this applies to control room personnel)

- technical or organizational modifications to the facility

- modifications of procedures and documents that affect facility operations

10.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities.

SKIFS 2000:1, Swedish Nuclear Power Inspectorate's Regulations Concerning the Competence of Operations Personnel at Reactor Facilities.

ANSI/ANS 3.1-1993: *Selection, Qualification, and Training of Personnel for Nuclear Power Plants*, 1993 (American Nuclear Society).

ANSI/ANS 3.5-1993: *Nuclear Power Plant Simulators for Use in Operator Training*, 1993 (American Nuclear Society).

Regulatory Guide 1.149: *Nuclear Power Plant Simulators for Use in Operator Training* (NRC).

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.

Five V&V 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 the HSIs are provided to address all identified personnel tasks
- *HFE Design Verification* - a check to determine whether the design of the HSIs 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
- *Final Plant HFE/HIS Design Verification* - The final product as built conforms to the verified and validated design that resulted from the HFE design process

The V&V evaluations should begin with HSI task support verification to identify missing or potentially unnecessary HSIs. Then, the HSIs should undergo HFE design verification to ensure the HSIs are acceptably designed according to HFE principles. Integrated system validation of the "final" HSI design should be performed on dynamic, high-fidelity representations 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 verifying that the "as built" design includes all design requirements identified through the 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 in the plant against the description.

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 Licensee Submittals

Licensee documents addressing V&V should be identified.

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

(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

However, portions of the V&V are performed in an iterative manner over the course of the design project, so a strict ordering is not always practical or desired.

11.4.2 HSI Task Support Verification

(1) All aspects of the HSIs (e.g., controls, displays, alarms, 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 risk-important actions of the PSA/HRA) should be verified as available through the HSIs.

(2) It should be verified that the HSIs do not include extraneous information, displays, controls, etc., that do not support operator tasks. This includes nonfunctional decorative details such as borders and shadowing on graphical displays.

(3) For modifications to plant systems that do not include modifications of the HSIs, task-support verification should identify any new demands for monitoring and control, and determine whether they are adequately addressed by the existing HSI design.

(4) Task-support verification should address configurations in which old HSIs are permanently deactivated, but not removed (e.g., abandoned in place). Criteria (2), above, states that the HSIs should not contain any information, displays, or controls that do not support the operator's tasks. This verification should identify deactivated HSIs that may have potentially negative effects on personnel's performance, such as obstructing the view of important information or adding visual clutter which may interfere with monitoring. Deactivated HSIs requiring further evaluation through HFE design verification or integrated system validation should be identified.

11.4.3 HFE Design Verification

(1) Aspects of the HSIs (e.g., controls, displays, alarms, procedures, and data processing) affected by the plant modernization program should be verified to be consistent with accepted HFE principles, standards, and guidelines.

(2) Deviations from accepted HFE principles, standards, and guidelines 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.

(3) When both old and new versions of similar HSIs are permanently present in design, this verification should ensure that their means of presentation and methods of operation are compatible, such that personnel performance will not be impaired when the use of old and new components is alternated.

11.4.4 Integrated System Validation

A number of different factors at work affect people's ability to function. These factors include: the layout of the workplace, equipment, job aids, the physical environment, how work is supervised and organized, procedures, communication with others, operators' workload, and working hours. Proper integrated system validation helps ensure that such testing and evaluations consider these factors.

(1) "Design principles and solutions shall be tested under conditions corresponding to those which can occur during the intended application in a facility" (SKIFS 1998: Chapter 3, 2§, p. 5).

(2) "The design solutions shall be adapted to the personnel's ability to, in a safe manner, manage the facility as well as the abnormal events, incidents and accidents which can occur" (SKIFS 1998: Chapter 3, 3§, p. 5).

(3) "Analyses of the man-technology-organization (human factors) should be carried out as well as recurrent evaluations performed" (SKIFS 1998: On Chapter 2 3§, Point 6, p. 28).

(4) An implementation plan for integrated system validation should provide sufficient detail to ensure that aspects of human performance important to safety are adequately addressed and that a process for examining and assessing these aspects has been adequately defined. The plan should reflect relevant human factors considerations associated with the following topics: validation team, test objectives, validation testbeds, plant personnel, operational conditions, performance measurement, test design, data analysis and interpretation, and development of validation conclusion. Figure 11-1 below illustrates the need for both a reliable testbed and a well-trained validation crew.

