GE Energy

David H. Hinds
Manager, ESBWR

PO Box 780 M/C L60
Wilmington, NC 28402-0780
USA

T 910 675 6363
F 910 362 6363
david.hinds@ge.com

MFN 06-086

Docket No. 52-010

March 31, 2006

U.S. Nuclear Regulatory Commission
Document Control Desk
Washington, D.C. 20555-0001

Subject: **ESBWR Human Factors Engineering Licensing Topical Report (LTR)–NEDO-33268**

By the reference letter, GE committed to provide the subject LTR to support the ESBWR Design Certification. The LTR was identified in the reference as NEDO-33xxx, *Human System Interface Design Plan*, but has been renamed to *ESBWR Human Factors Engineering Human-System Interface Design Plan*. The subject LTR is enclosed.

The purpose of this plan is to:

- Establish the process by which HSI design requirements and associated work place factors are identified, refined and verified
- Apply HFE principles and criteria to translate functional and task requirements to the detailed design of alarms, displays, controls and other aspects of the control and instrumentation systems and HSI
- Achieve an integrated design of the ESBWR MMIS/HSI

If you have any questions about the information provided here, please let me know.

Sincerely,

George Stramback for

David H. Hinds
Manager, ESBWR

D068

Enclosure:

MFN 06-086 – Licensing Topical Report

- NEDO-33268, "ESBWR Human Factors Engineering Human-System Interface Design Plan," March 2006

Reference:

MFN 05-140, Letter from David H. Hinds to U. S. Nuclear Regulatory Commission, *Submittal Schedule for Licensing Topical Reports Related to ESBWR (TAC # MC8168),* November 22, 2005

cc:		
	WD Beckner	USNRC (w/o enclosures)
	AE Cubbage	USNRC (with enclosures)
	LA Dudes	USNRC (w/o enclosures)
	GB Stramback	GE/San Jose (with enclosures)
	eDRF	0000-0051-1679

Enclosure

MFN 06-086

NEDO-33268, Licensing Topical Report ESBWR Human-System Interface Design Implementation Plan

GE Energy
Nuclear

3901 Castle
Hayne Rd
Wilmington, NC 28401

NEDO-33268
Revision 0
Class I
DRF#0000-0051-1679
March 2006

LICENSING TOPICAL REPORT

ESBWR
HUMAN-SYSTEM INTERFACE DESIGN
IMPLEMENTATION PLAN

INFORMATION NOTICE

This document NEDO-33268, Revision 0, contains no proprietary information.

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT PLEASE READ CAREFULLY

The information contained in this document is furnished for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and participating utilities, and nothing contained in this document are construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to **any unauthorized use,** General Electric Company makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table of Contents

List of Tables

List of Figures

1 Introduction

The Human System Interface (HSI) design process translates functional and task requirements into HSI characteristics, displays, software, and hardware for monitoring, control and protection functions during normal and accident situations. The HSI is based on the use of a structured methodology that guides designers in identifying and selecting candidate HSI approaches, defining the detailed design, and performing HSI tests and evaluations. It describes the development and use of Human Factors Engineering (HFE) guidelines that are tailored to the unique aspects of the ESBWR design, (e.g., a style guide to define the design-specific conventions).

The HSI design methodology is developed and establishes standardization and consistency in applying HFE principles. With the increased use of digital instrumentation systems in advanced nuclear power plant designs, the nuclear industry developed a consolidated standard to address accident monitoring that was more flexible than Regulatory Guide 1.97R3. The NRC under Regulatory Guide 1.97R4 has endorsed this standard. The result is that instead of prescribing the instrument variables to be monitored (as was the case in Revision 3), performance-based criteria may be used for selecting variables.

Moreover, rather than providing design and qualification criteria for each variable, the standard criteria are based on the accident management functions of the given type of variable (IEEE Std. 497-2002). Thus for new designs a more flexible, performance-based criteria for the selection, performance, design, qualification, display, and quality assurance of accident monitoring variables has been established. The classification scheme is summarized in Table 1 with alternate sources of information identified for defining human tasks.

The process and the rationale for the HSI design are documented and managed under General Electric Energy Nuclear (GEEN) Quality Assurance (QA) and ESBWR specific Program Plans.

An objective of the HFE program is to resolve issues related to the detailed design of specific aspects of the Man-Machine Interface System (MMIS) during HSI design rather than at HSI Verification and Validation (V&V). Acceptable display formats or alarm system processing design tradeoffs are resolved during the HSI design activities through the systematic application of HFE principles and criteria and integrated under the ESBWR-specific software management plans and derived implementation plans.

1.1 Purpose

The purpose of this plan is to establish the process by which HSI design requirements, and associated work place factors are identified, refined and verified for the Main Control Room (MCR) and in the Remote Shutdown System (RSS) area, consistent with accepted HFE practices and principles.

This plan will systematically apply HFE principles and criteria in order to translate functional and task requirements to the detailed design of alarms, displays, controls and other aspects of the control and instrumentation systems and HSI. This plan will achieve an integrated design of the ESBWR MMIS/HSI.

The methods and criteria defined in this plan are used by the MMIS Design Team, Control Room Design Team (CRDT), and other users.

Figure 1 shows where this HSI Design Implementation Plan fits into the overall HFE Process.

1.2 Scope

The Scope of this HSI Design Implementation Plan is to establish:

1. The methods and criteria for designing the HSI in accordance with accepted human factors practices and principles;
2. Information and control requirements for implementation in the HSI design to:
    a. Support critical tasks identified through task analyses, including the displays, controls, and alarms necessary for the execution of those tasks;
    b. Identify plant parameters that are used for calculation of operation limits that will also become fixed position alarms, displays, and controls in the MCR as described in the ESBWR Design Control Document (DCD) Chapter 18.
    c. Satisfy the MCR layout and configuration plan as shown in the ESBWR DCD Chapter 18.
    d. Limit errors associated with risk-important human actions;
    e. Identify human errors when feasible.
3. Methods for comparing the consistency of the HSI human performance, equipment design and associated workplace factors with that modeled and evaluated through the task analysis;
4. HSI design criteria and guidance for MCR operations during periods of maintenance and test; and

5. Test and evaluation methods for resolving HFE/HSI design issues. These test and evaluation methods will include the criteria to be used in selecting HFE/HSI design and evaluation tools.

1.3 Definition of Terms

1. Human-System Interface (HSI)

   This is the means through which personnel interact with the plant, including the alarms, displays, controls, and job performance aids. This includes maintenance, test, and inspection interfaces as well.

2. Local Control Station (LCS)

   An operator interface related to nuclear power plant (NPP) process control that is not located in the MCR. This includes multifunction panels, as well as, single-function 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.

3. Man-Machine Interface Systems (MMIS)

   The MMIS encompasses all instrumentation and control systems provided as part of the ESBWR which perform the monitoring, control, alarming, and protection functions associated with all modes of plant normal operation (i.e., startup, shutdown, standby, power operation, and refueling) as well as off-normal, emergency, and accident conditions.

4. MMIS Design Team (Design Team)

   The Design Team is a team of engineers, as defined in the MMIS Design Implementation Plan, responsible for the design of the MMIS systems. MMIS are those systems which perform the monitoring, control and protection functions.

5. Control Room Design Team (CRDT)

   The CRDT is a subset of the Design Team. The CRDT is responsible for the overall coordination of the design of the Main Control Room (MCR).

2 References

2.1 Supporting Documents

1. ESBWR DCD Chapter 18 revision 1, October 2005 (GE 26A6642BX)
2. Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217
3. Operational Experience Review (OER) Plan, NEDO-33262
4. System Functional Requirements Analysis Implementation Plan, NEDO-33219
5. Allocation of Functions Implementation Plan, NEDO-33220
6. Task Analysis Implementation Plan, NEDO-33221
7. Human Reliability Analysis (HRA) Plan, NEDO-33267

2.2 Codes and Standards

1. IEEE Std. 1023-1988, Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating stations.
2. IEEE Std. 497-2002, Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.

2.3 Regulation and Regulatory Documents

1. 10CFR50, Domestic Licensing of Production and Utilization Facilities, December 1981
2. 10CFR73, Physical Protection of Plants and Materials, Paragraph 55, August 1980
3. NUREG-0696, Functional Criteria for Emergency Response Facilities, 1980
4. NUREG-0700, R2 Human System Interface Design Review Guideline.
5. NUREG-0711, R2 Human Factors Engineering Program Review Model,
6. NUREG-0737, Supplement 1, Requirements for Emergency Response Capability
7. NUREG-0800, Standard Review Plan (SRP)

8. NUREG-0800, SRP Section 3.9.4, Control Rod Drive Systems

9. NUREG-0835, Human Factors Acceptance Criteria for the Safety Parameter Display System.

10. NUREG-0899, Guidelines for the Preparation of Emergency Operating Procedures, 1982

11. NUREG/CR-4227, Human Engineering Guidelines for the Evaluation and Assessment of Video Display Units, 1985

12. NUREG/CR-5228, Techniques for Preparing Flowchart Format Emergency Operating Procedures (Vols. 1 & 2), 1989

13. NUREG/CR-5439, Human Factors Issues Associated with Advanced Instrumentation and Controls Technologies in Nuclear Plants

14. Regulatory Guide 1.97R4, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident

2.4 Departments of Defense and Energy

1. AD/A223 168, System Engineering Management Guide. (Defense Systems Management College, Kockler, F., et al)

2. ESD-TR-86-278, Guidelines for Designing User Interface Software

3. MIL-H-46855B, Human Engineering Requirements for Military Systems, Equipment and Facilities

4. MIL-HDBK-759A, Human Factors Engineering Design for Army, Material

5. DOD-HDBK-761A, Human Engineering Guidelines for Management Information Systems

6. MIL-STD-1472D, Human Engineering Design Criteria for Military Systems, Equipment and Facilities

7. DOD-HDBK-763, Human Engineering Procedures Guide

2.5 Industry and Other Documents

1. Advanced Light Water Reactor, Utility Requirements Document, Volume III, Chapter 10, Man-Machine Interface Systems

2. ANSI HFS-100, American National Standard for Human Factors Engineering of Visual Display Terminal Workstations (American Nat'l. Standards Institute)

3. ANSI/ISA-S 18.1, Annunciator Sequences and Specifications (Instrument Society of America)

4. ANSI/ISA-S5.5, Graphic Symbols for Process Displays (Instrument Society of America)

5. BNL TR-E2090-T4-1-9/96, Human-Systems Interface Design Process and Review Criteria, 1996

6. BNL TR-E2090-T4-4-12/94, R1, Group-View Displays: Functional Characteristics and Review Criteria, 1996

7. EPRI CS-3745, Enhancing Fossil Power Plant Design, Operation, and Maintenance: Human Factors Guidelines

8. EPRI NP-3448, Procedure for Reviewing and Improving Alarm Systems, 1984

9. EPRI NP-3659, Human Factors Guide for Nuclear Power Plant Control Room Development, 1984

10. EPRI NP-3701, Computer-Generated Display System Guidelines, 1984

11. EPRI NP-4350, Human Engineering Design Guidelines for Maintainability, 1985

12. EPRI NP-5795, Control Room Deficiencies, Remedial Options and Human Factors Research Needs, 1991

13. EPRI TR-101814, Human Factors Guidelines for Fossil Power Plant Control Rooms and Remote-Control Stations, 1993

14. IAEA Technical Reports Series No. 387, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, 1999.

15. IEC 60964, Design for Control Rooms of Nuclear Power Plants – 1st Edition, CEI/IEC 964: 1989, 1989-03

16. INPO 83-036, Human Engineering Principles for Control Room Design Review (NUTAC)

17. INPO 83-042, Control Room Design Review Survey Development Guideline (NUTAC)

18. INPO 85-017, Guidelines for the Conduct of Operations at Nuclear Power Stations (NUTAC)

19. INPO-83-026, Control Room Design Review Implementation Guideline (NUTAC)

20. INPO-83-003, Guideline for an Effective Safety Parameter Display System (SPDS) Implementation Program (NUTAC).

3 Summary of Human Factors Analysis for HSI Design

3.1 Background

The importance of human operators in the safe and reliable operation of NPPs has been increasingly recognized, especially since the accidents at Three Mile Island (TMI) and Chernobyl. A human operator possesses many desirable features that cannot be matched by current levels of machine automation. Humans are creative and flexible and can use stored knowledge, routines and patterns to cope with novel and unexpected situations. Humans are excellent detectors of signals in the midst of noise and can extract useful data from incomplete sets of information. However, these human abilities are unlikely to be effective or consistent under adverse conditions if operators are overloaded with tasks or if the HSI does not provide timely, adequate, relevant and accurate information or is cumbersome to use.

Prior to TMI, the information requirements for supporting human performance were implicitly addressed in NPP designs by using intuitive common sense and applicable engineering practices. The human operator was primarily involved in carrying out physical control actions. However, analyses following TMI clearly demonstrated that more systematic and comprehensive approaches to meeting information requirements (particularly in control rooms) were needed. Such a systematic process is shown in Figure 1.

In addition, the role of the operator was redefined from that of just a physical controller to include decision-making. These changes are reflected in the guidelines and standards developed by the NRC, EPRI and IEEE in the USA, and internationally by the IAEA and IEC, to assist designers and operations staff in improving human performance through an enhanced HSI. This created a greater emphasis on the use of simulators for:

- Developing and validating the HSI;
- Developing and validating requirements for operating and emergency procedures;
- Training and qualifying operators;
- Periodically requalifying operators.

Simulators range from those which emulate a portion of the plant or a system (i.e. part-task simulators) to those which fully reproduce the control room environment (i.e. full-scope simulators). Both have been used to facilitate HSI designs that support safe, efficient and reliable operator performance during all phases of normal plant operation, abnormal events and accident conditions, as well as for maintenance, test, surveillance and inspection activities. To achieve operator performance goals, information, displays, controls, and other interface devices in the control room and other plant areas are systematically designed and implemented consistent with good HFE practices.

3.2 Application of HFE principles in the design of the HSI

The principal objectives of the HSI design are to provide the indications, controls and status displays necessary for tasks allocated to the operator and to provide the operator with accurate, complete, and timely information regarding the functional status of plant equipment and systems. An additional objective of the HSI design is to permit plant commissioning to take place effectively and to permit timely modifications and maintenance of the HSI.

The need for functional isolation and physical separation where safety and non-safety systems are brought into close proximity are integrated into the design.

The control room should provide an environment in which the staff is able to perform its tasks without discomfort, excessive stress, or physical hazard. In accordance with habitability requirements, appropriate measures should be taken to safeguard the occupants of the control room against potential hazards such as unauthorized access, undue radiation resulting from an accident condition, toxic gases, and consequences of fire, which could jeopardize necessary operator actions.

In order to maximize the plant capacity factor to assure a satisfactory return on the financial investment, consideration should be given in the HSI design to:

- Facilitating planned operations;
- Minimizing the occurrence of any undesired power reduction or plant trip caused by erroneous decision-making and actions, or by local disturbances associated with malfunction or failure of I&C systems.

The HSI basic design is capable of being adapted to meet specific utility desired features related to MMIS that enhance the ability of operators to carry out monitoring, planning and response tasks.

The ESBWR HSI design implementation starts with the results of the operations analysis (system functional requirements analysis, allocation of functions, and task analysis) and with the existing design bases included in the Advanced Boiling Water Reactor (ABWR) Standard Safety Analysis Report (SSAR). These results and design bases are translated into hardware and software design requirements which are, in turn, written into the applicable specifications and included in the hardware drawings and software programs.

In order to evaluate these requirements (e.g., operator time critical and reliability critical requirements), studies and tests are performed as necessary. Mockups and models are constructed and/or dynamic simulations performed as necessary to validate the designs. Also, reflected in the hardware and software designs are the HFE guidelines summarized in Sections 4.2 for standard HSI and 4.3 for special features of the MCR. These guidelines are drawn from documents referenced in Sections 2.3 (Regulation and Regulatory Documents), 2.4 (Departments of Defense and Energy) and 2.5 (Industry and Other Documents).

Figure 2 defines the overall design process described in this plan. In this figure, the expected inputs and outputs are identified. The relationship between this plan and other implementation plans is also identified in Figure 2.

3.3 General Requirements for Human Factors Engineering

The design uses the following human factor elements, as defined in the MMIS plan, to address HFE issues during the HSI design process as shown in Figure 2. These elements are summarized in the following subsections.

3.3.1 HSI Design Inputs

The following sources of information provide input to the HSI design process:

(1) *Analysis of Personnel Task Requirements* - The analyses performed in earlier stages of the design process are used to identify requirements for the HSI. These analyses include:

- Operational experience review - Lessons learned from other complex human-machine systems, including ABWR reference designs and designs involving similar HSI technology are used as an input to HSI design.

- Functional requirement analysis and function allocation - The HSI supports the operator's role in the plant, e.g., appropriate levels of automation and manual control.

- Task analysis - The set of requirements to support the role of personnel is provided by task analysis. The task analysis identifies:

  - tasks that are necessary to control the plant in a range of operating conditions for normal through accident conditions;

  - detailed information and control requirements (e.g., requirements for display range, precision, accuracy, and units of measurement);

- task support requirements (e.g., special lighting and ventilation requirements); and
- risk-important HAs and their associated performance shaping factors, as identified through HRA are given special attention in the HSI design process.

- Staffing/qualifications and job analyses - The results of staffing/qualifications analyses provide input for the layout of the overall control room and the allocation of controls and displays to individual consoles, panels, and workstations. They establish the basis for the minimum and maximum number of personnel to be accommodated and requirements for coordinating activities between personnel.

(2) *System Requirements - Constraints imposed by the overall Instrumentation and Control (I&C) system are considered throughout the HSI design process.*

(3) *Regulatory Requirements - Applicable regulatory requirements are identified as inputs to the HSI design process.*

As the design progresses the HFE team may identify other requirements that become inputs to the HSI design

3.3.2 Concept of Operations

The HFE team will develop a concept of operations indicating personnel staff composition and the roles and responsibilities of individual staff members based on anticipated staffing levels. The concept will identify the relationship between personnel and plant automation by specifying the responsibilities of the crew for monitoring, interacting, and overriding automatic systems and for interacting with computerized procedures systems and other computerized operator support systems.

The concept will provide a high-level description of how personnel will work with HSI resources. Examples of the types of information that are identified is the allocation of tasks to the MCR or local control stations, whether personnel 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 are displayed to the entire crew.

Coordination of operations staff activities, such as the interaction with auxiliary operators and coordination of maintenance and operations are addressed.

3.3.3 Functional Requirement Specification

The HFE team will develop functional requirements for the HSI to address the concept of operations; personnel functions and tasks for their roles derived from function, task and staffing/qualifications analysis; and requirements for a safe, comfortable working environment. The HSI requirements will address the various types of HSIs , e.g., alarms, displays, and controls.

3.3.4 HSI Concept of Design

The HFE team may use several approaches for developing a concept design as described in NUREG-0711R2. The HFE team may use the HSI functional requirements, including development of a functional requirement specification, modification of predecessor designs, surveys of the state-of-the-art in HSI technologies, or predecessor and ABWR reference designs. Human performance issues identified from previous operating experience with the predecessor designs may be resolved in the conceptual design.

Evaluation of the conceptual design can include comparison with operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments. Alternative concept designs may be considered for elements of the HSI. Evaluations will provide reasonable assurance that the selection process is based on a thorough review of design characteristics and a systematic application of selection criteria. Tradeoff analyses, based on the selection criteria, will provide a rational basis for the selection of concept designs. HSI design performance requirements are identified for components of the selected HSI concept design. These requirements are based on the functional requirement specifications but are refined to reflect HSI technology considerations identified in the survey of the state of the art in HSI technologies and human performance considerations identified in the human performance research. A flow chart that illustrates the process for designing computer generated displays is shown in Figure 3.

3.3.5 HSI Detailed Design and Integration

(1) Design-specific HFE design guidance (Style Guides) is developed and HFE Guidelines are utilized in the design of the HSI features, layout, and environment. Additional information concerning the Style Guide appears in Section 5.1.

(2) The HSI detailed design supports personnel in their primary role of monitoring and controlling the plant while minimizing personnel demands associated with use of the displays (e.g., window manipulation, display selection, display system navigation). High-level HSI design review principles reflect NUREG-0700R2 guidelines.

(3) For risk-important Human Actions (HAs), the design seeks to minimize the probability that errors will occur and maximize the probability that an error is detected if one is made.

(4) When developing functional requirements for monitoring and control capabilities that may be provided either in the control room or locally in the plant, the following factors are considered:

- communication, coordination, and workload
- user feedback
- local environment
- inspection, test, and maintenance
- importance to safety

(5) The layout of MMIS within consoles, panels, and workstations is based upon (a) analyses of operator roles (job analysis) and (b) systematic strategies for organization such as arrangement by importance, frequency of use, and sequence of use.

(6) Personnel and task performance is supported during minimal, nominal, and high-level staffing.

(7) The design process addresses the use of the HSIs over the duration of a shift where decrements in performance due to fatigue may be a concern.

(8) HSI characteristics 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 will address conditions such as loss of lighting, loss of ventilation, and main control room evacuation. For the remote shutdown facility and local control stations, requirements address constraints imposed by the ambient environment (e.g., noise, temperature, contamination) and by protective clothing (if necessary).

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

(10) Modifications to predecessor HSI designs to be used for ESBWR applications, are reviewed to address the following considerations.

(a) As practical, maintain consistency with user's existing strategies for gathering and processing information and executing actions in the task analysis.

(b) As practical, maintain or improve existing support for crew coordination through shared view of plant information and, awareness of others' actions and crew communications.

(c) Development of design requirements to assure that the relationship between plant systems are consistent with original design, if the modification changes the degree of integration between plant systems.

3.3.6 HSI Tests and Evaluations

The HFE team will develop testing and evaluation plans for the HSI designs that can be iteratively conducted throughout the HSI development process. The types of tests and evaluations performed will vary depending on the specific point in the design process and appropriate data collection methods (Figure 4).

The methodology used for testing applies the following criteria:

3.3.6.1 Trade-Off Evaluations

To adequately consider human performance the HFE team will use the following example factors when performing trade-off analyses and evaluations to make design choices.

- personnel task requirements
- human performance capabilities and limitations
- HSI system performance requirements
- inspection and testing requirements
- maintenance requirements
- use of proven technology and the operating experience of predecessor designs.

The HFE team will make explicit trade-off evaluations to determine the relative benefits of selected design alternatives.

3.3.6.2 Performance-Based Tests

The HFE team will plan performance-based tests to address the specific questions and design features being addressed. The tests, and selection of participants, will depend on the purpose of the evaluation, the questions being addressed, and the maturity of the design. The performance measures will consider measurement characteristics, identification and selection of variables, and performance criteria. Testbed selection is based on test requirements and design maturity.

To the degree possible the test design will minimizes bias, confounds, and error variance (noise). Test data are analyzed using established analysis techniques such as those shown in Figure 5. Design solutions are developed to address problems that are identified during the testing and evaluation of the HSI design.

3.3.7 HSI Interim Design Documentation

The design details of the ESBWR MMIS are captured within the GEEN QA documentation system. These interim engineering reports will provide input to the HSI design report. (See Section 7) They include:

- HSI requirements and design characteristics developed from operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations, as well as records of the basis of the design changes

- Detailed HSI descriptions including its form, function and performance characteristics

- The results of tests and evaluations performed in support of HSI design.

4 HSI Design Criteria

Human Factors Engineering criteria as defined in Section 4.0 is applied along with all other design requirements to select and design the particular equipment for application to the MCR and Remote Shutdown System HSI. The HSI design will implement the information and control requirements that have been developed in the task analysis, including the displays, control and alarms necessary for the execution of those tasks identified in the task analyses as being critical tasks. The equipment design configuration will satisfy the functional and technical design requirements and insure the HSI is consistent with HFE principles.

The HSI design criteria applied to the ESBWR MCR will also be implemented into the design of the information displayed on the video display units (VDUs) located in the ESBWR Technical Support Center (TSC) and Emergency Offsite Facility (EOF). The information displayed in the TSC/EOF and Emergency Operating Procedures (EOPs), i.e., a subset of information available to the operator in the MCR. HSI as defined for ESBWR also includes the operator interface at the RSS displays.

Typically, the order in which various kinds of HSI are addressed is dictated by the amount of lead time required for construction, progressive availability of design information, and time needed to satisfy training requirements. Human factors efforts are completed within the overall plant development schedule. HSI development is performed in accordance with the MMIS and HFE Implementation Plan NEDO-33217.

Usually, physical layout of the plant is determined early so that building construction can begin. Thus, MCR workspace interfaces are considered first. Panel design then proceeds within constraints of workspace design decisions. Communications system interfaces are next considered, within constraints of workspace and panel design decisions. Evaluation of at least some parts of communications system design is completed in sufficient time for equipment to be used in final stages of personnel training. The design of HSI is performed using the integrated systems approach.

Human factor design criteria have been developed through experience and evaluation of previous interface designs. Applicable human capabilities and characteristics for the project are provided as fundamental human factors design data, consistent with prior use in ABWR designs. Such data include HFE requirements that are directly applicable to the plant staff for the MCR, RSS and other HSI. The data also includes HFE requirements that are applicable to operators and maintenance staff. Related areas include the following:

1. Anthropometric considerations
2. Population human perceptual system capabilities
3. Auditory and visual capabilities and characteristics
4. Human ability to process information

4.1 Operating Experience Review of Previous NPP MMIS Designs

In many previous HSI designs, the importance of the human factors in plant operations was generally overlooked. Today, the benefits of improved HSI have been demonstrated by incorporating lessons learned from industry operating experience through a human factors engineering program in existing plants. For example, adding mimics and system boundaries on control panels helped operators select proper valve alignments at a glance. Such improvements in existing MCR and HSI were stimulated through the difficult process of identifying human factors discrepancies (HEDs) (i.e., design features that are incompatible with personnel capabilities). This shows the importance of HF program planning for new plant designs, such as the ESBWR, where the benefit is to significantly reduce the number of HEDs.

4.1.1 Existing Operating Plants

Following the accident at Three Mile Island (TMI), utilities took actions to correct these deficiencies. Appendix A characterizes the human factor principles derived from operating experience reviews of previous NPP HSI designs (NEDE-33217).

The Detailed Control Room Design review (DCRDR) reports for the Kuo Sheng, Perry, Susquehanna, and Riverbend plants have been obtained. The Human

Engineering Discrepancies (HEDs) in those reports serve as relevant operating experience in the design and layout of ESBWR HSI.

4.1.2 Other Industries

The HFE Design Team performs a review of MMIS being used in other industries such as fossil plants, aerospace, petrochemical, etc. This review focuses on the following ESBWR design areas:

- Use of flat panel and video display unit (VDU) displays
- Use of electronic on-screen controls
- Use of wide display panel (WDP)
- Use of prioritized alarm systems
- Automation of process systems
- Operator workstation design integration

Those operating experience reviews include:

- Review of reports provided by industry organizations (i.e., EPRI, INPO, etc.)
- Review of applicable research in these design areas, as may be documented in reports from universities, national laboratories, and the NRC, and in proceedings published by HFE professional societies
- Review of applicable research and experience reports published by HSI equipment vendors

The operating experience review in each of the three areas specified above also includes feedback obtained from actual users. If the documents selected for the conduct of the operating experience review for a particular area do not include the results of user feedback, then interviews with users of at least two applications of that particular technology area are also conducted.

Finally, the results from all these operating experience review activities are entered into the HFE Issue Tracking System to assure that the ESBWR implementation reflects the experience gained by the resolution of design problems in other industries.

4.2 Standard Design Features

Using requirements from the ESBWR Design Control Document (DCD), results of the operations analysis (system functional analysis, allocation of functions and task analysis), and the operating experience of BWRs and ABWRs, as part of the design development a program is undertaken for the purpose of "studying the application of man-machine technologies to enhance the efficiency of operation control of NPPs". A variety of tests, studies and evaluations are performed in a number of areas of control room equipment design. These studies and evaluations culminate in the fabrication and testing of prototype control room HSI equipment designs.

The HSI design program includes (1) consideration of existing control room operating experience; (2) a review of trends in control room designs and existing control room data presentation methods; (3) evaluation of new HSI technologies, alarm reduction and presentation methods; (4) results of operations analyses and (5) validation testing of prototype. The prototype is evaluated in accordance with the methods and criteria defined in this plan and the Human Factors V&V Implementation Plan. Following the completion of the prototype tests and implementation of their results, the detailed control room MMIS standard design features are finalized.

4.2.1 Listing of Features

The MCR MMIS design incorporates the following standard ESBWR design features:

1. A single, integrated control console staffed by two operators; the console has a low profile such that the operators can see over the console from a seated position.
2. The use of non-safety related VDUs for non-safety system control and monitoring and safety system monitoring.
3. The use of a separate set of on-screen controls VDUs for safety system control and monitoring. The operation of this set of VDUs is independent of the DCIS, and all equipment associated with their functions of safety system control and monitoring are divisionally separate and qualified to standards for safety related, Class 1E equipment.
4. The use of dedicated function switches on the control console.
5. Operator selectable automation of predefined plant operation sequences.
6. The incorporation of an operator selectable semi-automated mode of plant operations, which provide procedural guidance on the control console VDUs.
7. The capability to conduct all plant operations in an operator manual mode.

8. The incorporation of a WDP which presents information for use by the entire control room operating staff.
9. The inclusion on the WDP of fixed-position displays of key plant parameters and major equipment status.
10. The inclusion in the fixed-position displays of both Class 1E qualified and non-Class 1E qualified display elements.
11. The independence of the fixed-position displays from the DCIS equipment that performs the calculations for process monitoring functions.
12. The inclusion within the WDP of large VDUs driven by the DCIS.
13. The incorporation of a "monitoring only" shift supervisor's console with VDUs that can display any screen format (image) available to the operators on the MCC VDUs.
14. The incorporation of the safety parameter display system (SPDS) function as part of the plant status summary information which is continuously displayed on the fixed-position displays on the WDP.
15. The use of fixed-position alarm tiles on the WDP.
16. The application of alarm processing logic to prioritize alarm indications and to filter unnecessary alarms.
17. A spatial arrangement between the WDP, the MCC and the shift supervisor's console which allows the entire MCR staff to conveniently view the information presented on the WDP.
18. The use of VDUs to provide alarm information in addition to the alarm information provided via the fixed-position alarm tiles on the WDP.

The MCR contains the MCC, the WDP, the shift supervisor's console, and other peripheral equipment such as a workstation for an assistant supervisor. The spatial arrangement of the MCC, the WDP, and the shift supervisor's console is a standard ESBWR design feature. The arrangement is depicted in the Control Building General Arrangement Drawing.

The MCC is located directly in front of the WDP for optimum viewing efficiency by plant operators seated at the MCC. The shift supervisor's console is also in front of the WDP, but at a somewhat greater distance than the MCC so that the shift supervisor is positioned behind the MCC operators. This arrangement enables all MCR personnel to view the contents of the WDP.

The relative plant system locations on the console are generally (1) safety related systems and nuclear steam supply system (NSSS) on the left, (2) overall plant supervision in the center, and (3) balance of plant (BOP) on the right. Flat panel displays on the left side of the console are divisionally dedicated and qualified to Class 1E standards. Flat panel displays at the center and right areas of the console provide monitoring and control of non-safety related NSSS and BOP systems.

4.2.2 Location and Protection

1. Location

   The MMIS related to HSI is located where it is not affected by the consequences of plant internal hazards such as missile, radiation, fire, etc., and where operators can easily gain access under all the plant conditions, yet evacuate from the location if the location becomes uninhabitable.

2. Protection

   The design of the MMIS provides, within the design basis, protection against fire, radiation, internal and external missiles, earthquake and appropriate security measures to control access to HSI software.

   a. Fire Protection

      Attention is given to using nonflammable materials in the HSI. The HSI area in the MCR is equipped with fire detection and fire suppression systems.

      Electrical equipment in the HSI is designed to neither cause nor support a fire as far as this is reasonably achievable. Cable circuits and switchgear associated with the HSI are protected against the consequences of fire. Cable insulation and sheathing materials are fire-retardant and consistent with applicable national codes for flame propagation, release of combustion products and materials where applicable.

   b. Radiation Protection

      The staff is protected against direct radiation in any accident situation. The control room is designed in accordance with applicable codes, standards and regulatory requirements for habitability. Radiological protection is considered in the design. Breathing apparatus is available to the staff.

c. Missile Protection

The HSI design includes assessment and protection against missiles originating from inside and outside the control room.

d. Earthquake Protection

The HSI equipment related to safety functions, the air-conditioning system and emergency illumination systems are designed in accordance with the applicable codes and standards for postulated design events.

e. Security

The HSI is designed to allow for control of access to plant system control and databases. Access to the MCR is in accordance with the site security plan.

4.2.3 Space, Configuration and Environment

1. Space

The operator work area has sufficient space to allow the staff to perform all necessary actions, while minimizing operator movement in abnormal conditions. Attention is paid to providing work areas, writing space and storage space for documents:

a. Work areas which are manned on a continuous basis are designed for seated operation and adequate seating are provided, but should also permit standing operations.

b. Where writing and access to documentation are normal parts of HSI duties, adequate writing space is made available. Laydown space for the documentation while in use is available.

c. Storage space for documents is provided close to the operating position to avoid the documents being laid on consoles, desks, etc.

2. Configuration

The MMIS is designed giving due consideration to:

a. Plant owner's operating principles

b. Assignments of functions to the operators and the DCIS.

c. Centralized or local control philosophy, which determines the extent of controls present in the control room

d. Supervision criteria, which determine the number of VDUs, indicating instruments, recorders, alarms and indicating lights on the panels

e. Plant and technological choices (segregation between different divisions, use of automatic control sequences, dimensions of instruments and controls, extent of automation and/or multiplexed controls)

f. The control room has such operating areas as are necessary, where each operator can obtain access to all controls and information required to perform the tasks assigned to him in all operational and accident conditions.

g. The operating area and HSI equipment such as control desks, boards and panels are arranged according to human factors engineering principles:

4.2.3.1 Grouping of operating areas

Ideally the MCR and LCS is divided into operating areas where each operator has all the controls and indications required to perform the tasks assigned to him in various operating conditions including start up, normal operation, shutdown and emergencies. Consideration is also given to tasks related to maintenance, testing, and inspection activities.

The configuration should minimize interference between operator tasks.

4.2.3.2 Control boards and arrangement

The arrangement of control panels, desks and boards in the MCR and LCSs will:

a. Allow each operator to have sufficient space between the panels, etc., for immediate and direct access to the information and controls pertinent to his tasks,

b. Minimize conflicting paths for the various operators,

c. Facilitate communications and coordination between the operators,

d. Minimize reflections.

4.2.3.3 Size and shape

Size and shape of HSI equipment such as control desks, boards, panels and chairs are determined from the anthropometric requirements and other human engineering considerations to be satisfied.

4.2.4 Environment

Environmental conditions in the MCR should be such that the operators can perform their tasks effectively and comfortably. The environmental conditions will be consistent with the MCR habitability requirements.

The MCR environmental specification includes requirements for:

1. Heating, Ventilation and Air-Conditioning (HVAC)

   The MCR ventilation system design includes measures to cope with postulated accident conditions of the plant. The HSI is designed in accordance with the MCR environmental conditions.

2. Illumination

   In the design of the lighting system in the MCR, special attention is given to uniformity, shadows, glare, reflections and highlighting.

   An emergency lighting system continuously provides illumination necessary for task performance even on failure of the normal system.

3. Auditory Environment

   Auditory environment of the HSI is designed considering a relevant database on human auditory capability and characteristics.

The special environmental requirements for the MCR are defined in the Post Accident Monitoring (PAM) references RG 1.97 and IEEE 497.

4.2.5 Panel Layout

4.2.5.1 Priority

Guidelines, based on reference documents in Section 2 are established and applied for the layout and arrangement of alarms, displays and controls belonging to a function of a system as well as for priority rankings between similar elements in the layout of the panels.

4.2.5.2 Positioning

The positioning of displays, indicators and controls on vertical panels and sit-down consoles are based on the following criteria:

a. Alarm panels and plant parameters located on the WDP vertical section are visible from the operating area of the HSI.

b. Frequently used controls are within convenient reach. The related indicators and displays are readable from the operating position.

c. Displayed information and related controls are functionally grouped.

4.2.6 Location Aids

4.2.6.1 Grouping of display information and controls

It is essential that the displayed information and controls be logically grouped. Controls and displays should be placed within the control room at locations which promote efficient procedures, safe operation and maximum operator awareness of the current system condition. There are three general methods for achieving this condition. These include: (1) grouping by task sequence, (2) grouping by system function, and (3) grouping by importance and frequency of use.

a. Grouping by Task Sequence - Controls and displays should be assigned to work stations so as to minimize operator movement. To the extent practical, this assignment should consider both normal and emergency procedures. It should be practical to perform all frequently occurring routine tasks, and time sensitive emergency tasks, with a minimum of human movement from panel to panel.

b. Grouping by System Function - Within the constraints of grouping by task sequence, controls and displays should be assigned to panels in functional groups related to system structure. This grouping should promote easy understanding of the relationship between controls and system, and should assist graphic or pictorial display of system relationships.

c. Grouping by Importance and Frequency of Use - Within the constraints of grouping by task sequence and by system function, controls and displays should be assigned to panels depending on their importance and frequency of use. Controls or displays that are neither important to plant safety nor frequently used should be installed in secondary panel locations.

4.2.6.2 Visable and Audible Coding

Coding principles are established in an early stage of HSI design. The coding principles are consistent with guidelines of NUREG-0700R2, which superseded NUREG/CR-5908 . The coding system is consistent throughout the HSI. This applies to location, information, color, and illumination codes. Coding should be consistent between HSI in the MCR, LCS, and back panels. The MCR simulator coding is consistent with the plant MCR. The equipment symbols, abbreviations, and acronyms are defined in the DCD. Use of symbols for coding of components should be consistent with the shapes defined in the DCD. New shapes are defined and documented.

The coding method selected for application is determined considering the relative advantages of the types of coding.

Coding method and guidelines are as follows:

1. Physical Coding

   a. Size coding - Not more than three different sizes are used for discrimination by absolute size.

   b. Shape coding - Number of shapes should be limited in shape coding.

   c. Color coding - The number of colors used for coding is kept to the minimum to provide necessary information. Less than eight colors preferable and not more than 12 colors, including black and white, are used.

      To ensure the correct use of color coding, the following rules should be applied:

      i) Color should be used in a redundant mode. This is necessary to allow for variations in lighting conditions.

      ii) The choice of colors should allow all users to discriminate between each color under all conditions of use.

      iii) The colors used contrast adequately with the background of the display. In addition, adjacent colors contrast adequately with each other.

      iv) Consistency of meaning assigned to each color is essential. The use of color codes with symbols is consistent across all applications within the control room and LCS.

      v) For VDU display, the background color should be pure and free from noise patterning.

      vi) In selecting color codes, common human perception of the color meaning (e.g., red-stop, green-go, etc.) as well as industry standards and practices which have been identified for advanced control rooms are used.

   d. Auditory coding - Auditory coding by frequency is permissible but not more than five separate frequencies should be used. Auditory coding may be implemented based on frequency, rate of change, patterns, and location of auditory device. EPRI has performed studies related to alarm systems and these are considered.

e. Intensity coding - Use of intensity coding should be minimized (i.e., contrast between two characters on a screen) auditory and visual displays.

2. Information Coding

Coding of displays can improve the usability of the information by aiding comprehension and assimilation. The code employed enhances the flow of information from the process to the user and does not require the user to decipher information in order to use it.

The most important factor of the code is to enhance discrimination.

Purely abstract codes such as arbitrary associations of items with data are avoided because they are difficult to learn and use.

3. Location Coding (structuring coding)

The use of consistent relative positioning of information can reinforce the intended message in addition to the information transmitted by a pointer, character, a group of characters or a symbol.

4. Data Coding

A major use of data coding is abbreviations. Abbreviations used on labels, displays and VDU formats should comply with a standardized set of abbreviations based on formal rules which meet the user population needs. Abbreviations are used consistently between VDUs, labels, etc.; coding on VDU displayed information are consistent with coding used on the WDP. This includes the use of colors and abbreviations.