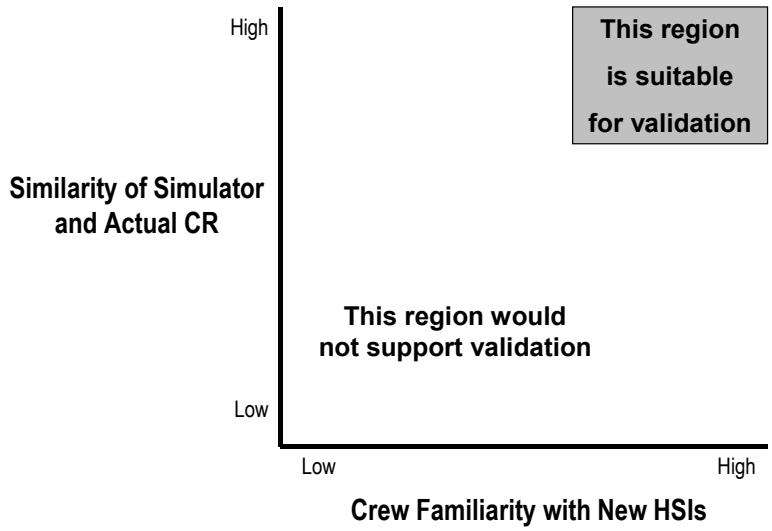

Figure 11-1 Validation as a function of crew familiarity with HSIs and similarity of HSIs in the simulator to the actual control room

(5) The evaluation of the integrated system validation should be conducted in accordance with the approved implementation plan.

(6) The results of the integrated system validation evaluation, as reported in the analysis results reports and the HFE design team evaluation report, should provide evidence that the integrated HSIs can be effectively operated by personnel within all performance requirements.

(7) All design requirements identified through the integrated system validation evaluation should be documented and all issues should be documented in the issue tracking system.

11.4.5 Human Factors Issue Resolution Verification

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

11.4.6 Final Plant HFE/HSI Design Verification

(1) Following V&V activities, a description should be developed of the detailed design and its performance criteria.

(2) Aspects of the design that were not addressed in 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 final (as-built in the plant) HSIs, procedures, and training should be compared with the detailed design description to verify that they conform to the design that resulted from the HFE design process and V&V activities. Any identified discrepancies should be corrected or justified.

11.5 Reference Documents

SKIFS 1998:1, Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilities.

SKI 99:10: *Verification and Validation of Human Factors Issues in Control Room Design and Upgrades*, 1999 (Green and Collier).

ANSI/AIAA G-035-1992: *Guide to Human Performance Measurements*, 1993 (ANSI).

Handbook of Validation of Control Room Upgrades (Report No. 1738), 1998 (Bladh, K., Borg, A., Eveneus, P.).

IEC 1771: *Nuclear Power Plants Main Control Rooms--Verification and Validation of Design*, 1995 (IEC).

NUREG-0700: Human-System Interface Design Review Guideline, revised periodically (NRC).

NUREG/CR-6393: *Integrated System Validation: Methodology and Review Criteria*, 1997 (J. O'Hara et al.)

12 ELEMENT 11 – DESIGN IMPLEMENTATION

12.1 Background

Plant systems and HSI modifications may be installed in the plant using many different methods, such as:

- Modifications made during one extended outage, where old equipment is removed and the new equipment is installed. When the plant starts up, the crew uses the new HSIs.

- Modifications made during several normal (or slightly extended) outages where during each outage some old equipment is removed and the new corresponding equipment is installed. When the plant starts up, the crew uses both the new HSIs and some old HSIs. The plant is thus in a temporary interim configuration until the final outage where the installation of new equipment is completed.

- Modifications made during one or more outages where new equipment is installed and the old corresponding equipment is left operational. When the plant starts up, both old and new HSIs are functional.

There are advantages and disadvantages to each approach.

12.2 Objective

The objective of this review is to ensure that licensee's implementation of the modernized plant systems and HSIs considers the impact of the implementation method on crew performance and provides the necessary support to ensure safe operations.

12.3 Licensee Submittals

Licensee documents addressing design implementation should be identified.

12.4 Review Criteria

(1) The licensee should ensure that the reactor fuel is safety monitored during the shutdown time period while the physical modifications are being implemented in the control room.

(2) Operations and maintenance crews should be fully trained and qualified to operate and maintain the plant with respect to all modifications prior to starting-up with the new systems and HSIs in place.

(3) The licensee should have a plan in place to monitor the initial phase of startup to ensure that:

- Operational and maintenance problems that arise with personnel interactions with the new systems and HSIs are identified and addressed

- Personnel are sufficiently familiar with the new systems and HSIs to support safe operations and maintenance

- Any negative transfer of training from the old removed HSIs to the corresponding new HSIs is identified and corrected

- No new problems are created based on coordination of tasks between the remaining old HSIs and new HSIs

- No unanticipated negative effects on crew interaction and teamwork arise.

12.5 Reference Documents

IEC 62096 *Nuclear Power Plants – Instrumentation and Control: Guidance for the Decision on Modernization*, 2001 (IEC).

13 REFERENCES

SKIFS 1998:1, *Swedish Nuclear Power Inspectorate's Regulations Concerning Safety in Certain Nuclear Facilitiess*.

SKIFS 2000:1, *Swedish Nuclear Power Inspectorate's Regulations concerning the Competence of Operations Personnel at Reactor Facilities.*

SKI 99:10: *Verification and Validation of Human Factors Issues in Control Room Design and Upgrades*, 1999 (Green and Collier).

10 CFR 50.34 (f), *Additional TMI related requirements*, U.S. Code of Federal Regulations, Part 50.

10 CFR 50.47, *Emergency Plans, U.S. Code of Federal Regulations*, Part 50, "Domestic Licensing of Production and Utilization Facilities," Title 10, "Energy."

10 CFR 50.54, *Conditions of license*, (j) through (m), that address operations staffing, U.S. Code of Federal Regulations, Part 50, "Domestic Licensing of Production and Utilization Facilities."

ANSI/AIAA G-035-1992: *Guide to Human Performance Measurements*, 1993 (ANSI).

ANSI/ANS 3.1-1993: *Selection, Qualification, and Training of Personnel for Nuclear Power Plants*, 1993 (American Nuclear Society).

ANSI/ANS 3.5-1993: *Nuclear Power Plant Simulators for Use in Operator Training*, 1993 (American Nuclear Society).

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

ANSI/AIAA G-035-1992: *Guide to Human Performance Measurements*, 1993 (ANSI).

Bladh, K., Borg, A., Eveneus, P. (1998). *Handbook of Validation of Control Room Upgrades* (Report No. 1738). Malmo, Sweden: SwedPower-Vattenfall.

BNL TR E2090-T4-4-12/94, Rev. 1: *Group-View Displays*, 1996 (W. Stubler and J. O'Hara).

IAEA Safety Series INSAG-7, *The Chernobyl Accident: Updating of INSAG-1*

IAEA-TECDOC-668: *The Role of Automation and Humans in Nuclear Power Plants*, 1992 (International Atomic Energy Agency - International Working Group on NPP Control and Instrumentation).

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

IEC 1226: *Nuclear Power Plants – Instrumentation and Control Systems Important for Safety – Classification,* 1993 [International Electrochemical Commission (Bureau Central de la Commission Electotechnique Internationale)].

IEC 1771: *Nuclear Power Plants Main Control Rooms--Verification and Validation of Design*, 1995 (IEC).

IEC 62096 *Nuclear Power Plants – Instrumentation and Control: Guidance for the Decision on Modernization*, 2001 (IEC).

IEEE Std. 1082-1997, "IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations."

Information Notice 95-48: Results of Shift Staffing Study, 1995 (NRC).

International Standards Organization (2000). *Ergonomic Design of Control Centres -- Part 1: Principles for the Design of Control Centres* (ISO 11064-1). Geneva, Switzerland: International Standards Organization.

Kirwan, B. and Ainsworth L. (Eds). (1992). *A Guide to Task Analysis*. London: Taylor and Francis.