Abbreviations and acronyms for the ESBWR Project are defined in the DCD. New abbreviations or acronyms are identified and documented in the place of use (i.e., document, drawing, etc.).

5. Enhancement coding

Enhancement coding can be used to reinforce the data being transmitted. The available techniques include reverse video and blinking of 3 Hz to 5 Hz on VDU displays and symbol size and style brightness on all types of displays.

4.2.6.3 Labeling

Adequate labeling is provided in the control room. The labeling is consistent with NUREG-0700R2, other labeling in the plant, and in accordance with accepted human factors engineering practices and principles for readability by the user population. Additional guidelines related to labeling may be found in applicable documents in Section 2.

The criteria for the labeling areas should consider the following:

1. Labels should appear on all components, systems and are readily visible by plant personnel.
2. Labels should be designed and mounted so that text is oriented horizontally for ease of reading.
3. The format of presentation (e.g., order, position) should be consistent on all labels.
4. The acronyms and abbreviations should be concise and consistent in all systems, DCDs, drawings, procedures and easily identifiable to the full names.
5. Characters used on labels should be sized for optimum viewing with considerations for the local environment conditions (e.g., illumination).

4.2.7 Information System

Information systems are provided to inform operators of the plant status and variables important to safety and availability. The system also provides information on the plant status for remote on-site and off-site safety experts during accident conditions. During normal operations a rate of appearance of information signals used to derive digital displays of key alarms and steady state values can be on the order of several hundred signal changes per day, which can be handled by normal display systems.

It has been shown through simulator observation and small scale tests that operators cannot read VDU information on alarms faster than about one alarm title every 10 seconds, and their analysis of the implication of patterns of alarms which exists takes longer (several minutes). Therefore, displays need to be designed to identify those cues, which need a positive action, and present them in a way, which does not overload the operators' perceptive ability, and which remains under their control, even at high rates of change of the input information used to generate the displays.

During major transients and plant trips at a nuclear plant the rate of input information signals used to generate display changes increases significantly over steady state conditions. This produces an 'avalanche' or 'flood' of changes to the displays.

Nuclear plants have experienced rates of appearance of changed information of about 1,000 changes appearing in a period of a few seconds. Changes can continue to appear at over 200 changes per minute, several times and for minutes at a time, for up to an hour after a trip. The display system needs to cover the range of rates that are expected.

4.2.7.1 Information Functions

The system has data acquisition, display and alarm functions. The system also has recording and memory functions for the plant process variables important to safety and availability, for analysis and for reporting within the operating organization and external authorities.

Information processing functions should also be provided to support high-level mental processing by the operator as a means of:

- Aiding decision making
- Improving monitoring performance and capability
- Improving availability and reliability of information
- Providing feedback for organization of actions
- Improving communication between staff
- Improving a record of transients and accidents for analysis purposes
- Expanding available information to cover implicit data

The information system provides data acquisition, data processing, display and alarm functions for operators and non-shift support staff. The system also provides recording and printing functions.

The functions defined below are provided in the ESBWR through the HSI in the MCR. Plant status is also available at remote terminals located in the TSC, RSS and the EOF.

1. Information for operators

   In accordance with the design features of the ESBWR, the overall plant status is monitored by MCR operators using information presented on the wide display panel (WDP).

   The operator is able to obtain at any time, detailed plant information, from the information presented in HSI (i.e., VDUs and flat display panels).

Deviations from normal operation are indicated by visual and audio devices. When these occur, the information systems enable the operators to:

a. Recognize any current or potential plant safety or availability hazards

b. Know the actions being taken by automatic systems

c. Analyze the cause of the disturbance and follow its course

d. Determine any necessary manual counteractions

The design basis for information systems, including their measurement devices, takes into account their importance to safety. The intended safety function of each system and its importance in enabling the operators to take proper pertinent actions in anticipated operational occurrences or accident conditions are identified in the SFRA and are used as an input to any MMIS categorization method selected.

2. Information function for non-shift support staff

Although the MCR is the information and control center of the plant for the operators during both normal operation and accident conditions, it may also be used as the primary center to direct the initial stages of off-site activities depending on national, state, local and utility principles for emergency operations support.

Provision is made for three active observers and advisors in the main controlling area of the MCR as follows:

a. Shift Technical Advisor

b. ESBWR Nuclear Unit Plant Manager

c. Communicator

Information systems may be extended to supply information to separate outside support facilities.

3 Printing

An adequate number of printers are provided in or adjacent to the MCR to allow for hard copy output of process variables and chronological information about the performance and behavior of the plant.

Hard copy output of plant variables may be necessary for the following purposes:

a. Backup information for shift operators providing short-term and long-term trends

b. General operational information for plant management

c. Short-term and long term analysis of operation, transients and accidents

4.2.7.2 Distributed Control and Information System (DCIS)

The requirements related to data acquisition and processing systems are covered in the ESBWR DCD Chapter 7, Instrumentation and Control Systems.

The DCIS provides redundant and distributed control and instrumentation data communications networks to support the monitoring and control of interfacing plant systems. These systems include electrical devices and circuitry (such as multiplexing units, bus controllers, formatters and data buses) that connect sensors, display devices, controllers, and actuators which are part of these plant systems. The DCIS also includes the associated data acquisition and communication software required to support its function of plant-wide data and control distribution.

4.2.7.3 Display System

The display system is designed as a HSI of the information system, considering the human capabilities and characteristics of the user population.

1. The major functional requirements of the display system are as follows:

   a. The display system covers appropriate variables, consistent with the assumptions of the safety analysis and with the information needs of the operator in normal operation and accident conditions. The accuracy and range of displays are consistent with the assumptions of the safety analysis.

   b. A display is provided for indicating bypassed or deliberately inoperable conditions of plant and auxiliary systems.

   c. Safety related information displays are suitably located and specifically identified.

   d. Appropriate types of displays are developed depending on the intended purpose for the displayed information.

   e. The display system should also consider support for maintenance, test, and inspection activities.

2. There are many types of displays available such as:

   a. Display with Indicators and Lamps

      Information display arrangements with analog or digital indicators, indication lamp, illuminated graphic symbols, etc., are made based on human characteristics and ergonomic considerations.

      Principles of the location aids such as coding by color, shape, etc., are applied to those indicators, lamps, etc., themselves. Scales of analog indicators and the movement of indication are consistent to changes of relevant process variables and the population human perceptual system capabilities.

   b. VDU Displays

      The major functional requirements for VDU displays are as follows:

      i) Necessary information is available to the operator whenever it is required.

      ii) The display communicates the intended information to the operators without ambiguity or loss of meaning.

      iii) Symbols are standardized and the range of symbol sizes is limited.

      Direction of process flow paths and sequence events in schematic displays should be in accordance with population human perceptual system capabilities and mimics on control room panels.

      VDU displays are designed considering human factors and design criteria shown above and should be compatible with both the associated controls and instrumentation and the perceptual and cognitive needs of an operator.

   c. Large Screen Displays

      Consider using large screen displays when:

      i) A group of operators is required to interact as a team based on the same information.

      ii) One or more operators are required to move about, and require frequent referral to information required to make decisions.

iii) Space or other considerations such as a limited number of individual displays preclude the use of individual displays for each team member to call up the commonly used information.

iv) It may be desirable to have general (e.g., overview or summary) information available to persons who should not interrupt ongoing group operations by looking over the shoulders of individual operators to view their individual displays.

Direct-view or projection VDU systems offer the advantage of allowing use of displays developed for smaller screens. If screen size is limited by space or other considerations, existing displays may be redesigned using larger characters and symbols to achieve the character heights required.

d. Large Wall-Sized Fixed Mimic

The HSI design includes an integrating overview mimic in the MCR. This mimic meets the requirements for integration into the HSI design process.

This mimic is intended to support the operation team approach to control activities by providing a spatially dedicated, continuously available reference to the status of essential equipment controlled in the MCR.

The overview mimic provides for the display of a limited number of critical plant operating parameters. The specific parameters are determined in the design process, to enable the operators to shutdown the reactor as described in Sections 18.4.2.11, 18F and 18G1.4.4 of the ESBWR DCD.

Specific parameters are listed in Section 4.3.5.3.

The overview mimic provides for the display of the system equipment operational status, e.g., flow or no-flow, energized or de-energized, on or off, open or close, etc., of a limited number of essential components controlled or monitored from the MCR. The specific displays are determined in the design process; however, the following are considered for incorporation:

- Feedwater and condensate system pumps
- Containment Isolation valves
- Safety systems valves
- RWCU/SDC pumps and valves

- Power supply breakers
- Auxiliary power supply breakers
- Safety and relief valves
- Circulating water pumps

The overview mimic provides for the spatially dedicated display of certain key alarms or similar alarm-like information which needs to be brought to operator attention. The specific items to be displayed are determined in the HSI design process for the alarm system.

The plant parameters to be displayed on the overview mimic are defined on the WDP Arrangement Drawings.

e. Design

The requirements of a display or suite of displays are determined with a proper and systematic analysis of the proposed use of the data being displayed. For each proposed item of information, the HSI designer should consider the following attributes:

- For whom is the data required? Formats should be structured or revised to meet operator needs.
- For what purpose or purposes is the data required? (e.g., maintenance data are separated from operational data).
- Whether comparisons with other data on VDU formats or other displays are required.
- When is the data required? (e.g., relevance to operator actions).
- The accuracy with which the data are read.
- The characteristics of the data in terms of rate of change, noise, etc.
- What errors of interpretation are acceptable, if any?
- The degree of detail or abstraction which is required.

Following the occurrence of an event or transient only the following should appear as alarms:

- Alert operators to off normal conditions which require them to take action;
- Redirect the operators, to the extent possible, to the appropriate response;
- Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions;
- Minimize distractions and unnecessary workload placed on the operators by the alarm systems.

The location of data display facilities should take into account the intended operational staffing levels, the assignment of operational responsibilities and functions and the need to optimize the number of displays consistent with adequate manning of each operator workstation. The latter consideration is dependent on anthropometric factors such as viewing angle, viewing distance, proximity to associated controls and indications, etc., and amount of data to be referred to.

The HSI design team identifies and documents all bases and assumptions.

f. General requirements of VDU design

Display should be as simple, clear and comprehensible as possible. Where complex or highly detailed displays are necessary, a good organization and structure are required.

The HFE design team uses a HSI design specification to assure that all applicable HFE practices and principles are applied in a consistent manner for all VDU display designs. The specification will assure that the "look and feel" of all of the Graphical User Interfaces (GUI) is consistent. The specification is based on a GUI Style Guide applicable to the HSI.

Where safety criteria require raw, unprocessed data to be presented in addition to the processed information, the display organization and identification differentiate between the two types of information. The HSI design is consistent with the NE_DCIS design specifications and the applicable references for HFE guidelines in Section 2.

i) Availability

Necessary information is displayed to the operator whenever it is required.

ii) Legibility

Information shown on VDU is clearly presented in all operating conditions.

To obtain the necessary legibility of the VDU, the format specification is based on HSI documents and design team recommendations.

iii) Accuracy

The display communicates the intended information to the operator without ambiguity or loss of meaning. The scaling of graphs and histograms enables the operator to resolve indications adequately and the maximum or current value is annotated with the numerical value on the graph. For digital displays, the number of decimal places displayed matches the required accuracy of the measurements.

iv) Consistency

Standardization of displays can be beneficial, but it does not take precedence over the more important criteria defined above.

All items within a suite of displays which represent the same information should be similarly named.

When using the same items on different displays they should be consistent for each display. This includes data fields, symbols, etc. Grouping techniques should be consistently applied with standardized headings and style.

g. Form of presentation, use of symbols and graphics

The most important design principle is to make the display as simple and clear as possible, while not losing either essential detail or important principles and relationships.

The display format needs to consider operator issues in dealing with high rates of information changes during transient and trip conditions. For example:

- suitable logic for prioritizing the information flow is needed to minimize the potential for information overload and

- the time resolution for displays should address realistic operator needs, considering transients in the ESBWR inherently occur slower than in previous BWR plants.

Symbols should be standardized and the range of symbol sizes should be limited to a progression which allows easy recognition of the various sizes.

Related plant items should be organized in a way that reflects their functional relationship with the appropriate degree of abstraction being employed, yet avoid complicating the display. The presentation should be compatible with other related forms of information display within the same location. Use of grouping and coding techniques for enhancement of the perceptions of displayed information is important.

Process flow paths and event sequence should generally progress from left-to-right and from top-to-bottom, in accordance with population human perceptual system capabilities. Schematic displays on the VDUs should be formatted and oriented in accordance with the fixed-position mimic.

Sequence and message construction should present good syntax and where possible a standardized hierarchical message structure should be employed.

The layout of information should reflect the sequence, if any, in which it is used. Rows of tabular information are normally divided into groups of not more than five.

4.2.7.4 Alarm system

1. Alarm System Features

The WDP and MCC alarms provide all the necessary information for surveillance of the plant in off-normal plant conditions. The ESBWR alarm system is a subsystem of the DCIS. This system will:

a. Display alarm information that enables the operator to understand off-normal plant conditions and minimize distraction and unnecessary workload placed on the operators

b. Enable the operator to distinguish between alarms for which corrective actions are not completed and alarms which cannot be canceled without the intervention of the maintenance service (e.g., component being shutdown for maintenance)

c. Perform processing functions, to give the operator the most representative information of abnormal conditions

d. Display functions, to permit the operator to easily identify each alarm, its seriousness and, to the extent possible, cue the operators to the appropriate response

e. Provide the capability for the operators to periodically confirm that it is functioning properly, i.e., test alarms.

f. Assure visual consistency between all forms of displays (e.g., light boxes, status lights, and various VDUs.)

g. Minimize nuisance alarms

Moreover, for each alarm, a procedure document, (e.g., alarm sheet or alarm response procedures (ARPs) is provided to explain to the operator the likely reasons of the alarm and the corrective actions required. Computer based operator aids may be used for explaining the importance of particular combinations of alarm signals.

2. Display of Alarms

The display of alarms on alarm-tiles or on VDUs meets the following:

a. An alarm is annunciated where the operator has the necessary means for initiating corrective actions;

b. Any new alarm starts an audible warning and flashes a tile light or VDU symbol;

c. An alarm may be steadied after it has been acknowledged;

d. The steadied alarm is indicated to ensure that its existence is not forgotten;

e. When the cause of alarm has been corrected, the alarm display may be returned to the normal mode manually or automatically. In either case, the control room staff is notified by audible and visual cues that the cause has been corrected.

4.2.8 Controls

Controls are used for manual control operations as well as for backup to automatic control operations under both normal and abnormal operations. Maintenance, test, and inspection tasks are also considered in the design process. Controls are designed to ensure ease of operation and to minimize operator errors..

Controls for ESBWR can be separated into two categories. The first category includes control functions that must be converted into hardware devices to automatically control power, flow, pressure, level etc. to match plant conditions. The second category of control elements provides support to manual controls that have been identified in the HFE analysis process. Those displays, controls and alarms are identified in the task analysis and HSI reports.

1. Control Elements

   Mechanical characteristics of control elements, such as size, operating pressure of force, tactile feedback, etc., meet capabilities and characteristics specified in the anthropometric database.

2. Ergonomic Consideration

   The controls selected are suitable for operator use in the MCR and RSS environment and match the ergonomic characteristics of the expected user population.

   Controls meet the following requirements:

   i) To minimize operator error, control movements will conform to population human perceptual system capabilities;

   ii) Maintain consistency for color, shape and size coding, control movements, as well as selection of controls for similar control functions;

   iii) Placement of controls in keeping with their conformance to safety functions.

3. Prevention of Erroneous Activation

   Erroneous activation of controls is minimized by means such as locating controls at proper positions, use of fixed protective structures, i.e., movable covers or guards, interlocking controls, application of priority of actuation or the combination of two selected control actions by the operator to initiate a plant operation.

4. Computer Aided Functions

   Computer aided functions are introduced for controls, where possible, as operator aids to prevent erroneous actuation. This is accomplished by means of a sequential logical actuation interlock or an operator guide with the computer aided display system.

4.2.9 Control-Display Integration

Controls and their associated displays are correctly integrated to ensure effective operation of the plant. Control-display integration is in accordance with the proposed method of plant operation as identified in the operators analysis performed for each system by the HFE Design Team.

The control-display integration meets the following principal requirements:

1. Hardware controls should be located near the associated display. Operation of controls should produce a compatible change in the relevant display.
2. The operation of systems and components by "soft" and "hard" switches. Soft switches are controls located in the VDUs.
3. The form of control adopted is consistent with HSI requirements.
4. The grouping of controls and their associated displays reflect the need to achieve system objectives that are consistent with the user's mental thought process.
5. Where sequence of use is a key factor, the organization of controls and displays reflects cause/effect relationships.
6. The organization of controls takes into consideration any user population stereotype groupings.
7. The form of codes used for displays and their associated controls is consistent between the MCR and RSS.

For a touch screen, each selectable item or region is a minimum of 15 mm on a side to allow for finger size and parallax inaccuracy.

4.2.10 Communication System

Communication systems are provided to facilitate safe and efficient plant operation. Consideration is given to the design of communication systems to be used in the abnormal or accident conditions to communicate with the emergency facilities.

Access and changes to the communication system should be administratively controlled.

Provision of nonverbal communication systems such as data-links (between computers), and other forms of message systems are desirable, between the control room, and other emergency facilities in order to provide secondary (backup) communications.

The communication systems are designed in accordance with accepted HFE principles, practices and guidelines as defined in the applicable documents in Section 2.

1. Verbal Communication Systems

   a. On-site Telephone Communications

      For general communication under normal operating conditions, a telephone system with a necessary number of extensions is installed. The telephone system allows the operations staff to preprogram telephone numbers. The number of extensions provided in the control room is based on the MCR operational requirements. The MCR and TSC telephone systems are designed in accordance with regulatory requirements for emergency response facilities (EOF). Capability is provided for communication among operators and maintenance technicians using portable, wireless communication equipment supported by appropriate base stations, antennas, amplifiers and/or repeaters. The voice communication systems are designed in accordance with operating utility requirements.

      Voice communications systems and equipment are provided to support all phases of operations and maintenance, including emergency operations.

   b. Plant-wide Paging and In-plant Telephone System

      A page system is provided to give capability of plant-wide paging of personnel. This paging system reaches all areas of the plant (i.e., no dead areas).

      For use during maintenance, testing or repair, communication by radio to the control room using mobile transmitters is provided, unless all relevant local points can be reached by other systems.

      Operating radio frequency interference analysis is considered in the design, cabling, location and testing of the I&C systems. Areas where transmitters may not be used, such as the control equipment room, are identified and appropriate warning signs posted.

c. Off-site Communications

A speech and/or computer-based system is provided for communication to the off-site authorities and emergency, governmental and public agencies. These systems are designed to meet local requirements.

d. Local Arrangement

The MCR is also designed as the communication center of the plant for normal operation and during the early stages of an accident. Communications equipment for communicating with locations off-site should be located on a special communication desk or panel with extensions on the MCR desk and other locations as appropriate.

For TSCs or EOFs, the equipment is designed to permit information transmission according to the specified tasks for these locations.

2. Non-verbal Communication Systems

Non-verbal communication systems between the control room and emergency facilities will be available in accordance with utility administrative controls for distribution of plant information. Data communication links between computers in the MCR and emergency facilities will be in accordance with utility administrative controls.

4.2.11 Other

1. Utilization of computers

Computers, are provided to enhance the man/machine interface capability, and will meet the following:

a. Computer system failure will not lead to any loss of plant safety function.

b. The computer system is designed not to cause or require plant trip following a single failure of the computer. Care is taken to minimize the consequence of common mode failure.

c. Hardware and software are designed to facilitate modification changes after initial installation.

d. Ease of verification and validation of hardware and software is considered during the HSI design process.

2. Power Supplies

   Power supplies for the HSI meet reliability and availability objectives consistent with those requirements for systems important to safety in the HSI, i.e., systems which are required to be available for use at all times during operation or accident conditions and are connected to non-interruptible power supplies.

3. Qualification

   A qualification program is provided to confirm that safety-related equipment and systems in the HSI are capable of meeting, on a continuing basis, the design basis performance requirements (e.g., range, accuracy, response) needed for functioning under the design basis environmental conditions. The program includes a plan to ensure that the equipment is qualified for the intended period of use, and provide for timely requalification or replacement, if necessary. The ESBWR HSI consists of hardware controls and software controls located on VDUs and/or FPDs. Those safety systems displayed and controlled using FPDs are appropriately qualified.

4. Maintainability

   The HSI are designed to facilitate surveillance, testing, maintenance, and failure diagnosis and associated repair or replacement. Methods provided for maintenance of the systems are designed so that plant safety will not be affected. Access clearances are based on criteria specified in applicable references in Section 2.

5. Repairs

   The HSI are designed, considering panel layout and equipment configuration, to ease repair of the equipment. HSI components are selected in accordance with standardization guidelines and in consideration of repair facilities and spare parts.

6. Testability

   The HSI are designed to permit test and calibration of the necessary functions, without difficulty, at necessary intervals.

4.3 Main Control Console HSI

The work station for the two licensed reactor operators that operate the controls in the MCR is the MCC. It is configured such that each operator is provided with controls and monitoring information necessary to perform assigned tasks and allows the MCR operators to view all of the displays on a WDP from a seated position.

The design of the information and controls located at the operator sit-down workstation is integrated with the design of the mimics displayed on the wide display panel (WDP) for consistency in nomenclature, symbols, and color.

The HSI design will include features which facilitate operator activities that tend to keep the operators alert and attentive. Features of the HSI are designed based upon applicable industry research and publications to assure operator vigilance. The basis for the features, including a review of the experience of selected HSI features, is part of the documented design.

The MCC, in concert with the WDP (based on the referenced Japanese ABWRs), provides the controls and displays required to operate the plant during normal plant operations, abnormal events and emergencies. The MCC controls and displays include the following:

1. Non-safety related on-screen control VDUs for non-safety system control and monitoring, and safety system monitoring, driven by the NE-DCIS.

2. Safety-related on-screen control VDUs for safety system control and monitoring, driven by the E-DCIS. The operation of these VDUs is fully independent of the DCIS.

3. Fixed-position, dedicated function switches.

The MCC design does not contain fixed-position displays because the standard ESBWR design does not require them at the MCC. All fixed-position displays (FPD) are located at the WDP based, in part, on the rationale for fixed-position displays (such as diversity) and the relatively compact configuration of the MCC. The MCC is also equipped with both interplant and external communications equipment. The minimum set of controls, displays and alarms, based upon a review of the ESBWR EPGs, have been allocated to the MCC and WDP.

4.3.1 VDUs Driven by the NE-DCIS

A set of on-screen control VDUs is incorporated within the MCC for the following functions and tasks:

1. Monitoring of plant systems, both safety and non-safety related

2. Control of non-safety related system components

3. Presentation of system and equipment alarm information

The NE-DCIS displays and controls non-safety systems, including the alarm system. The NE-DCIS is independent from the safety related safety systems and their associated processors. All systems, safety and non-safety may be displayed on the non-safety VDUs, but safety systems may only be controlled from the safety system VDUs. Moreover, non-safety parameters may not be displayed on safety related FPDs.

4.3.2 VDUs Driven by the E-DCIS

Safety related VDUs that are physically separate, and functionally independent, of the NE-DCIS are installed within the MCC. The VDUs are dedicated, divisionally separated devices, qualified with their supporting display processing equipment, to Class 1E standards. These VDUs are only used for monitoring and control of equipment within a given safety division.

4.3.3 Fixed-Position, Dedicated Function Switches

Fixed-position, dedicated function switches are installed on the MCC. The switches are implemented in hardware, so that they are located in a fixed-position and they are dedicated in the sense that each individual switch is used only for a single function, or two very closely related functions (e.g., valve open/close). The dedicated function switches provide faster access and feedback compared to that obtainable with soft controls. Assigning functions to fixed-position switches based on established criteria is part of the HSI design implementation process.

Some of the dedicated function switches are for actions such as initiation of automated sequences of safety and non-safety related system operations, manual scram, and reactor operating mode changes The fixed-position function switches on the MCC are identified on the MCC Panel Arrangement Drawing.

4.3.4 Automation Design

The ESBWR incorporates selected automation of the operations required during normal plant startup/shutdown and during normal power range maneuvers.

The Plant Automation System (PAS) is the primary ESBWR system for providing the automation features for normal ESBWR plant operations.

1. Automatic Operation

   During transitions between plant operation modes, the PAS, when in automatic operation, will perform sequences of automated plant control operations by sending mode change commands and setpoint changes to lower level, non-safety related plant system controllers. The PAS cannot directly change the status of a safety related system. When a change in the status of a safety related system is required to complete the selected operation sequence, the PAS provides prompts to guide the operator in manually performing the change using the appropriate safety related HSI controls provided on the MCC.

The operator can stop an automatic operation at any time. The PAS logic also monitors plant status, and will automatically revert to manual operating mode when a major change in plant status occurs (e.g., reactor scram or turbine trip). When such abnormal plant conditions occur, PAS automatic operation is suspended and the logic in the individual plant systems and equipment directs the automatic response to the plant conditions. Similarly, in the event that the operational status of the PAS or interfacing systems changes (e.g., equipment failures), operation reverts to manual operating mode. When conditions permit, the operator may manually re-initiate PAS automatic operation.

Evaluation of the effects of automation strategies on operator reliability and the appropriateness of the automation design are confirmed in accordance with the system design requirements and the user performance criteria established in accordance with the Human Factors Verification and Validation Implementation Plan. The results of the evaluation are placed in the HFE Issue Tracking System.

2. Semi-Automated Operation

   The PAS also includes a semiautomatic operational mode which provides automatic operator guidance for accomplishing the desired normal changes in plant status; however, in this mode, the PAS performs no control actions. The operator must activate all necessary system and equipment controls for the semiautomatic sequence to proceed. The PAS monitors the plant status during the semiautomatic mode in order to check the progression of the semiautomatic sequence and to determine the appropriate operator guidance to be activated.

3. Manual Operation

   The manual mode of operation in the ESBWR corresponds to the manual operations of conventional BWR designs in which the operator determines and executes the appropriate plant control actions without the benefit of computer-based operator aids. The manual mode provides a default operating mode in the event of an abnormal condition in the plant. The operator can completely stop an automated operation at any time by simply selecting the manual operating mode. The PAS logic will also automatically revert to manual mode when abnormal conditions occur.

4.3.5 Wide Display Panel (WDP)

The WDP provides information on overall plant status with real-time data during all phases of plant operation. The information on the WDP can be viewed from the MCC and the shift supervisors' console. All displays on the WDP are legible to operators, either standing, or seated behind the MCC.

The WDP is approximately 3 m high and 10.5 m wide. It has three major components; the fixed-position (mimic) display, the top-level alarm display, and the large VDU. Fixed-position alarm tiles are positioned in the top portion of the fixed-mimic display. The WDP includes fixed-position displays, a large variable display and fixed-position (spatially dedicated) alarm windows which present safety related information and are qualified to standards for Class 1E equipment. The WDP may contain fixed-position, dedicated function switches pending final analysis of operator tasks. Any fixed-position function switches on the WDP are identified on the WDP Panel Arrangement Drawing.

4.3.5.1 Fixed-Position Displays

The fixed-position displays are digitally controlled, optoelectronic devices dedicated to displaying single, alphanumeric or graphical, items of information. There are two sets of fixed-position displays, and each set of displays is driven by its own group of processors (display controllers) as explained below:

1. Safety related devices are one set of fixed-position displays that are qualified to Class 1E standards, along with their supporting display controllers. These safety related fixed-position displays provide the operators with a set of diverse displays for confirming critical parameters independently of the safety related VDUs. This set of fixed-position displays is physically separate, and functionally independent, of the NE-DCIS that includes the second set of fixed-position displays discussed next.

2. Non-safety related devices along with their display controllers are a second set of fixed-position displays that are not qualified to Class 1E standards. These displays are driven by the NE-DCIS. This second set of fixed-position displays is used for critical plant parameter information, as defined by the SPDS requirements of NUREG-0737, Supplement 1 and the Type A post-accident monitoring (PAM) instrumentation required by Reg Guide 1.97.

Assigning functions to fixed-position displays based on established criteria is part of the HSI design implementation process. The fixed-position displays on the WDP are identified on the WDP Panel Arrangement Drawing. Any fixed-position displays on the MCC are identified on the MCC Panel Arrangement Drawing. Human factors aspects related to safety system status monitoring (Item I.D.3 of NUREG-0660) will also be addressed as part of the detailed HSI design implementation process.

4.3.5.2 Large Variable Display

The large variable display at the WDP is a set of four VDUs driven by the DCIS. The four VDUs can be used to display four different video images simultaneously, or they can be operated synchronously to display one large, composite video image. Any

VDU image resident in the DCIS (e.g., those used for VDUs at the MCC) can be shown on this large variable display.

4.3.5.3 Safety Parameter Display System (SPDS)

The principal purpose of the SPDS is to aid control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether abnormal conditions warrant corrective action by operators to prevent core damage. During emergencies, the SPDS serves as an aid in evaluating the current safety status of the plant, in executing symptom-based emergency operating procedures, and in monitoring the impact of engineered safeguards or mitigation activities.

The SPDS is required to be designed so that the displayed information can be readily perceived and comprehended by the MCR staff. Compliance with this requirement is assured because of the incorporation of accepted HFE principles into the overall implementation process. All of the continuously displayed information necessary to satisfy the requirements for the SPDS, as defined in NUREG-0737, Supplement 1, are included in the fixed-position displays and the SPDS design and implementation are evaluated against the requirements of Paragraph 3.8a of NUREG-0737, Supplement 1, to confirm that all applicable criteria are met. Selection of the parameters for inclusion in the SPDS display is based, in part, upon the ESBWR emergency procedure guidelines (EPGs). The SPDS also operates during normal operation, continuously displaying information from which the plant safety status can be readily and reliably assessed. Principal functions of the SPDS are integrated into the overall control room display capabilities in a manner which complies with of NUREG-0737, Supplement 1.

Displays of critical plant variables, sufficient to provide information to plant operators about the following critical safety functions, are continuously displayed on the WDP as an integral part of the fixed-position displays:

- Reactivity control
- Reactor core cooling and heat removal from the primary system
- Reactor coolant system integrity
- Radioactivity control
- Containment conditions

Displays to assist the plant operator in execution of symptom-based emergency operating procedures are available at the MCC VDUs. Examples of these VDU displays are trend plots and operator guidance. Information regarding entry conditions to the symptomatic emergency procedures is provided through the fixed-position display of the critical plant parameters on the WDP. The critical plant parameters on the WDP are also viewable from the shift supervisors' console. The supplemental SPDS displays on the VDUs on the MCC are also accessible at the shift supervisors' console and may be provided in the TSC and, optionally, in the EOF. The SPDS displays are available to be displayed on display equipment defined by the utility.

Entry conditions to symptomatic emergency operating procedures are annunciated on the dedicated hardware alarm windows on the WDP. The WDP also displays the containment isolation status, safety systems status, and the following critical parameters:

- RPV pressure
- RPV water level
- Core neutron flux (startup range and power range instruments)
- Suppression pool temperature
- Suppression pool water level
- Drywell temperature
- Drywell pressure
- Drywell water level
- Control rod scram status
- Drywell oxygen concentration (when monitors are in operation)
- Drywell hydrogen concentration (when monitors are in operation)
- Wetwell oxygen concentration (when monitors are in operation)
- Wetwell hydrogen concentration (when monitors are in operation)
- Containment radiation levels

The oxygen monitoring instrumentation system is normally in continuous operation and, hence, the WDP includes continuous fixed-position display of wetwell and drywell oxygen concentrations. The hydrogen monitoring instrumentation is automatically started on a loss of cooling accident signal and, hence, continuous display is not required. Additional PAM parameters, such as effluent stack radioactivity release, may be displayed on demand by operator choice on either the large variable display or the MCC VDUs.

4.3.6 Fixed-Position Alarms

Fixed-position alarm tiles on the WDP annunciate the key, plant-level alarm conditions that potentially affect plant availability or plant safety, or indicate the need for immediate operator action. The fixed-position alarms on the WDP are identified on the WDP Panel Arrangement Drawing.

4.3.7 Alarm Processing Logic

Alarm prioritizing and filtering logic enhances the presentation of meaningful alarm information to the operator and it reduces the amount of information which the operators must absorb and process during abnormal events. Alarm prioritizing is accomplished through three categories of alarm signals. The first is important alarms which notify the operators of changes in plant status regarding safety, and include items that are to be checked in the event of accidents, principle events or transients. The important alarms are displayed on the fixed-position tiles.

The second category of alarm signals is the system-specific alarms which are provided to notify the operators of system-level abnormalities or non-normal system status. The system-specific alarms are also shown on the fixed-position tiles. Examples of these are:

- Feedwater pump trips caused by system process, power sources or control abnormalities.
- Valve closures in cooling or supply lines
- Decreases in supply process values
- Loss of a backup system
- System isolation
- Safety systems are being bypassed

Equipment alarms are the third category of alarms in the prioritizing scheme.

Alarm suppression is based upon the following concepts:

- Suppression Based on the Operating Mode: The plant operating mode is defined on the basis of the hardware or process status, and alarms which are not relevant to the current operating mode are suppressed. For example, alarms which are needed in the "RUN" mode but are unnecessary in the "SHUTDOWN" mode are suppressed.

- Suppression of Subsidiary Alarms: Alarms are suppressed if they are logically consequent to the state of operation of the hardware or to the process status. For example, scram initiation (a plant-level alarm condition announced with a fixed-position alarm tile on the WDP) will logically lead to scram accumulator low pressure (also an alarm condition). Such subsidiary alarms are suppressed if they simply signify logical consequences of the system operation.

- Suppression of Redundant Alarms: When there are overlapping alarms, such as "high" and "high-high" or "low" and "low-low", only the more severe of the conditions is alarmed and the others are suppressed.

4.3.8 Equipment Alarms

Alarms which are not indicated by fixed-position alarm tiles on the WDP (i.e., those alarms of nominally lower level importance such as those related to specific equipment status) are displayed by the MCC VDUs. The supplemental alarm indications and supporting information regarding the plant-level alarms which are presented on the WDP are also presented on the VDUs.

4.3.9 Shift Supervisor's Console

The console provided for shift supervisors is equipped with VDUs. Any screen format (image) available to the operators at the MCC is also available to the shift supervisor.

4.4 HSI Technology

4.4.1 Introduction

Due to increasing regulatory and utility requirements, and demands for greater plant availability, it is necessary to incorporate in future plants, innovative designs reflecting advances in computer-based technology. In recent years, the major NSS vendors have been developing control complexes that make use of computers to process plant parameter data and display information to personnel. Computer based applications reduce the number of hardwired instruments needed to provide information about plant operations. In addition, computer-aiding routines can be incorporated to unburden plant personnel, thereby allowing them to direct their attention to monitoring, and analysis and decisions regarding plant operations.

4.4.2 HSI Technology Application

The MCR standard design features include equipment based on various HSI technologies for plant process control and monitoring. A summary listing and description of the applied HSI technologies follows below. The term "technology" is defined as the equipment, including both hardware and software, employed to directly accomplish the functions of control and monitoring of the plant processes. The list excludes equipment for support functions such as panels, cabinets, control room lighting, air conditioning, and plant communication equipment.

1. Hardware switches such as multi-position rotary, push-button, rocker, toggle and pull-to-lock types.

2. Soft switch, the functions of which may be changed through the execution of software functions

3. Continuous adjustment controls, such as rotary controls and thumbwheels (for remote shutdown panels but not for MCR)

4. VDUs with full color screens, including large reverse projection screens, cathode ray tubes and flat panel display screens.

5. On-screen control utilized with VDU and FPD devices.

6. VDU screen formats such as large screen optical projection display formats; text displays, including menus, tabular information, and graphical displays, including trend plots, 2-D plots, P&IDs and other diagrams and pictorial information.

7. Analog meters which employ a hardware medium to pictorially or graphically present quantitative and qualitative information concerning plant process parameters. This includes analog meters using digitally controlled light-emitting diodes (LEDs) and digital readouts .

8. Fixed-position digital displays which present alphanumeric information in a hardware medium. These can be backlit.

9. Fixed-position hardware mimic displays which schematically represent plant systems and components and their relationships utilizing pictorial elements, labels and indicator lights.

10. Fixed-position alarm tiles which use light to indicate the alarm state.

11. An audio signal system which is coordinated to the fixed-position alarm tiles and utilizes prioritization and alarm reduction logic and predefined setpoints to alert operators to plant status changes.

12. Printers and printer/plotters used to provide hard copy output in the form of plots, logs and text.

13. Keyboards which are composed of alphanumeric and/or assignable function keys and function as computer input devices.

4.4.3 Minimum Displays, Controls and Alarms

The Emergency Procedure Guidelines (EPGs), and the important operator actions identified in the Probabilistic Risk Assessment (PRA) or other studies, provided the bases for an analysis of the information and control capability needs of the MCR staff. The analysis defined a minimum set of controls, displays, and alarms which will enable the MCR staff to perform the actions that would be specified in the emergency operating procedures and the important operator actions identified in the PRA. The information and controls identified from that analysis do not necessarily include all those from other design requirements (such as those from SPDS).

4.5 Requirements Developed from Operations Analyses

Operations analyses (system functional analysis, allocation of functions and task analysis) results are used in the design of the HSI.

Figure 8 shows how the system functional requirements analysis, allocation of functions and task analysis implementation plans are interrelated and provide input to the HSI design.

The system functional requirements analysis determines the performance requirements and constraints of the HSI design and establishes the functions which must be accomplished to meet these requirements.

The allocation of functions is done to take advantage of areas of human strengths and avoid allocating functions to personnel which would be impacted by human limitations. The allocation of functions to personnel, systems or personnel-system combinations is made to reflect: sensitivity, precision, time and safety requirements, required reliability of system performance and the number and level of skills of personnel required to operate each system.

The task analysis will identify the behavioral requirements of the tasks associated with individual functions. Task analysis will provide one of the bases for making design decisions; e.g., determining before hardware fabrication, to the extent practicable, whether system performance requirements can be met by combinations of anticipated equipment, software and personnel; assure that human performance requirements do not exceed human capabilities; be used as basic information for developing manning, skill, training and communications requirements of the system; and form the basis for specifying the requirements for the displays, data processing and controls needed to carry out the tasks.

The types of task requirements information that are identified in the Task Analysis Implementation Plan, include:

1. Information and Decision-Making Requirements
2. Response Requirements
3. Feedback required to monitor and evaluate the adequacy of actions taken.
4. Cognitive, physical and difficulty level of workload
5. Task Support Requirements
6. Workplace Factors
7. Staffing and Communication Requirements
8. Potential Hazard Identification.

The HSI design is based on the staffing requirements defined in the staffing and qualification plan. The MCR staff, size and roles are finalized after the completion of the MMIS V&V activities.

4.6 HSI Design Methodology

A summary of the HSI design process (Figure 2) is presented in the following steps:

Step 1: *Workspace and Environmental Conditions Design*

The external MCR and RSS display features are defined. (e.g. (MCR dimensions, Consoles, etc.)

Step 2: *Panel Layout Design*

The components to be mounted on the MCR and RSS panels and console, and their organization and arrangement are defined.

Step 3: *Alarm and Annunciator System Design*

The alarm and annunciator system are defined.

Step 4: *Displays and Control Design*

The information and controls requirements derived from the analysis of operations and other inputs (Figure 2) are implemented into the MCR and RSS components.

Step 5: *Communication System Design*

Design aspects of a communication system are defined.

4.6.1 Workspace and Environmental Conditions Design

The proposed dimensions for the MCR and the consoles are defined to assure that the MCR arrangement allows for the necessary support staff work areas. Initial minimum requirements were based on the EPRI NP-5795, 1991. The arrangement may be modified in accordance with the detailed human factors analysis and utility requirements.

Human factors specialists work closely with other development team participants and confer with architect-engineers to identify design constraints to help define the size and shape of control room. They help to coordinate control system engineering concerns with layout alternatives, suggesting advantageous console configurations and profiles and recommending arrangements of major furnishings. Human factors specialists also interact with lighting system engineers, heating and air-conditioning engineers, decorators, and other design specialists responsible for decisions that will influence environmental conditions and other aspects of control room habitability. They also assess preliminary layouts, identifying potential performance degrading effects of design features and recommending ways to overcome them. They are given sign-off authority for drawings at each step in control room design to ensure that human factors issues are adequately addressed.