NASA Technical Memo No. 103885: *Human-Centered Aircraft Automation: A Concept and Guidelines*, 1991 (NASA - C. Billings).

NRC (2002). *Human System Interface Design Review Guidelines* (NUREG-0700). Washington, DC: U.S. Nuclear Regulatory Commission.

NRC (2002). *Human Factors Engineering Program Review Model* (NUREG-0711). Washington, DC:
U.S. Nuclear Regulatory Commission.

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

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

NUREG-0700: *Human-System Interface Design Review Guideline*, revised periodically (NRC).

NUREG-0737, *Clarification of TMI Action Plan Requirements*, November, 1980.

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, 1992 (NRC).

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

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

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

NUREG/CR-5319, *Risk Sensitivity to Human Error*, P. Samanta, S. Wong, S. Haber, W. Luckas, J. Higgins, and D. Crouch, April, 1989.

NUREG/CR-6393: *Integrated System Validation: Methodology and Review Criteria*, 1997 (O'Hara, et al.).

NUREG/CR-6400, *Human Factors Engineering (HFE) Insights for Advanced Reactors Based Upon Operating Experience*, J. Higgins and K. Nasta, 1996.

NUREG/CR-6633: *Advanced Information Systems: Technical Basis and Human Factors Review Guidance*, 2000 (J. O'Hara, et al.).

NUREG/CR-6634: *Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance*, 2000 (J. O'Hara, et al.).

NUREG/CR-6635: *Soft Controls: Technical Basis and Human Factors Review Guidance*, 2000 (W. Stubler, et al.).

NUREG/CR-6636: *Maintenance of Digital Systems: Technical Basis and Human Factors Review Guidance*, 2000 (W. Stubler, et al.).

NUREG/CR-6637: *Human-System Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance*, 2000 (W. Stubler, et al.).

NUREG/CR-6684: *Advance alarm systems: Guidance development and technical basis*, 2000 (Brown, et al.)

NUREG/CR-6689: "Proposed Approach for Reviewing Changes to Risk-Important Human Actions," 2000 (Higgins, J. and O'Hara, J).

Plans and Preparedness in Support of Nuclear Power Plants, 1980 (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 1.97: *Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environmental Conditions During and Following an Accident* (NRC).

Regulatory Guide 1.105: *Instrumentation Setpoints* (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).

Regulatory Guide 1.149: *Nuclear Power Plant Simulators for Use in Operator Training* (NRC).

Vicente, K., (1999). *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*. New Jersey: Lawrence Erlbaum Associates.

GLOSSARY

Component - The meaning of the word component depends on its context. In context of the entire plant, it is an individual piece of equipment such as a pump, valve, or vessel; usually part of a plant system. In a human-system interface context, a component is one part of a larger unit, such as one meter in a control board. In a maintenance context, a component is a subdivision of a unit of equipment that can be treated as an object by the maintainer, but which can be further broken down into parts. A mounting board together with its mounted parts is an example of a component.

Function - (1) A software supported capability provided to a user to aid in performing a task. (2) A process or activity that is required to achieve a desired goal; see, e.g., "Safety function."

Function allocation -The process of assigning responsibility for function accomplishment to human or machine resources, or to a combination of human and machine resources.

Functional requirements analysis - The examination of system goals to determine what functions are needed to achieve them.

Functional requirements specification _ A specification which identifies the functions and characteristics that the human-system interface and its components accomplish or satisfy.

Human action - See "risk-important human actions."

Human factors - A body of scientific facts about human characteristics. The term covers all biomedical, psychological, and psycho-social 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 interfaces (HSIs) - A human-system interface (HSI) is that part of the system through which personnel interact to perform their functions and tasks. In this document, "system" refers to a nuclear power plant. Major HSIs include alarms, information displays, controls, and procedures. Use of HSIs can be influenced directly by factors such as, (1) the organization of HSIs into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise. HSI use can also be affected indirectly by other aspects of plant design and operation such as crew training, shift schedules, work practices, and management and organizational factors.

Integrated system validation - Integrated System Validation is an evaluation using performance-based tests to determine whether an integrated system design (i.e., hardware, software, and personnel elements) meets performance requirements and acceptably supports safe operation of the plant.