MCC profiles that are compatible with task requirements have been defined in DCD Chapter 18. Interactive implications of proposed MCC profiles and configurations for control room size and shape are assessed. The MCC profiles and dimensions must be consistent with the defined user population, regulatory criteria e.g., NUREG 0700R2 and the utility requirements. General requirements for ambient environmental conditions in the control room are defined as well as recommendations for preliminary layout of the MCR.

The steps included are the following:

1. Define Proposed MCR Dimensions

   The MCR is as compact as possible while accommodating all necessary equipment and allowing for freedom of movement in performing assigned tasks. A compact MCR reduces walking and viewing distances associated with task performance, enhances unaided voice communications, and discourages incursions by unauthorized visitors

a. Identity architectural-engineering constraints.

b. List major equipment that must be accommodated.

c. Estimate required floor space with dimensions.

2. Define Proposed MCC Configurations

Basic types of console configurations may be characterized as circular, U-shape, wing shape, or L-shape.

The main control room panel (MCRP) System Design Description (SDD) presents the MCR, MCC and the large display panel design based on the ESBWR DCD and the ESBWR Standard Plant Design Program. To define proposed MCR configurations:

a. Consider advantages and disadvantages of different types of configuration using results of task analysis.

b. Select proposed MCR configurations

3. Define Proposed MCC Profiles

a. Determine appropriateness of standing, seated, or sit-stand console profiles

b. Adjust profile for operator viewing

c. Determine relation to console profiles in other plant locations

d. Select proposed MCC profiles

4. Assess Interactive Implications of Proposed MCC Selections

5. Define General Requirements for Ambient Environmental Conditions

Human engineering principles and criteria are applied to design of work environments. Drawings, specifications and other documentation for work environment, MCR staff, facilities and MMIS reflect incorporation of human engineering requirements under normal, abnormal and emergency conditions.

After proposed MCC configurations and profiles have been defined, and their iterative implications for MCR size and shape have been assessed; the ambient environmental conditions necessary to support personnel performance are generally defined as follows:

a. Determine lighting requirements

b. Identify ways to moderate sound

c. Consider influences of surface properties in the control room

d. Specify climatic conditions

6. Produce Recommendations for MCR Preliminary Layouts

   a. Consider the criteria included in the applicable regulatory guidelines, and utility requirements in preparing MCR preliminary layout recommendations:

   b. Locate operator furnishing in relation to consoles.

   c. Provide access space, e.g., for repair and testing activities.

   d. Ensure adequate storage space for MCR staff and safety equipment.

   e. Locate provisions for shift supervisor's activities.

   f. Establish means for limiting visitor access.

   g. Locate personal conveniences, e.g., restroom, locker, kitchen.

   h. Locate aisle way doors for personnel passage.

7. Review of Alternative Designs by HFE Team

8. Define Dimensions for Selected MCC Profiles

9. Define Detailed Design Features for Desks and Other Furnishings

10. Identify Hazard Avoidance Features

11. Define Specific Lighting Features

4.6.2 Panel Layout Design

Panel layout design is conducted in the following series of steps:

1. Define an approach for organizing panel areas to reflect the results of the operations analyses, mock ups, walk through, desktop analysis, etc.
2. Identify general requirements for panel layouts through labeling, demarcation and coding.
3. Select basic instrument types that satisfy information and response requirements and are compatible with panel design concepts.
4. Determine strategies for preventing accidental activation of controls and reflect in the controls selection.
5. Define conventions for the use of color in panel designs.
   a. Identify potential color applications in panel designs.
   b. Select a limited number of candidate colors and define associations.
   c. Consider use of color combinations in labeling, demarcation and mimic designs.
6. Establish labeling conventions.
7. Consider applicable criteria included in Section 2. References
8. Establish requirements for spatial separation of instruments.
9. Establish conventions for lines of demarcation and mimic designs.
10. Establish component coding conventions for instruments and produce recommendations for panel layout.

4.6.3 Alarm and Annunciator System Design

Alarm and annunciator system design is based on a coherent, consistent rationale for alerting and informing personnel about various kinds of deviant plant conditions. An effective system distinguishes the nature of alarm conditions according to established criteria and, using either a code associated with the alarm or an annunciated message, provides information that is a basis for subsequent action. The system takes full advantage of what's known about functional dependencies in plant operations, and presents information in ways that are compatible with human capabilities and limitations.

To avoid unnecessary imposition of design constraints, alarm and annunciator system design is initiated soon after panel layout design efforts are underway. Human factors efforts are coordinated with those of other development team participants.

The alarm system is designed in accordance with the criteria of NUREG-0700 R2, and utility requirements. The design and placement of alarm and annunciator system displays and controls must be responsive to workspace design constraints.

The WDP alerts the operator with a problem related to system or plant level alarms. These visual and auditory cues then focus the operator to a specific system or systems. For detailed alarm information, the operators then view specific information for the alarm message on a VDU or FPD.

Extensive use of VDUs and FPDs in the MCR reduces the use of fixed alarm windows.

The annunciator philosophy for the ESBWR design, and the annunciator warning system, is based on the concepts presented in the ESBWR DCD. The reference documents in Section 2 provide additional information for annunciator warning system design.

4.6.4 Displays and Controls Design

Good design specifications for hardwired displays and controls, VDUs, FPDs and other control devices (i.e., keyboard, touch sensitive, etc.) help to ensure that features of displays and controls procured for use in the MCR support required task performance. Effective display and control designs facilitate reliable information transfer between plant staff and sensor or actuation elements in equipment components.

The following steps are involved in addressing design of displays and controls:

1. Establish specifications for display/control movement relationships

2. Establish standards for quantitative scale designs

3. Define applications to verify readings (i.e., rapid assessment of acceptabilitiy of displayed values)

4. Review preliminary MCC design decisions to verify that appropriate varieties of display and control instruments have been selected.

5. Define Features for Indicator Light, Counter, and Meter Design in accordance with HFE Guidelines.

6. Design of Computer-Generated Displays

   Establish a systematic procedure for defining and designing computer-generated displays. The process is illustrated in Figure 3 and is briefly described in the following steps.

a. Conceptual Design

Develop a display system conceptual design based on information from plant and process flow diagrams. Perform Preliminary allocation of primary and backup mode operation to operator or machine for the following functions:

- Safety and protection
- Monitoring
- Loop control
- Procedure execution
- Supervisory control
- Diagnosis and remedial action

Assign functions to the display system within the areas listed above.

Establish display organization approach to be used for each primary and backup mode consistent with the ESBWR display hierarchy for VDUs shown in Figure 9.

Establish preliminary display characteristics design conventions, such as:

- Format and layout
- Coding (color, dynamics, size, etc.)
- Nomenclature, labeling, and identification technique(s)

b. Information and Control Requirements Definition and Synthesis

Taking into account the information and control requirements obtained from operations analysis, determine the type and number of display types to be used for each information requirement and select information presentation techniques appropriate to the information to be conveyed.

Determine technique(s) to be used to control the display system, including:

- Method for accessing display pages
- Changing display parameters
- Responding to alarms
- Changing controller state (e.g., ON/OFF, OPEN/CLOSED)
- Method of configuration control

- Restriction of system use to authorized personnel

c. Specification of Pictures

- Assemble required information for operator functions and tasks into a display structure.
- Develop sketches of information presentation techniques for required information.
- Combine information presentation techniques onto display frames.

d. Identification of Constraints

Identify plant-specific constraints on:

- Display system implementation:
- Space and location
- Power availability
- Operating environment
- Signal access
- Use of existing display equipment
- Demands of operator
- Industry standards, guidelines, and regulatory requirements
- Maintenance requirements

e. Specification of Displays/Hardware/Software

- Determine if display frames can be implemented within constraints.
- Determine hardware system requirements.
- Determine software requirements.
- Determine user-display dialogue.
- Write specifications for the hardware/software/display system design.

4.6.4.1 Features for VDU Display and FPD Design Specifications

for graphical user interface (GUI) is prepared and is used as design input to the NE-DCIS for human system interface (HIS). This helps to ensure consistency in VDU and flat panel displays (FPD) designed by different team participants or suppliers. The GUI style guide applies to GUI displays used in the MCR for both VDUs and FPDs and GUIs used at safety related local panels in the plant.

Features for Computer Processing Control Design Specification

4.6.4.2 Features for Computer Processing Control Design Specifications

The requirements for operator interaction with the VDU or Flat Panel Display GUI are identified in the Style Guide for Graphical User Interfaces. The style guide defines the requirements for touch screen interfaces. The design specification for the dynamic or static icons (display primatives) displayed to the operator on the VDUs or FPDs are specified in the Display Primatives Design Specification. This document is maintained and revised during design of the GUI. The icons defined in the specification are based upon the system engineering Piping & Instrumentation Diagram (P&ID) symbols. Selected symbols not found in the P&ID library such as bar graphs for tanks, etc., are added to the specification as necessary. The Display Primatives Design Specification is intended to maintain the consistency of "look and feel" and configuration of the GUI. The Specification also defines the control pads, tagout, lockout, and pull-to-lock functions associated with applicable valves or rotary equipment.

4.6.4.3 Display System Implementation

1. Paper Displays of Operator HSI

   Figure 1 defines the overall process for the development, verification, and validation of the MCR and LCS operator interfaces. The paper displays for each system are reviewed by the system responsible engineers, HFE, operations, operators, and other members of the CRDT. These paper versions of the HSI are inputs to those who build the displays.

2. Dynamic HSI

   The displays are built to the specification of the design input, including spacing, colors, etc. As illustrated in Figure 1, the displays now appear as they would in the MCR VDUs or FPDs. Using stand alone VDUs or FPDs the proposed displays are reviewed for technical accuracy, HFE criteria and consistency with the draft operating procedures. Utility operators, using a development simulator, evaluate selected sets of system displays and provide early operator input during the design process.

3. Validation of the HSI is performed using a completed display simulator. This is discussed in detail in the Human Factors V & V Implementation Plan.

4.6.5 Communications System Design

The following methodology is applied in the design of the communication system:

1. The location of communications nodes within the MCR and throughout the plant, based on identified communications requirements, should first be identified.
2. Call densities should be estimated for each communications node and the required number of channels determined.
3. Noise characteristics should be identified at each node to establish needs for mechanisms to compensate for degrading masking effects.
4. Communications equipment that could be used to satisfy requirements is identified.
5. Establishing standards for transmission characteristics.
6. Select appropriate mechanisms to compensate for masking effects of noise characteristics identified in different plant areas.
7. Detailed design features to be incorporated in communications system equipment should be specified.

Detailed criteria can be found in Vol. 1, Part 2, Section 6 of NUREG-0700, and EPRI NP-3659, Chapter 7.

4.7 HSI Design Analyses, Reviews and Evaluations

This section provides a description of the methods and tools to be used for analysis, reviews and evaluations of the HSI during the design process.

Reviews and evaluations are conducted, as necessary, to resolve human engineering problems specific to the HSI including operator time critical, reliability critical requirements, and other requirements derived from task analysis. Human engineering problem areas are brought to the attention of this activity, and include the estimated effect on the system if the problem is not studied and resolved. These reviews and evaluations are accomplished in a timely manner, i.e., such that the results may be incorporated in the HSI design.

Section 1.2.3 of NUREG-0700R2 provides references to guidelines that may be used in the design and evaluation of advanced HSI. Section 2 identifies the NUREGs, including NUREG/CR-5908, that have been folded into NUREG-0700R2. Many technical areas not fully addressed in Section 3.1.9 of NUREG/CR-5908 such as alarm systems, graphical representation, etc., have now been addressed in

NUREG-0700R2. As part of the HSI design process and Human Factors Verification and Validation processes, static and dynamic evaluation may need to be performed to verify HSI design of VDU interfaces and also control console designs.

4.7.1 Criteria Used in Selecting HFE/HSI Design and Evaluation Tools

Appropriate design tools and techniques are selected to analyze the HSI design, depending on the nature of the aspect being evaluated. There are two main types of HSI analysis. The first analysis uses applicable documents presented in Section 2 to verify that the HSI design meets established human factors criteria. The second analysis verifies that the HSI meets other technical requirements established as design requirements from task analysis, operator evaluation, and applicable plant procedures.

1. Procedures that are appropriate for the evaluation of HSI include, but are not limited to:

    a. Checklists

    b. Structured interviews

    c. Direct observation of operator behavior

    d. Analysis of historical records of operational problems with similar equipment

    e. Physical measurement

    f. Experiments

    g. Subject matter expert (SME) rating of alternative designs.

2. Criteria that may be used in selecting HFE techniques are the following:

    a. Type of design. Taking into account the type of design, there are some techniques that may not apply.

    b. Type of technology (proven or not). In accordance with Section 3.2 of the EPRI URD NP-5795, the MCR design uses proven technology. Advanced systems, equipment, software and firmware may be justified if proven in other applications as defined in the EPRI URD NP-5795, or in ABWRs.

    c. Relative time to perform.

    d. Relative complexity.

    e. Relative cost.

f. Relative cost effectiveness.

g. Demonstrated by use of dynamic displays, simulator, etc.

The design evaluation is based on the objectives of the systems design. What should the system do, who will use it, where will it be used and when will it be used. If the objectives are clear, the evaluation of the results is made simpler. Numerous methods are available for evaluation of designs. Figures 4 and 5 provide guidance on selecting appropriate and useful methods.

4.7.2 Definition of the Design/Evaluation Tools for the HSI Design Analyses

Considering the criteria listed in Section 3, Criteria to be used in selecting HFE/HSI Design and Evaluation Tools, the following techniques are used in the conduct of the HSI design analyses.

4.7.2.1 Design Criteria Checklist

This checklist includes a series of equipment and facilities design requirements taken from human engineering standards and guides that address HSIs. The checklist is divided into categories of design criteria corresponding to major equipment or facilities. These categories might consist of visual displays, audio displays, controls, etc.; NUREG-0700R2 provides examples of checklist formats. The HSI Style Guide is also used during the design process to design, develop, and evaluate the displayed HSI.

In addition to design criteria, results/recommendations from other HFE activities may be used. Inputs from task analysis, design documents, and preliminary system operation, maintenance or test procedures may all be used to evaluate the design. From these "inputs", detailed design or "output" consist of panel drawings, display formats, plant procedures, and input to training or staffing.

4.7.2.2 Drawings

Engineering sketches and drawings are precise outline drawings used to provide design information for an item, facility, or subassembly which is a component or part of the total system. By a logical procedure of depicting related drawing "views", intricate and complicated shapes are clearly shown. Exact and detailed sizes are provided without ambiguity. Individual parts are identified for assembly and are located in the assembly in their correct functional position. In addition, descriptive notes provide information as to materials, finishes, and directions for manufacture and assembly. Engineering drawings or sketches of interest to the HFE Design Team may be further categorized as:

1. Hardware drawings

2. Workspace layout drawings

3. Console drawings

4. Panel arrangement drawings

Console drawings in particular, contain information as to the man-machine interface; for example, the Seat Reference Point (SRP) and Eye Reference Point (ERP) are indicated.

4.7.2.3 Mock-ups

Mock-ups are constructed in the development of the man-machine system as tools used to evaluate the system design before the actual manufacture of system hardware.

A mock-up is used, primarily, to assist in the design and arrangement of system/equipment located on the MCRP. The material used is low cost and consistent with the fidelity of the mock-ups. Soft material, such as laminated foam may be used to construct low fidelity mock-ups. A mock-up that is expected to support hardware may require a sturdy subframe. The dimensional tolerances should be consistent with the use of the mock-up. All structures may be simulated except hidden parts which are inaccessible after the mock-up is completed. In hidden parts areas, it is not necessary to maintain accuracy. The degree of operation is specified for operational hardware. The number and type of operation that is provided often covers a wide range. As part of the evaluation, the drawings may be printed full-scale and placed on the mock-up for evaluation. Also, video projection techniques may be used.

These mockups will provide a basis for resolving access, workspace and related human engineering problems, and incorporating these solutions to the problems into HSI design. In those design areas where systems/equipment involve critical human performance and where human performance measurements are necessary, functional mockups may be provided. The mockups are available for inspection as needed.

In addition to the performance of normal, abnormal, and emergency evaluations, the mock-up is also used to evaluate maintenance, tests, and inspection activities. Based on the fidelity of the mock-up, volume studies may be performed to assess equipment pull-space, personnel, and tool envelopes for these activities.

4.7.2.4 Questionnaires and Interviews

Questionnaires and interviews are used for obtaining information about the problems and positive system features that have been noted in the course of evaluations.

Questionnaires are generally not as effective as interviews for exploratory purposes. Either the respondent has to write too much or information is lost due to misinterpretation of the question. In addition, there may be difficulty in interpreting the respondents' written response without follow-up interviews.

1. Questionnaires

   The basic tool for obtaining subjective data is the questionnaire. It is the most frequently used and the most difficult to construct of the subjective techniques.

   The questionnaire is a subjective measurement tool for systematically obtaining attitudinal responses from a selected group of individuals. The questionnaire provides a structured method for asking a series of questions in order to obtain measurable expressions of attitudes, preferences, and opinions. The function of the questionnaire is to communicate information. When properly formatted, it also aids in the tabulation of data and analysis of results. The questionnaire is used to assess a wide variety of qualitative variables such as acceptance, ease of use and preference. A disadvantage of the questionnaire is that test participants won't respond in writing to the degree that they would in a verbal interview.

2. Interviews

   The interview technique is simply the process of the evaluator discussing the test events with the participants. This discussion should be structured in order to insure that the most information is obtained in the least amount of time. Specific variations to general interview technique may be of use for particular situations.

   The interview is one of the most significant evaluation methods used. It is simple, low cost, quickly used technique. The purpose of an interview is to find out either objective facts related to the system about which the interviewee has some knowledge, or subjective information, attitudes, or opinions about how the interviewee feels about some test aspect.

4.7.2.5 Test and Evaluation Methods for Evaluating and Resolving HFE/HSI Design Issues

4.7.2.5.1 The Evaluation Process

Evaluation is an integral part of the design process, with the results of evaluation efforts leading to interaction through the other phases of the design process. Therefore, planning for evaluation proceeds in parallel with design rather than after a prototype design has emerged.

It is necessary to establish the objectives of the design prior to the evaluation. These objectives must relate to four questions about the proposed design: what should the system do, who will use it, where will it be used, and when will it be used.

Without defined objectives, evaluation is almost meaningless. Therefore, one of the first things to be accomplished in an evaluation effort is determining objectives by reviewing design documentation and talking with the system designers. The product of these reviews and discussions become written objectives that are meaningful to all participants in the effort.

If the results of evaluation indicate that objectives have been achieved, then the existing design may be used and processes of design and evaluation can be terminated. However, it is unusual for evaluation to result in the conclusion that no system improvements are possible or desirable.

The evaluation process, which is to be efficient in terms of both time and cost, is an integral part of design. The evaluation process is iterative in the sense of including multiple phases of evaluation, with the results of each phase being used to enhance the design of the system as necessary to meet HFE goals.

The combined objectives of efficiency and design-oriented successive refinement dictate that the overall evaluation process includes multiple evaluation methods. Alternative methods may range from checklists or paper/electronic evaluations to part-task and full-scope simulator evaluations. The sequencing of these methods depends on the nature of the evaluative issues being addressed. There are three basic types of issues:

1. Compatibility

   A system is compatible to the extent that the physical presentations to the operator and the responses expected from the operator are consistent with human input-output abilities and limitations.

2. Understandability

   A system is understandable if the structure, format and content of the operator-system dialogue result in meaningful communication.

3. Effectiveness

   A system is effective to the extent that it supports an operator (or crew) in a manner that leads to improved performance, results in a difficult task being less difficult, or enables accomplishing a task that could not otherwise be accomplished.

To optimize the evaluation sequence, compatibility is assured before assessing understandability, and understandability is assured before assessing effectiveness.

Design tends to be a top-down process while evaluation is a bottom-up process as shown in Figure 6.

This difference in orientation obviously can present difficulties in terms of timing because it implies that evaluation cannot begin until at least an initial prototype design is available. In particular, it would seem difficult to integrate design and evaluation when by nature they must be pursued in sequence rather than in parallel.

Fortunately, this problem is more apparent than real. While the formal collection of evaluative data must necessarily follow the availability of a prototype, the planning required for evaluation can proceed in parallel with design. This means that as one follows the top-down design sequence, one should anticipate the questions that will later be asked at each level as the bottom-up evaluation sequence is followed.

If evaluation is pursued subsequent to design rather than in parallel with it, by evaluators who have not participated in the design process, the evaluators' first effort are to gain a top-down perspective of objectives. Without this perspective, the bottom-up evaluation will suffer from a lack of context.

At the effectiveness level, the sequence in Figure 6 has clear implications. System objectives are defined during design by anticipating those evaluation measures that reflect the degree to which objectives are achieved. The nature of the objectives dictates the type of evaluation (i.e., comparative versus absolute) and appropriate performance measures. In addition to expediting subsequent evaluation, defining measures also serves to assure that objectives are not ambiguous. A better design is likely to result, regardless of whether or not there is an actual evaluation.

At the understandability level, one is concerned with the nature of communications between operators and the system. In a sense, this communication process can be viewed as being between the operators and the designer. From this perspective, during design one determines what an operator would need to know (from training, documentation, or other displays) in order to understand the messages the designer is likely to communicate. Similarly, one assesses what is required for an operator to be able to formulate and transmit messages to the designer. This type of analysis is not only useful when evaluating understandability, but also helps to assure that understandability problems do not emerge in the first place.

At the compatibility level, the design and evaluation sequences overlap.

4.7.2.5.2 Methods of Evaluation

Figure 7 illustrates how multiple methods can be sequenced to pursue the evaluation issues. This figure is not meant to imply that all five types of evaluation (i.e., electronic, paper, part-task, full-scope, and in-plant) are required for every evaluation effort. The methods employed first are those that are relatively fast and inexpensive and that can be employed earliest in the design process.

Electronic, paper and part-task simulator evaluation methods are used in the design phase.

Full-scope simulator and in-plant evaluation methods are used in the integrated verification and validation process.

1. Electronic Evaluation

The primary purpose of the electronic evaluation is to assess compatibility in the sense of determining the degree to which a design takes advantage of MCR operator's abilities while avoiding their limitations.

Since much of the documentation and design is being developed on computers, an electronic version of documentation will be available early in the design phase allowing for evaluating and resolving HFE/HIS design issues. Previous operations experience feedback data is available for previous BWR/ABWR designs and will be utilized in the ESBWR design. This allows for an on-going iterative design approach with enhancements being continuously added for improving the HFE/HIS design.

2. Paper Evaluation

A paper evaluation will be performed if the electronic evaluation method is not available. The inputs required for a paper evaluation include a working prototype. Scale drawings are sufficient for a partial, formative paper evaluation, but not for a complete formal paper evaluation. This is because drawings, or even static pictures of displays, do not allow for assessing the full range of compatibility issues; available design documentation on objectives (specifications), and access to designers to obtain information that is not documented.

The results of a typical paper evaluation include a list of problems identified (human engineering deficiencies) and recommendations for modifying the system to eliminate the problems.

In order to expand the scope of a paper evaluation to include understandability and perhaps a few effectiveness considerations, the design team carefully analyzes the system design to see that it satisfies information requirements and to assess, if possible, the degree to which system objectives are achieved.

The paper evaluations of compatibility are performed by an analyst using a human factors engineering guide (checklists). If a systematic design has been used in process for design, the paper evaluation may be quite straightforward. The paper evaluation of compatibility may be performed by a human factors specialist. Personnel who are thoroughly familiar with the systematic design process may be in a position to perform an acceptable paper evaluation. Further, since investigation of compatibility issues does not require experimentation, a paper evaluation can be performed with very limited assistance from operations personnel. This has the obvious advantage that a paper evaluation can be rather efficient in terms of operations personnel time.

A paper evaluation of compatibility and/or understandability does not begin until after a verified prototype is available. This does not preclude qualitative analyses and informal evaluations of tentative display formats. Such activities are essential to an integrated design and evaluation process. However, avoid using formal evaluations as the primary means for catching incomplete or inadequate engineering and/or programming.

It should be noted that both the electronic and paper evaluation methods may be use in a static or "dynamic" evaluation process. When used statically, the images (either on paper or electronic screen) can be examined from a human factors perspective. When used dynamically, the images can be used in a talk-through process to verbalize what would be expected to appear in a specified event, and to examine this from a human factors perspective.

3. Part-Task Simulator Evaluation

A wide range of part-task simulators is possible, with static mockups on the low end.

The primary objective of part-task simulator evaluation is to assess understandability. As discussed earlier, this involves determining whether operators can comprehend the messages transmitted to them by the system, and whether they can communicate their desires, and perhaps intentions, to the system. These determinations involve several questions:

a. What messages will the system typically transmit to operators?

b. What will operators need to know in order to comprehend these messages?

c. What messages will the operators typically transmit to the system?

d. What will operators need know in order to formulate and communicate these messages?

How will the requirements specified above be satisfied by training, documentation, and/or other displays? These questions are asked and answered during design. The purpose of evaluating understandability is to assess the validity of the answers generated during design by answering the following questions:

a. Do operators actually comprehend the messages presented by the system?

b. Do operators correctly formulate responses to these messages?

c. Do operators correctly communicate their responses to the system?

In order to evaluate these questions the part-task simulator will need to be of higher fidelity. The software should clearly represent the completed design as close as possible, and the hardware necessary to perform the evaluation at this level should represent the final design hardware. The workstations should be fabricated to the detail necessary to perform the evaluation. The results of a part-task simulator evaluation include a thorough assessment of understandability and an initial evaluation of effectiveness. In addition to an assessment of understandability, results include identification of the specific deficiencies that must be eliminated to achieve an acceptable level of understandability.

The electronic screen formats which form a major portion of the HSI are developed in preliminary form as a portion of the HSI part-task simulator and are developed in final format in compliance with the HSI design requirements as part of the entire MMIS software development activity.

Dynamic simulation techniques are utilized as a human engineering design tool when necessary for the detail design of equipment requiring critical human performance. Consideration is given to use of various models for the human operator, as well as man-in-the-loop simulation. The simulation equipment is intended for use as a design tool, although its use as training equipment is considered in any plan for dynamic simulation.

5 Human-System Interface (HSI) Description

Using the applicable sections of NUREG-0700R2, a conformance specification is prepared that defines the hardware and software requirements for the DCIS, including the VDUs.

5.1 Hardware Guidelines for HSI Displays

1. Large screen displays are designed so that the off-centerline viewing angle is sufficient for multiple viewers. This prevents obstruction by other people for required observers. It is desirable for the luminance at the maximum viewing angle is at least half the luminance at screen center.

2. Preference is given to selection of equipment which is less susceptible to burn-in of images that are displayed on a VDU for long periods.

3. Non-glare coatings are provided for the displays. Displays should be positioned so that the user's line of sight to the far edge of the display is within 20° above or 40° below the horizontal and within 35° in a horizontal plane when viewed from the normal position of the operator.

4. The following minimum resolutions for user interface devices are appropriate:

VDU	1280 x 1024 pixels, 256 colors, 20 in. diagonal size.
Flat Panel Display	minimum 640 x 480 pixels, 256 color, 17 in. diagonal size.

5. The aspect ratio is established to be consistent between displays, and a ratio of 4:3 may be appropriate.

6. Maximum display jitter is established, and a value of less than 0.0002 mm/mm viewing distance jitter in any 1 second period may be appropriate.

5.2 Touch Screen Devices

Guidelines for touch screen devices include:

1. Should respond to touch pressure and indicate that the user's finger is over a selectable button or target by a change in color, shade, border or background. The button or target are selected when pressure are released. A separate action is required to cause an action to occur, except for actions which only change displays.

2. Should respond to a selection pressure (typically 0.25 to 1.5 N), with the pressure sensitivity being:

   a. Consistent across entire screen;

   b. Capable of adjustment and calibration.

3. Should exhibit cursor location and tracking which:

   a. Is precise with respect to finger location;

   b. Is consistent across the entire screen;

   c. Is not affected by angle of contact with screen;

d. Produces no cursor movement other than that requested by the user;

e. Does not allow the cursor to go beyond display bounds.

4. Should not reduce light transmission or affect color to such an extent that usefulness is affected.

5. Should have a method of disabling the effects of the touch screen for cleaning.

6. Should have a trackball Option.

6 Software Guidelines for HSI Displays

The screen structures and contents are defined in the HSI report that addresses each system. The criteria for the size of the text (font style and character size) are defined in the HSI Style Guide. The "look and feel" of each display is governed by the requirements of NUREG-0700R2 and the Display Primatives Specification.

6.1 Display Content Guidelines

Each page will have a title which describes the contents or purpose of the display. Subsidiary pages are indicated by the form of the display title. Each page will have a unique page identifier displayed on the page, by which the page can be referred to. Multipage displays will have page numbers (e.g., "page x of y").

In displays which represent a portion of a larger diagram, the location of the display in the larger diagram is shown.

Date/Time is shown in 24 hour format in a fixed position on all displays.

The display will not be overly dense with information (not more than 50% density).

Displays are laid out so that the flow of signals, process variables, user attention, or information is generally from top to bottom or left to right.

Related controls, items, and information are grouped so that it is easy to locate a desired item.

6.1.1 Display Partitioning

Displays will incorporate regionalized information such as the following. To the extent practical, regions will not overlap and will have consistent locations for all displays.

1. The Title area

2. The View area where the primary information is displayed.

3. The Dynamic Display icon which is active and shows that the computer system is operating and in communication with inputs.

4. The View Tool area which contains time, date, plant identification, and soft function keys for interdisplay navigation.

5. The View-Control area which appears only when needed, contains buttons to select and control plant components.

6.1.2 Data Display

1. The display will not imply more data precision than the lesser of what is necessary for the purpose of the display, or which exists in the measured parameter.

2. The reliability (quality) of data points are determined based on status supplied with the data point value from the multiplexing system Data that is determined to be unreliable will be visibly indicated in an appropriate manner.

3. Units on numeric indications are consistently displayed.

4. If valid data are not available, a display (P&ID, table, or other) is posted with dynamic elements suppressed or displayed with bad data indication until they have been updated with valid data.

6.1.3 Arrangement of Fields and Records

Titles for rows and columns should be easily distinguishable from the data entries and rows and columns ordered in ways which are significant to the user. Numeric data normally are justified on the decimal point. In tables with many rows, visual means should be provided to aid horizontal scanning.

6.1.4 Visual Coding

1. Colors used should be easily discernible from each other. Recommended color scheme examples are provided in Table 2.

2. Consideration should be given to some additional visual cue other than color. Other possible features include: shape change, line thickness, or additional characters such as '!', '?', etc.

3. Dimming may also be used to indicate that a particular menu or other choice is not currently available

4. Coding by differences in brightness may be used. Generally, not more than two brightness levels are used. Differing brightness is used for emphasis and de-emphasis.

5. Tagged-out component display rules will be established and could indicate a different color background on any display which shows the component.

6.1.5 Blinking

Blinking may be used where appropriate. Typically, two different rates are allowed between 5 Hz and 0.8 Hz. The difference between the faster rate and the slower rate is usually at least 2 Hz. The time the blinking item is on is usually at least as great as its off time. Blinking items within any single window are usually synchronized. Typically a fast blink indicates an alarm condition which has not been acknowledged and as low blink indicates return to normal.

6.1.6 Icons and Symbols

1. User interface icons are simple, closed figures used to represent actual objects or actions. Each icon is distinguishable from all other icons and will represent a single object or action (e.g., PRINT). Help is available to the user to explain the purpose of all icons.

2. Component symbols on system diagram screens are chosen from the standard symbol set utilized on ESBWR P&ID drawings.

6.1.7 Data Entry

1. The method of interaction between the user and the user interface are by direct manipulation of graphical objects, rather than keyboard entry when possible. The selection will take effect when the pressure on the touch screen is removed. Operation of a component will require a separate action, so that selection and operation are two actions.

2. The users are able to select points from a point list by touching the point on the list. The user will then be able to add the point to the set of points being trended. If the list is long, scroll bars are provided.

3. The users are able to create groups of variables in user defined trend sets. These sets are displayable as individual graphs of values on vertical axis vs. time on the horizontal axis (with user selectable time scales), or as multiple curves on one set of axes. The user is able to save a set definition and recall it for later use and editing. The capability for the user to protect certain predefined groups against change is provided

4. The user is able to control the presence and intensity of grid lines on the user displayed trend displays. The time scale and number of graphs on the display are controllable. The user is able to select the Y axis scale of each trend graph. The choices of linear and log (base 10) are available.

6.1.8 Feedback

The DCIS supplies feedback to all user inputs, positive or negative and provides feedback on the status of the display update during long processing (e.g., cursor hourglass).

6.1.9 Target Selection

Feedback on target selection is shown by enclosing a box around the selected item.

6.1.10 Confirmation & Prompting

1. Confirmation is provided for critical (i.e., plant control operations) and non recoverable entries or selections. Confirmation will require the user to either confirm or cancel the operation.

2. Prompting is provided whenever user input is required. On menus and dialogues, the prompt can be in the form of a title. Where data entry is permitted in certain fields only, these fields are visually distinct from other areas in the display.

3. The input field prompts indicate the required formats and acceptable values, if required for clarity.

4. Modal dialogues are used only when a user response is required before allowing an operation to continue (such as a confirmation).

5. An explicit action (such as touching ENTER or EXECUTE) is required to put the entered value into effect

6. The DCIS allows users to begin a new entry sequence prior to completing current entry sequence, by easily aborting the current entry sequence without adverse effects.

6.1.11 Bar Charts

Each bar or pair of related bars has a unique label. In a series of related bar charts, a consistent horizontal or vertical orientation is adopted. Deviation bar charts will have zero reference at the center of the bar chart.

6.1.12 Graphs

1. Graphs convey enough information to allow the user to interpret them without referring to additional sources. When multiple curves are displayed on one graph, labels are attached directly to each of the curves.

2. Old data are removed from the displayed graph after a fixed period of time.

3. For trend plots and similar items, the data history remains when the plot is not displayed; it is possible to call up the display again and see the same historical data, as if the display had not been dismissed.

6.1.13 Diagrams & Mimics

The amount of detail in mimics is tailored to the display to be used (e.g., a system mimic is shown on a VDU with considerable detail, on the FPD with less detail). The layout of the components common to various displays is consistent among the displays.

6.1.14 Messages

Messages are simple, concise, and yet descriptive and provide only information necessary to the user.

If additional information is available, messages indicate to the user how to access the additional information (e.g., button labeled "Detail...").

Error Messages shall:

1. Describe the error condition in terms understandable to the user.
2. Describe severity and impact of error condition. Color is one appropriate method for indication, if supplemented by descriptive text.
3. Reference the recovery method or provide connection to a help screen. Context-sensitive help is available.
4. Distinguish between types of user errors and computer system errors.
5. Be logged to an error log file.

6.1.15 Instructions (Help)

On-line help is always available from a simple touch screen operation. When entering the help system, context-sensitive help will initially be posted. Help is structured hierarchically (general to detailed). The help system will provide hypertext links between referenced sections. The help system is easily extendable. It is possible to move the help popup to another section of the screen.

6.2 Guidelines for GUI Presentation

6.2.1 Window Configuration

Tiling vs. overlapping: the user interface uses tiled windows. Popups are overlaid.

6.2.2 Controls

1. The following control types are available:

   a. Checkbox - functions as a toggle switch

   b. Icon - symbolic graphic item which represents an action or physical object

   c. Menu bar - a sequence of pulldown menus which can be cascading

   d. Option menu - temporary menu for display of options which always displays the current choice as the button label

   e. Pulldown menu - text menu for temporary display of choices

   f. Push button - user selectable button, with a single value

   g. Radio button - list of mutually exclusive choices, all visible in a rectangular arrangement

   h. Selection list - scrollable text list for presenting a long list of choices

2. There are dedicated function keys available on both FPDs and VDUs. The function keys are implemented as hard keys near, or as softkeys on, each FPD and each VDU. Typical function keys include:

   a. Call up Main menu

   b. Page forward

   c. Page back

   d. Call up the Plant Alarm menu

   e. Call up Trend display for current system (or index of trend displays if no system page is currently on the VDU)

   f. Call up Alarm display for current system

   g. Call up Parameter display for current system

   h. Call up System Diagram for current system

   i. Enter control mode

   j. Enter monitor mode

k. Print hard copy of screen

l. Acknowledge alarm

m. Call up related systems display related page

n. Expand left

o. Expand right

p. Call up System Automation display

q. Recall previous display

r. Copy display to large screen

s. Recall previous large screen display

6.2.3 Menu Configuration

1. Appropriate limits should be established for the number of items per menu and the number of levels of menu hierarchy.

2. Nonselectable menu items should be visible but disabled.

3. Menus in different displays should use option lists with consistent wording and organization.

6.2.4 Response Time

1. The HSI is designed with human capabilities in mind when selecting display components and system response rates. The refresh rates on the display screen should match standard computer screens to avoid operator fatigue.

2. Automatic information updates on the selected display screen will depend on the capability of sensors and computer calculations to provide new data points. Even during peak information load conditions when the computer is processing many multiple calculations, the variability in response time between sample requests should not be more than half the mean response time. Clearing the screen is not considered as an automated system response.

3. For manual entry display requests, response time is the time for complete redisplay with new values or information. If a manual action request cannot be completed in 1 second, feedback (e.g., hourglass cursor or similar) appears on the screen to indicate that the DCIS is working to respond. All displayed data that are dynamic and have valid values should be updated at a rate less than the display screen refresh rate. From human observational capability a rate faster

than 2-5 Hz has no interpretative meaning, thus nothing faster than 1 Hz is needed from the operator perspective.

4. Response times for hardware interface activities listed below will be defined in the DCIS specifications.

	Activity	Max Time (s)	Preferred Time (s)
1.	Control activation (e.g., touch point activation)		
2.	Request for a given service or display: complex		
3.	Request for a given service or display: system startup		
4.	Error feedback after completion of input		
5.	Information on next procedure		
6.	Response to simple query from list		
7.	Response to simple status inquiry		
8.	Response to complex query in table form		
9.	Request for next page		
10.	Response to "execute program"		
11.	Response to complex query in a graphic form		
12.	Response to graphic manipulation		
13.	Response to user intervention in an automatic process		

6.2.5 Portability

The software design is capable of being implemented on both X-Window/Motif and on Microsoft Windows/Windows-NT with minimal changes.

6.3 Human-Machine Interface Detailed Content Guidelines

6.3.1 User Dialogue

The Main Menu may include touch screen sensitive areas which allow selection of:

1. RPV CONTROL DISPLAY
2. REACTOR BUILDING CONTROL DISPLAY
3. PRIMARY CONTAINMENT CONTROL DISPLAY
4. RADIATION RELEASE CONTROL DISPLAY
5. EPG PLOTS
6. PLANT AUTOMATION SUMMARY

7. RWCU/SDC SUMMARY
8. ALARM SUMMARY
9. TRENDS SUMMARY
10. NSS SUMMARY
11. FW & CS SUMMARY
12. BOP SUMMARY

Selection of the plant alarm button calls up a list of one line for each major alarm.

Selection of the system alarm button while a system P&ID is displayed calls up a diagram which is a mimic of an annunciator panel, on which the lights flash as in a hardwired annunciator box. The view control area then contains buttons to silence and to acknowledge the alarms on that page.

The functionality of the components is defined in the Display Primatives Specification for both VDU and FPD displays.

6.3.2 Display Types

The display system should include two types of screens:

- Plant-level screens corresponding to operational phases;
- System-level screens by which traditional hard-wired instruments are replaced.

1. The following two types of screen menus should be provided, corresponding to the screen system.
   a. Plant-level operating screen menu
   b. System-level screen menu
2. The following switches should be provided for selection of system-level screens to enable quick selection of the following types of screens for each system.
   a. System Diagram
   b. System Trend
   c. System Alarm
   d. System Process Parameter

e. System Automation Progress Status

Touch controls to select and maneuver between each of these five types of screens for each system are available for quick navigation among these screens for the same system.

3. A function for selecting and displaying related screens are provided on each screen, so that those screens can be selected quickly from the other related systems' screens.