Local control station (LCS) - An operator interface related to 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 human-system interface (see "Simulator" and "Prototype").

Modification - Any type of change or modernization made to HSI components or plant systems that may influence personnel performance.

Operating experience review - A review of relevant history from the plant's on-going collection, analysis, and documentation of operating experiences and from interviews with plant staff.

Performance-based test - Tests that involve the measurement of behavior of personnel, the human-system interface, or aspects of the plant to address design issues and design acceptability.

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

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

Plant - The operating unit of a nuclear power station including the nuclear steam-supply system, the turbine, electrical generator, and all associated systems and components. In the case of a multi-unit plant, the term plant refers to all systems and processes associated with the unit's ability to produce electrical power, even though some systems or portions of systems may be shared with the other units.

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 "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."

Procedures - Written instructions providing guidance to plant personnel for operating and maintaining the plant and for handling disturbances and emergency conditions.

Prototype - A dynamic representation of a human-system interface that is not linked to a process model or simulator. A model of an interface which includes the functions and capabilities expected in the final system, though not in a finished form. (See “Simulator” and “Mockup”).

Risk-important human actions - Actions that are performed by plant personnel to ensure plant safety. Actions may be made up of one or more tasks. There are both absolute and relative criteria for defining risk important actions. From an absolute standpoint, a risk important action is any action whose successful performance is needed to ensure that predefined risk criteria are met. From a relative standpoint, the risk important actions may be defined as those with the greatest risk in comparison to all human actions. The identification can be done quantitatively from risk analysis and qualitatively from various criteria such as task performance concerns based on the consideration of performance shaping factors.

Safety - See “Personal safety,” “Plant safety,” “Safety evaluation,” “Safety function,” “Safety issue,” and “Safety-related.”

Safety evaluation - The regulatory 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 - 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 needed 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.

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. These are the SSCs on which the design-basis analyses of the safety analysis report are performed. They also should be part of a full quality assurance.

Simulator - A facility that physically represents the human-system interface configuration and that dynamically represents the operating characteristics and responses of the plant in real time. (see "Mockup" and “Prototype”).

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.

Style guide - A document that contains guidelines that have been tailored so they describe the implementation of HFE guidance to a specific design, such as for a specific plant control room.

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 close temporal proximity.

Task Analysis - A method for describing what plant personnel must do to achieve the purposes or goal of their tasks. The description can be in terms of cognitive activities, actions, and supporting equipment.

Top-down review - A review approach that follows top-down design. In a top-down design approach, the design starts at the "top" with high-level plant mission goals. These goals are then broken down into functions that are allocated to human and system resources and are further broken down into tasks performed to accomplish function assignments. Tasks are arranged into meaningful jobs and the human-system interface is designed to best support job task performance. The detailed design is the "bottom" of the top-down design process.

Validation - (see “Integrated system validation”)

Verification - The process by which the design is evaluated to determine whether it acceptably satisfies personnel task needs and HFE design guidance.

Appendix
Potential HFE Topics Based on International Standard IEC 1226

International Standard IEC 1226, *Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Classification*, was written to address the classification of NPP I&C functions, systems and equipment (FSE) according to their importance to safety. The Introduction section states that categorization would ideally be based upon a quantitative assessment of risk, ... and that where available these quantitative safety assessments should be used as the basis for categorization. It notes that quantitative criteria should take precedence where numerical safety assessment results are available.

Depending on how IEC 1226 is applied at a particular NPP, additional HFE review topics may be defined. Some potential questions related to aspects of IEC 1226 that may have HFE implications are listed below. It is recognized that these questions overlap to a certain extent between I&C and HFE areas of interest.

1. Provide the list of Category A, B, & C FSEs that resulted from the application of IEC1226 for your NPP.

2. Have the qualitative categorization results been compared to the PSA to see if there are any items that should be moved up in category based upon their risk importance?

3. In the qualitative categorization process of IEC1226, what postulated initiating events (PIEs) were used (see Section 3 of the Standard for definitions)?

4. Section 7, "Classification Procedure," Subsection 7.2 of IEC 1226 states that the categorization of I&C FSEs should continue iteratively throughout the design. Verify that this practice is followed, when necessary, as described in 7.2.