4. To provide a monitoring mode by three adjacent VDUs, a function/switch should be provided at the center VDU of the three, for displaying the same screen on VDUs to the left and right side.

6.3.3 Default VDU Locations of Plant Information

Capability will be provided to display "Plant Display" screens on respective default VDUs. The default locations are provided based on their proximity to related hardware switches. However, the user may call the Plant Display screens on any preferred VDU.

1. VDU#1: ECCS (GDCS and ADS)
2. VDU#2: Alarm
3. VDU#3: Trends
4. VDU#4: Core/NSS
5. VDU#5: Guides
6. VDU#6: Feedwater, condensate systems summary
7. VDU#7: Turbine/generator summary

Wide screen: Trends, the same role of VDU#3

6.3.4 Plant Alarm Pages

Pages contain lists of alarms which are currently in alarm or alert. The user is able to view a list which gives the status of a selected group of alarm points.

The user specifies filtering criteria for the current and historical alarm displays. The display information includes: points in alarm only, points in alert only, points in normal state only, and any combination of these. When the user displays an alarm list which excludes any alarms, the selected alarm list appears in one window of the display, and another window shows all changes in the state of alarm points which occur after the filtered list is shown.

Acknowledgment of alarms on one alarm page is accomplished by touching an acknowledge button. On successive pages of an alarm display, the page acknowledge buttons appear in a consistent location. It is possible to acknowledge alarms from the system page only, not from the plant alarm chronological summary page.

The history of alarm point status changes is available. The display of the history shows whether the change has been acknowledged or not, the time of the change, new status, point identification, description, units, and value.

The user is able to specify the order in which the filtered alarm lists are presented. Examples of possible orderings are: in order of importance, and within each importance category in reverse chronological order, with the most recent entry first; chronological order; by priority; by system.

6.3.5 Logs

The following log types should be provided:

1. Event log: control actions which are initiated by the user are recorded in a log, with a time stamp and the identity of the display device from which they were initiated.

2. Error log: errors encountered in the DCIS internal processing are written to a log, with time stamp and other diagnostic information.

6.3.6 Point Monitoring

The user is able to select points and display their current values and the previous values for some time in the past, for monitoring purposes.

6.3.7 Charts and Graphs

The following chart types should be provided:

1. Time-based: the user is able to select sets of pre-defined time based graphs. The graphs indicate the most recent data obtained at the right (or bottom) and older data progressively to the left (or top)

2. Plot-on-plot: The user is able to select any two monitored points and plot one against the other.

3. Bar graph: current severity, range, alarm and alert setpoints are displayed.

Each measured point which appears on any display has its previous historical values available to the system. These values are displayed in a graphic format which can be called up by touching the point on a graphic display. A popup menu then appears, from which the user can choose whether to display the point's history, or view alarms associated with the point.

When a point is displayed on an individual trend graph, its alarm points are displayed at the user's discretion. When the value is outside an alarm limit, the color of the trend line indicates the out of normal condition.

The user should be able to select a mode in which a pointer appears on any displayed graph, with the user able to move the pointer to any point on the displayed graph and read the numerical coordinates of the point from the display.

Bar graph groups should have the same X axis scale for all graphs in the group display to facilitate comparisons.

6.3.8 Diagrams & Mimics

System level Plant & Instrumentation Drawings (P&IDs) are provided and show sufficient detail to permit the user to perform the functions required from that display.

The contents of system diagrams such as P&IDs for operator use of a system are defined in system specific reports. The behavior of the displays is defined in the Display Primatives Specifications. The icons, parameters or bar graphs are driven by signal located in the system specific logic or an algorithm located in the respective processor software.

6.3.9 Displays and Controls

The displays and controls in Table 3 are required for plant operator monitoring and operation of the DCIS. Note that the DCIS has one operating mode, the NORMAL mode, for all modes of plant operation.

7 HSI Documentation and Reporting

As indicated in Section 3.3.7 and elsewhere in this Plan, various types of documentation is prepared throughout the process of development of ESBWR HSI as indicated below.

7.1 HFE Specifications for HSI

The HSI design process includes preparation of three HSI specifications. Due to the iterative nature of the design process, these specifications become more detailed during each iteration, and they may not become finalized until the process is completed. The HSI specifications include:

a. Style Guide for Graphical User Interfaces;

b. Display Primitive Design Specification; and

c. HSI Report

The Style Guide is based upon applicable excerpts from NUREG-0700R2. The Display Primitive Design Specification defines the manner in which the icons displayed on the VDU and/or FPD behave on each interface. The intent is to have a consistent look and feel for the HSI from one system to the other. The HSI report integrates the information on each system, from the system functional requirement analysis (SFRA), allocation of functions (AOF), and the system task analysis. This report is prepared by the HFE design team using results of the system specific task analysis to address system-general and specific operator interface requirements in the MCR and the RSS. Each system is identified by a system level name (e.g., the Standby Liquid Control System is SLC C41). The alarm and annunciator systems are also defined in the HSI report

7.1.1 HSI and Equipment Detail Design Documents and Drawings and HFE Issue Tracking

Human engineering principles and criteria applied to the design of HSI and equipment are reflected by the design documents and detail design drawings for these HSI and equipment to assure that the final product can be efficiently, reliably and safely operated and maintained. As a minimum, the types of engineering documents and drawings include the following:

1. Environmental drawings and data sheets for the MCR and RSS display areas

2. Illumination design drawings and data sheets for the MCR, back panels, and RSS display areas

3. Communication system drawings and data sheets for the MCR, back panel, and RSS display areas

4. MCR design drawing indicating the areas and rooms assigned to the plant staff as required by the utility.

5. Panel layout drawings for the large display panel, the MCC and the RSS display panel.

6. Documentation including description of the software interfaces located on the VDUs and flat panel displays. Applicable documents describe all of the formats to be displayed on the VDUs and flat panel displays.

7. Any applicable HFE reports prepared to document HFE and HSI evaluations performed in support of MMIS design.

8. Tracking of HFE Issues in the HFEITS

7.2 HFE Reporting

After completion of the HIS design in accordance with this implementation plan, the ESBWR HFE Team will perform an evaluation of the design and prepare the HSI Results Summary Report for NRC staff review. The results of the HFE Design Team's evaluation of the conduct, results and supporting analyses are documented in a HSI design report that includes the following:

- Summary of the objectives, methods, and procedures used by the HFE Team in performing the HSI design evaluation
- Summary of HSI requirements to designers
- The HFE Team's evaluation of the completed HSI design and supporting analyses, including an evaluation of compliance with the HSI Design Implementation Plan, the HFE Program Plan and the HSI Style Guide.
- Identification and evaluation of any deviations from the HSI Design Implementation Plan, the HFE Program Plan, and the HSI Style Guide.
- Summary of HSI display definitions and structure.
- Presentation and discussion of the HFE Team's findings.

Table 1 Summary of accident monitoring variable types/source documents

Type[1]	Selection Criteria for a measured plant variable [1]	Typical Source Documents[2]
A	Variable supports planned manual controlled actions to accomplish safety related function for which there is no automatic control.	Plant Accident Analysis Licensing Basis EPGs or plant specific EOPs[3] Plant AOPs[3]
B	Variable supports the process of assessing actions for accomplishing or maintaining plant critical safety functions.	Functional restoration EPGs or plant specific EOPs[3] Plant critical safety functions related to the EOPs Plant Critical safety function status tree
C	Variable indicates the potential for or actual breach of the three fission product barriers.	Plant Accident Analysis Licensing Basis Design basis for the fission product barriers EPGs or plant specific EOPs[3]
D	Variable indicates the performance of safety systems. Variable indicates the performance of auxiliary supporting features Variable indicates the performance of other systems necessary to achieve and maintain safe shutdown conditions. Variable verifies safety status	Plant Accident Analysis Licensing Basis Event specific EPGs or plant specific EOPs[3] Functional restoration EPGs or plant specific EOPs[3] Plant AOPs[3]
E	Variable monitors the magnitude of radioactive material releases through identified pathways Variable monitors the environment conditions used to determine the impact of releases of radioactive material through identified pathways Variable monitors the radiation levels and radioactivity in the plant environs. Variable monitors the radiation levels and radioactivity in the control room and selected plant areas where access may be required for recovery.	Procedures for determining radiological releases through plant identified pathways Procedures for determining plant environs radiological concentration Procedures for determining plant habitability

Notes

[1] The classification and definitions are from IEEE Std. 497-2002

[2] The identification of the manual action is developed through the Allocation of functions, the Task Analysis and the PRA/HRA

[3] During Design the results of allocation of functions and task analysis are substituted prior to EPG, EOP and AOP development

Table 2 Example of Coding Scheme

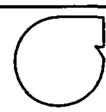
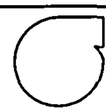
Equipment/ Component	Symbol	Color	Shape	Status	Condition
Pump		Cyan	Filled	Running	Normal
		White	Hollow	Not Running	Normal
		Red	Hollow	Not Running	Abnormal (Should be running)
		Red	Filled	Running	Abnormal (Should not be running)

Table 3 Required Displays and Controls for DCIS Operation

System Operating Mode/Task	Qualitative Information Needed	Quantitative Information Needed	Controls Needed	MCR	Back Panel	Local
Normal	PAS Subloop Automation Failure Status	None	None	x		
Normal	PAS Mode Status Pushbutton Switch	None	PAS Manual Mode PAS Semi-Automatic Mode PAS Automatic Mode	x		
Normal	PAS Phase Pushbutton Switch	None	PAS Startup PAS Shutdown PACS Power Range			
Normal	DCIS Operating Status	None	None	x		
Normal	Alarm Processing Operating Status	None	None	x		
Normal	Display Processing Operating Status	None	None	x		
Normal	Procedure Tracking Operating Status	None	None	x		
Normal	Fixed Mimic Display Operating Status	None	None	x		
Normal	Data Acquisition/ Communication Operating Status	None	None	x		
Normal	Data Recording Operating Status	None	None	x		
Normal	Data Archive Operating Status	None	None	x		

Table 3 Required Displays and Controls for DCIS Operation (Continued)

System Operating Mode/Task	Qualitative Information Needed	Quantitative Information Needed	Controls Needed	MCR	Back Panel	Local
Normal	Reactor Core Monitoring Operating Status	None	None	x		
Normal	Tech Spec Monitoring Operating Status	None	None	x		
Normal	Safety System Monitoring Operating Status	None	None	x		
Normal	Thermal Performance Monitoring Operating Status	None	None	x		
Normal	SPDS Operating Status	None	None	x		
Normal	Large Variable Display Operating Status	None	None	x		

Implementation Plan Process Flow Chart
PROCESS FOR PERFORMANCE AND PREPARATION OF HFE

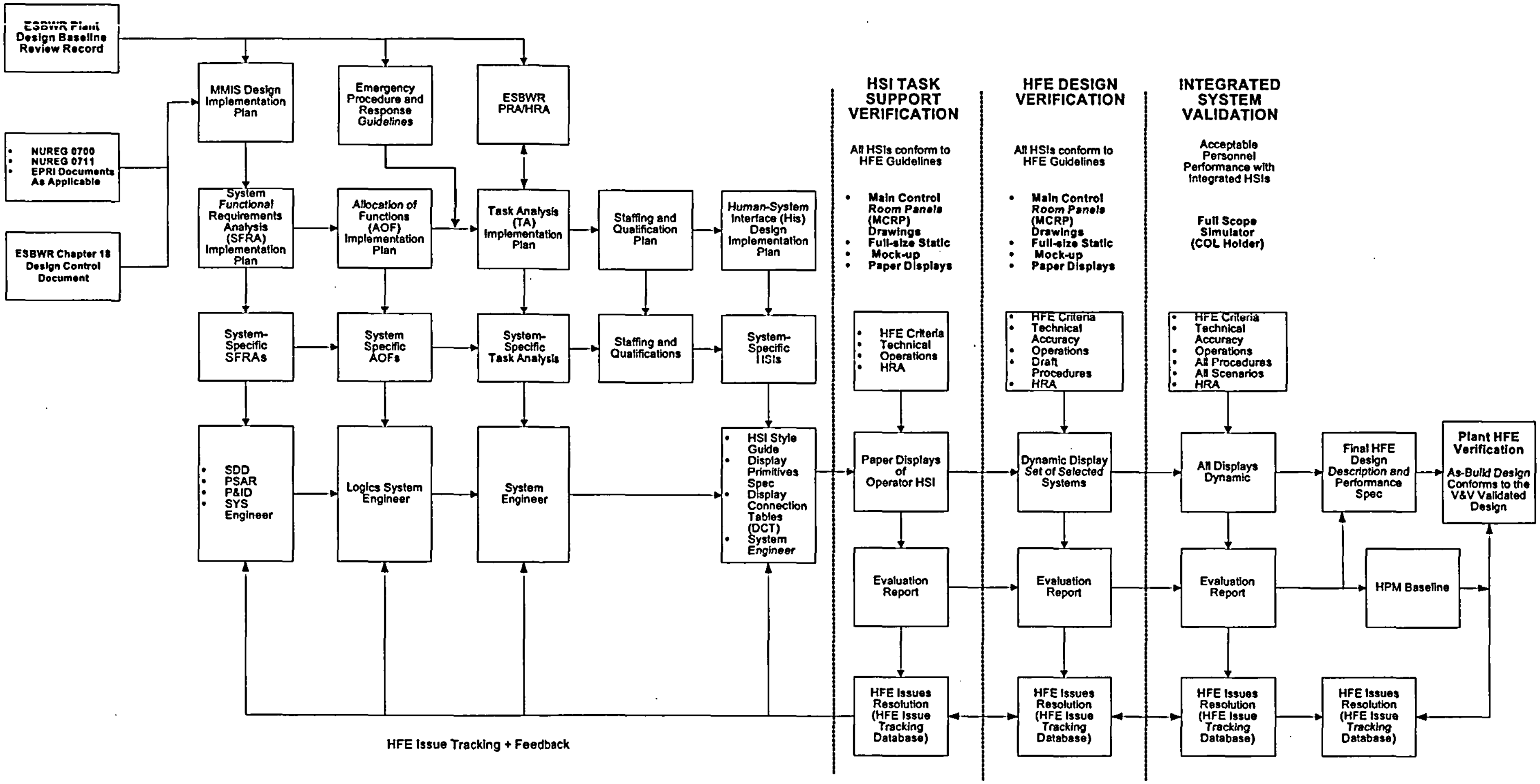


Figure 1 Human-System Interface Design Implementation Process

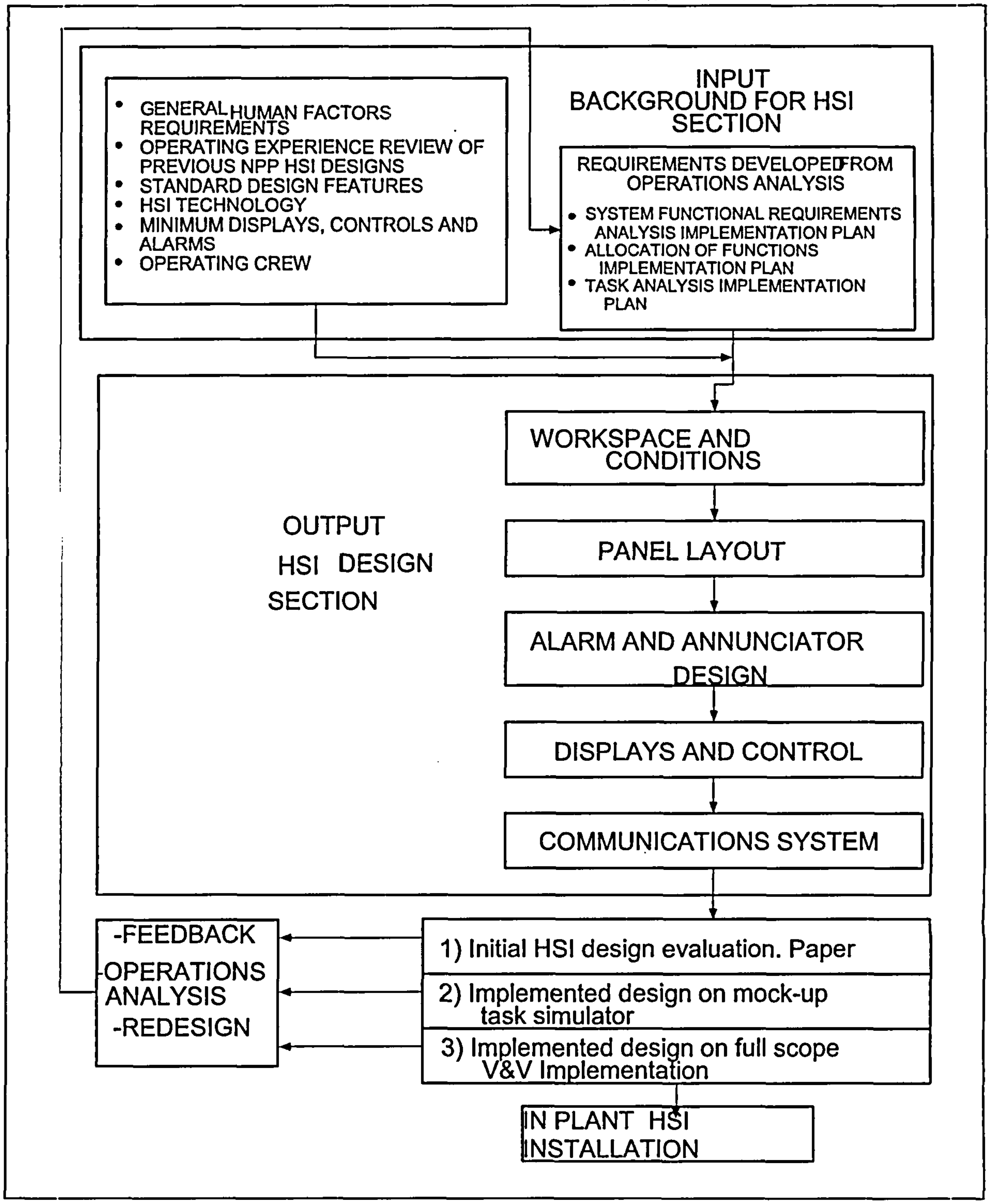


Figure 2 Design Process Block Diagram

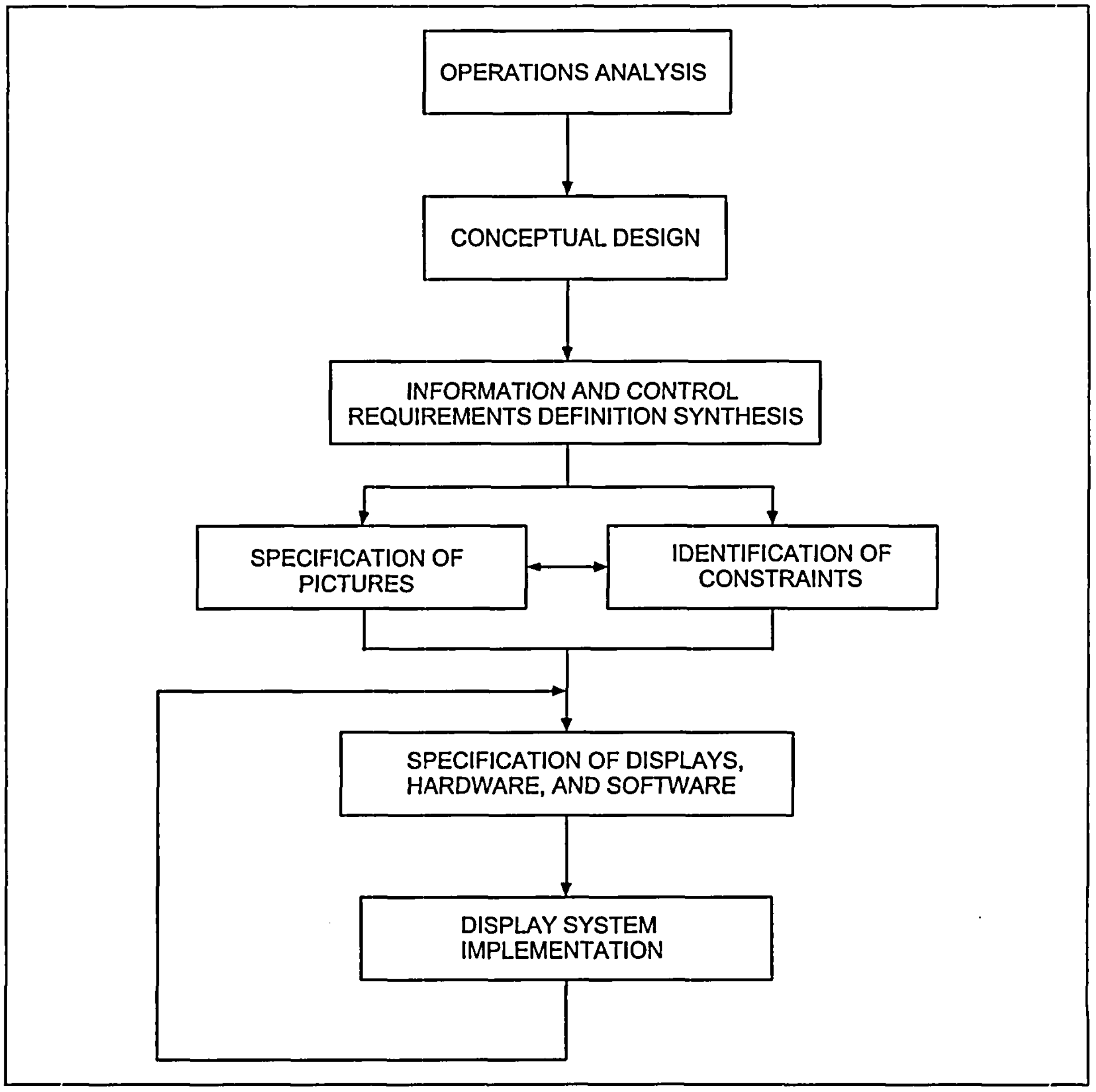


Figure 3 Flow Chart of Elements for Design of Computer-Generated Displays

	SCENARIO GENERATION	WORKLOAD ANALYSIS	PERFORMANCE MODELS	MMI EVALUATION	EVALUATION OF ALTERNATIVE DESIGNS	AUTOMATION IMPACT
CHECKLISTS	1	na	na	1	1	2
SUBJECT MATTER EXPERT INTERVIEWS	1	2	1	2	2	1
SUBJECT MATTER EXPERT RATINGS, RANKINGS	2	1	1	1	1	1
DIRECT OBSERVATION	2	1	1	1	2	na
EXPERIMENTS	na	2	2	1	1	1
DIRECT MEASUREMENTS	na	na	na	1	na	na
ANALYSIS OF HISTORIES	2	2	1	2	2	na