5. Section 8, "Determination of Requirements," requires compliance with adequate codes and standards to ensure that the FSE will function as stipulated in the functional specification. Verify that appropriate codes and standards are included in the specification for the control room I&C equipment.

6. Section 6 "Assignment Criteria" of IEC 1226, Subsections 6.1, 6.2, and 6.3 provide qualitative criteria for assignment of I&C to Categories A, B, & C. Also, Annex A provides examples of Category A, B, and C items. For a sampling of CR instrumentation and alarms, verify that they have been properly assigned. It appears that most of the CR controls, displays and alarm for equipment in safety related systems would be Category A or B.

7. Subsection 8.1.2.a, Specific requirements for Category A, notes that the design shall maintain simplicity for Category A items. For example lower category functions (such as special display calculations, and translation of communication protocols) shall be excluded from the FSE.

8. Section 8.2, "Requirements for ensurance of reliability," subsection 8.2.1 states that reliability shall be determined by either a quantitative PSA or by qualitative engineering judgment and included in the specification. It also states that the assumptions made in the reliability analysis with respect to maintenance, testing, and repair periods shall be

verified during operation and corrective actions taken if needed. Verify that reliability is in the specifications for the CR equipment and that there are plans for periodic confirmations during operation. Also verify that human error is considered in the reliability assessment (as per 8.2.2).

9. Section 8.2, "Requirements for ensurance of reliability," subsection 8.2.2.a states that a Category A I&C FSE shall have redundancy so that the single failure criterion is met. Verify this for selected Category A CR I&C.

10. Section 8.2, "Requirements for ensurance of reliability," subsection 8.2.2.a has requirements for built-in, self-testing features. If there are any of these features in the CR I&C, then verify that this paragraph is met.

11. Section 8.2, "Requirements for ensurance of reliability," subsection 8.2.2.b states that Category B items should have redundancy, but an alternative is if it can achieve reliability with it. However, if redundancy is not provided, then the equipment should be evaluated for single failures that can prevent operation and one should incorporate means to ensure that faults can be quickly detected and repaired. Verify that this has been met for selected Category B items in the CR.

12. Section 8.3, "Requirements for ensurance of performance," subsection 8.3.1 states that testing of components, modules, subsystems, and FSEs shall be carried out according to a quality assurance plan. Verify that the plant's quality assurance plan was used for this testing.

13. Section 8.3, "Requirements for ensurance of performance," subsection 8.3.1 also states that combined tests of installed I&C with the mechanical and fluid systems shall take place at the NPP before operation of the NPP in a mode requiring the safety functions of the I&C. Verify that plans exist for this combined testing.

14. Section 8.3, "Requirements for ensurance of performance," subsection 8.3.2.a states that functional testing of components, modules, subsystems and whenever practicable, complete FSEs, shall be carried out. Note this requirement in the V&V, Element 10.

15. Section 8.3, "Requirements for ensurance of performance," subsection 8.3.2.a states that where computer equipment is used, the system shall be subject to formal V&V. Note this requirement in the V&V, Element 10.

16. Section 8.3, "Requirements for ensurance of performance," subsection 8.3.2.a notes that testing may require the provision of bypass facilities. If bypass facilities are incorporated, then their integrity shall be justified to show that they would not compromise a safety function (e.g., physically restrict their use to a single train). Verify that this design feature is met and tested for any with these bypass features.

Section 8.3, "Requirements for ensurance of performance," subsection 8.3.2.b notes that testing of Category B display and alarm equipment shall include injection tests of relevant input signals to show satisfactory performance. Verify that such testing is planned for the CR and emergency control room Category B items.

www.ski.se

STATENS KÄRNKRAFTINSPEKTION
Swedish Nuclear Power Inspectorate

POST/POSTAL ADDRESS SE-106 58 Stockholm
BESÖK/OFFICE Klarabergsviadukten 90
TELEFON/TELEPHONE +46 (0)8 698 84 00
TELEFAX +46 (0)8 661 90 86
E-POST/E-MAIL ski@ski.se
WEBBPLATS/WEB SITE www.ski.se