1 = VERY USEFUL
2 = USEFUL
na = NOT APPLICABLE

Figure 4 Appropriate Data Collection Methods for HFE Activities

Figure 5 Usefulness and Efficiency of Alternative Evaluation Methods

METHOD OF EVALUATION	LEVEL OF EVALUATION		
	COMPATIBILITY	UNDERSTANDABILITY	EFFECTIVENESS
ELECTRONIC EVALUATION	USEFUL AND EFFICIENT	USEFUL AND EFFICIENT	SOMEWHAT USEFUL BUT EFFICIENT
PAPER EVALUATION	USEFUL AND EFFICIENT	SOMEWHAT USEFUL BUT INEFFICIENT	NOT USEFUL
PART-TASK SIMULATOR	USEFUL BUT INEFFICIENT	USEFUL AND EFFICIENT	MARGINALLY USEFUL BUT EFFICIENT
FULL-SCOPE SIMULATOR	USEFUL BUT VERY INEFFICIENT	USEFUL BUT INEFFICIENT	USEFUL BUT SOMEWHAT INEFFICIENT
IN-PLANT EVALUATION	USEFUL BUT EXTREMELY INEFFICIENT	USEFUL BUT VERY INEFFICIENT	USEFUL BUT INEFFICIENT

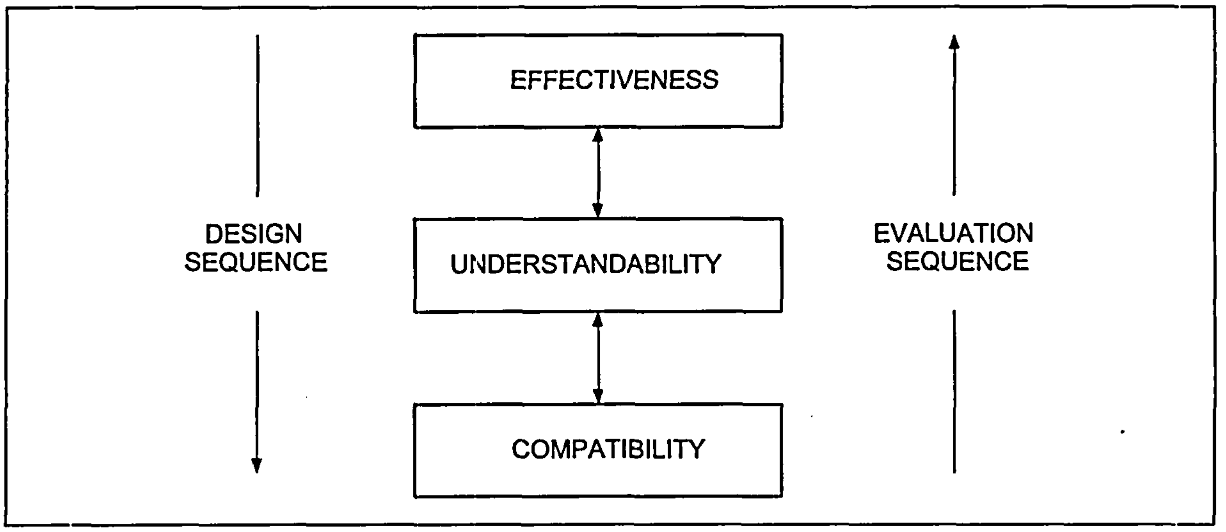
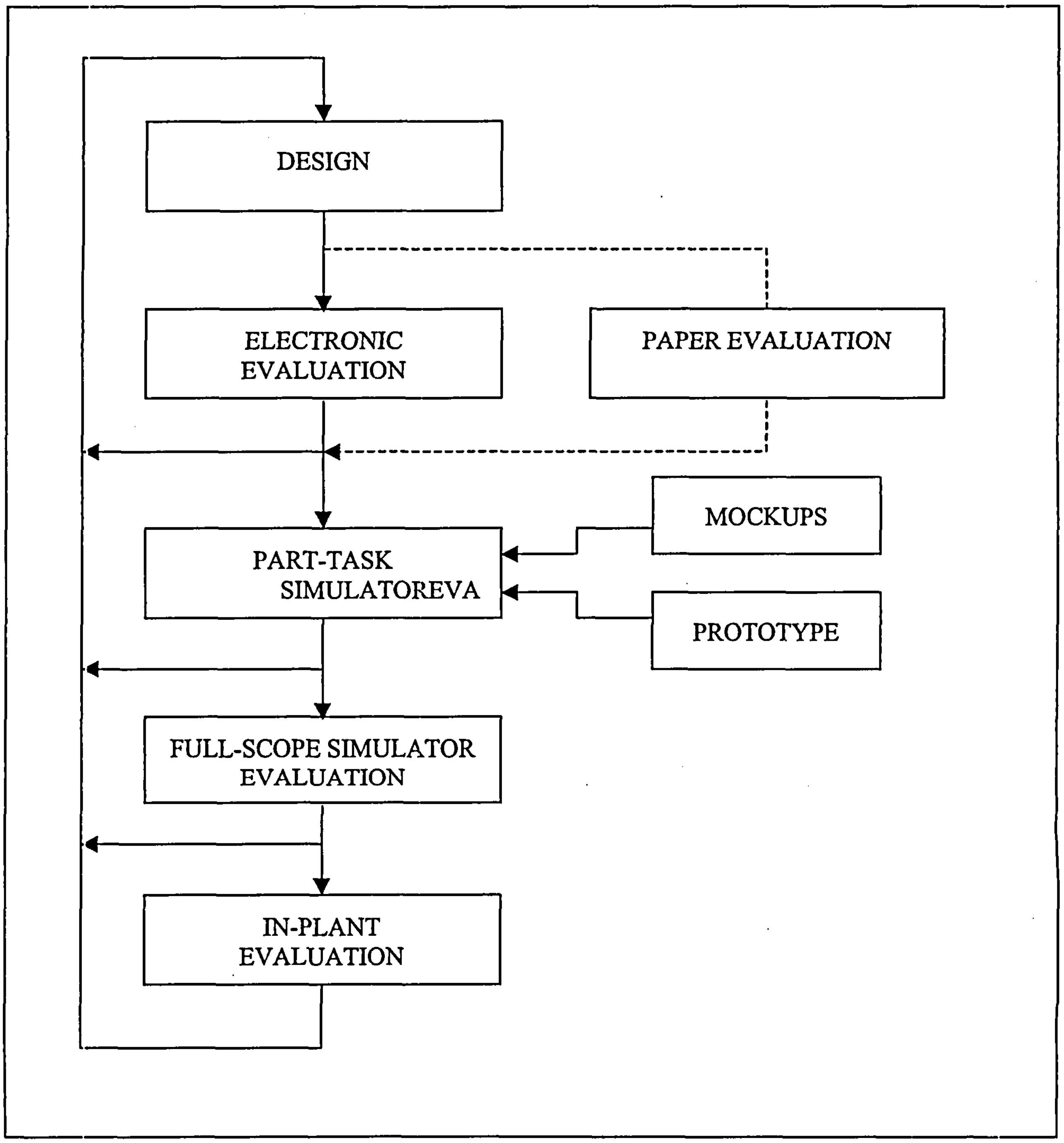


Figure 6 Levels of Design and Evaluation

Figure 7 Evaluation with Multiple Methods



Appendix A: Human Factor Principles Derived From Operating Experience Reviews of Previous NPP HSI Designs

A.1 Control Room Design

1. The large size of the control room and console and their configuration contributed to operator dissatisfaction.

2. Traffic flows should not be impeded by placement of consoles.

3. Adequate levels of illumination are necessary to ensure that visual effectiveness is sufficient for task performance. Emergency lighting should be available.

4. Noise levels in the MCR should be maintained within acceptable industry levels.

5. The climate control system in the control room should be capable of continuously maintaining temperature and humidity within the human comfort zone.

6. Convenient storage should be provided so that procedures, logs, and drawings needed for routine job performance are conveniently available. Storage should also be provided for equipment needed for emergency operation.

A.2 Control Board Design

1. Control boards should be optimized for minimum manning.

2. Panels in the control rooms were observed to have large arrays of identical controls and displays and repetitive labels. The systems, subsystems, and components should be separated by appropriate demarcation methods.

3. Controls and related displays should be located in close proximity so that the two items are readily associated and can be used conveniently with one another. Controls should be placed in an obvious and consistent order. The displays and controls used to monitor major system functions should be assigned to and arranged in functional groups.

4. Flow arrangements between CRT display formats and controls on panels should not differ.

5. Flow mimics should be used to aid (and not unintentionally mislead) the operators.

6. Panel arrangements for similar systems should be the same.

7. Location of controls in areas and orientations that render them vulnerable to accidental contact and disturbance should be avoided.

8. Unclear, illogical, overly complex, or mirror-imaged control board or panel layout arrangements have been observed to promote operational mishaps and should be avoided.

A.3 Computer

1. Computer data should be available on CRT and hard copy output.

2. Computer audible alarms should not be distracting.

A.4 CRT Displays

1. The nomenclature, labeling, and arrangement of systems on the CRT displays should be similar to the panels.

2. CRT displays should be comprehensible with a minimum of visual search. When data is presented in lines and columns, the lines of data should be separated by a space (blank line), one character high, every 4-5 lines.

3. Display access should be efficient and require a minimum of keystrokes.

4. CRT displays should have convenient brightness, focus, and degauss controls.

5. The character height should be the appropriate height for the viewing distance during normal and emergency conditions.

6. Visibility of CRT displays should not be affected by glare.

A.5 Anthropometric

1. Panel dimensions should accommodate the 5 to 95 percentile range of the user population to ensure that personnel can see and reach the displays and controls or the front and back panels. Displays should not be placed beyond the visual range of the operators.

2. Controls should not be located in the control panels that require the operator to lean into the panel. This is a potential health risk to the operator and to the equipment.

A.6 Controls

1. Large controls were observed to have been used in place of preferred smaller controls. Larger controls impact panel size and should be avoided.

2. Labeling or coding techniques should be used to differentiate controls and indicator lights of similar appearance.

3. Control configurations should not introduce parallax problems.

4. Control switches that must be held by the operator for operation should be avoided unless necessary.

5. Projecting control handles should not cover or obstruct labels.

6. Key lock switches require administrative control and should be avoided if possible.

7. Control handles should not be difficult to operate and should not cause the operators to resort to using unauthorized mechanical leveraging devices (i.e., "cheaters") to achieve reduced difficulty in operation.

8. Controls should be built and installed following standard conventions for OPEN/CLOSE and INCREASE/DECREASE. Setpoint scales should not move up in response to a downward movement of the controller thumbwheel.

9. Inadvertent operation of adjacent controls may be reduced through the use of shape coding such as using similar shaped handles for similar functions (i.e., pistol grips for pumps and round handles for valves)

A.7 Indicator Lights

1. Instances of improper use of qualitative indicators were observed where quantitative displays such as meters would be more effective.

2. Light status (on/off) should be visible to the operator. Extinguished bulbs should be obvious and a test method provided. Lamp designs should allow for easy access for lamp removal.

3. The use of so-called negative indications (the absence of an indication) should not be used to convey information to the operator.

4. Indicator design selection and layout should be standardized to conserve panel space.

5. A color code standard should be established for indicating lights.

A.8 Display and Information Processing

1. Plant parameter validity should not have to be inferred. In addition to secondary information, the quality or validity of the displayed parameter should be available to allow operators to readily identify improper ESF or other safety equipment status under various operating modes.

2. Necessary information should be available during events such as SBO (Station Black Out) and LOOP (Loss Of Offsite Power). Systems and indications such as Neutron Monitoring System, control rod position indication, and drywell area radiation indication should all be available during these events.

3. The MCR should contain an integrating overview display. The overview display should provide a limited number of key operating parameters.

4. The operators should use the same displays that are used during normal operation during accident conditions to ensure their familiarity with the interface.

A.9 Meters

1. Proper use of minor, intermediate, and major scale markings in association with scale numerals should be made. Formats should be customized to take into account identification of normal operating values and limits. Scale numerical progressions and formats should be selected for the process parameter being presented.

2. Placement of meters above and below eye level, making the upper and lower segment of the scale difficult to read, (especially with curved scales), can present parallax problems.

3. Meters were observed that fail with the pointer reading in the normal operating band of the scale. The instrument design should allow the operator to determine a valid indication from a failed indication.

4. Placement of meters on panels should prevent glare and reflections caused by overhead illumination.

5. Where redundant channels of instrumentation exist, software-based displays should provide for easy inspection of the source data and intermediate results without the need to display them continuously.

6. Data presented to the operator should be in a usable form and not require the operator to calculate its value. Scale graduations should be consistent and easily readable. Zone markings should be provided to aid in data interpretation.

7. Meter pointers should not obscure the scale on meters.

8. Process units between the control room instruments and the operating procedures should be consistent.

A.10 Chart Recorders

1. Recorders should not be used in place of meters. Recorders should be selected with consideration given to minimizing required maintenance and high reliability.

2. A recorder designed to monitor 24 parameters was observed to have 42 parameters assigned to it. This makes it extremely difficult to read the numerical

outputs on the chart paper. The inputs assigned should be consistent with the design of the recorder.

3. Operational limits should be defined on recorders. Proper selection of recorder scales will eliminate the need for overlays. The units for the process should be labeled on the recorder.

4. Monitored inputs should be assigned to recorder pens in alphabetical order. The correlation of pen color to input parameter should be clearly defined by multi-pen recorder labels.

5. The change of chart speed should also be noted on the chart paper when the paper is changed. The paper scales should match the fixed scales.

6. Recorders should have fast speed and point select capability.

7. Proper placement of recorders and adequate illumination should prevent glare and parallax problems with recorder faces.

8. The pointers should not cover the graduation marks.

9. When upper and lower pens coincide, the printout of the upper scale should still be visible.

A.11 Annunciator Warning Systems

1. Annunciators should be located near the control board panel elements to which they are related. Divisional arrangements should be consistent. Annunciators should be functionally located near the applicable System.

2. "Advisory alarms" reporting expected conditions should not be grouped with true alarms. The audio and visual warning system signal should be prioritized to reduce the audio and visual burden placed on the operators during an event.

3. Some alarms were observed to lack specificity. Multi-input alarms, e.g., xyz pressure/levels, hi/lo, frustrate, rather than inform the operator.

4. Excessive alarms were observed during emergency conditions. Auditory signals should be coded to aid the operator in determining the panel location.

5. Alarm operating sequence control should be placed at specific locations to encourage operator acknowledgment.

6. For standing and sit-down workstations, window size and lettering height should be consistent with the viewing distance.

7. The labels should use consistent abbreviations and nomenclature and not be ambiguous.

8. For traceability to response procedures, the windows should be identified with a location reference code.

9. A consistent color coding convention should be employed.

10. A "First Out" feature should be provided that presents prioritized parameters important to safety parameters for immediate operator response.

11. Means should be provided for identification of out-of-service annunciators.

12. Annunciators for conditions which signal an EOP entry condition should be located based on the functional analysis.

A.12 Coding of Displays and Controls

1. The color codes for the control boards should be systematically applied. Effective color coding should be used to aid in differentiating between identical controls placed in close proximity.

2. The coding of indicators should inform the operator whether a valve is open or closed.

3. Systematic approach to color and shape coding of controls should be taken.

A.13 Labeling

1. Label abbreviations, numbering, and nomenclature should be consistent. A label placement standard for the control room should be established. Labels should be placed consistently above or below the panel elements being identified and not placed between two components.

2. Hierarchical labeling schemes including size coding or differentiation of labels should be used to identify major console panels, sub-panels, and panel elements. Hierarchical labeling will eliminate the need to place redundant labels on control or display devices.

3. The content of the labels should be consistent with the procedures used by the operators.

4. The labels should meet the readability guidelines and should not be obscured by the equipment that they mounted near. A control room standard for labels should be established that address label character size and font.

5. Maintenance tags should not obscure or panel components such as displays.

6. To minimize the mispositioning of valves and other equipment, the controls and displays should be labeled with the unique number or name of the valve or piece of equipment.

A.14 Communications

1. Communications in the control room should consider the ambient noise levels in the control roomand plant. The control room operator should be able to communicate with necessary personnel in the plant. Communication equipment should also be provided at the remote shutdown panel.

2. Communications equipment design should not limit the operator's access to the controls or displays.

3. The communication system should be accessible from the operator's workstations.

A.15 Task Analysis

1. Controls and displays should be located for effective operator response to postulated events. Information needed by the operator in the control room should be readily available and not located at remote panels in the plant.

2. In addition to normal and emergency conditions, plant displays and controls should also consider low power and shutdown scenario information requirements.

A.16 Procedures

1. The measurement units in the procedure and the values indicated on display scales should be consistent.

2. Control board designs should make provisions for the operator's simultaneous referral to the procedures and the operation of the control boards.

3. The parameters displayed on electronic information systems or on the control boards should be designed to support the EOPs as well as other required monitoring tasks.

4. The safety function parameter status should be presented in an organized, readily accessible format compatible with the EOPs.

5. A procedure should address operator action in the event of computer, CRT, or printer problems or complete failure.

A.17 Operator Errors

1. Operator mishaps were observed to be caused by the absence of a timely, attention-getting indication (either qualitative or quantitative) that informs the operator that some element of the system is not operating properly.

2. Operator mishaps were also observed to result from incorrect lineup of valves.

A.18 Maintenance and Testing

1. The MCR should be designed in such a way that minimizes the need for maintenance and test personnel to work, or at least limit their presence, in the control room.

2. Control room displays should be designed and installed for easy calibration and replacement.

3. Access for inspection, operation, and routine maintenance of components should not be restrictive.

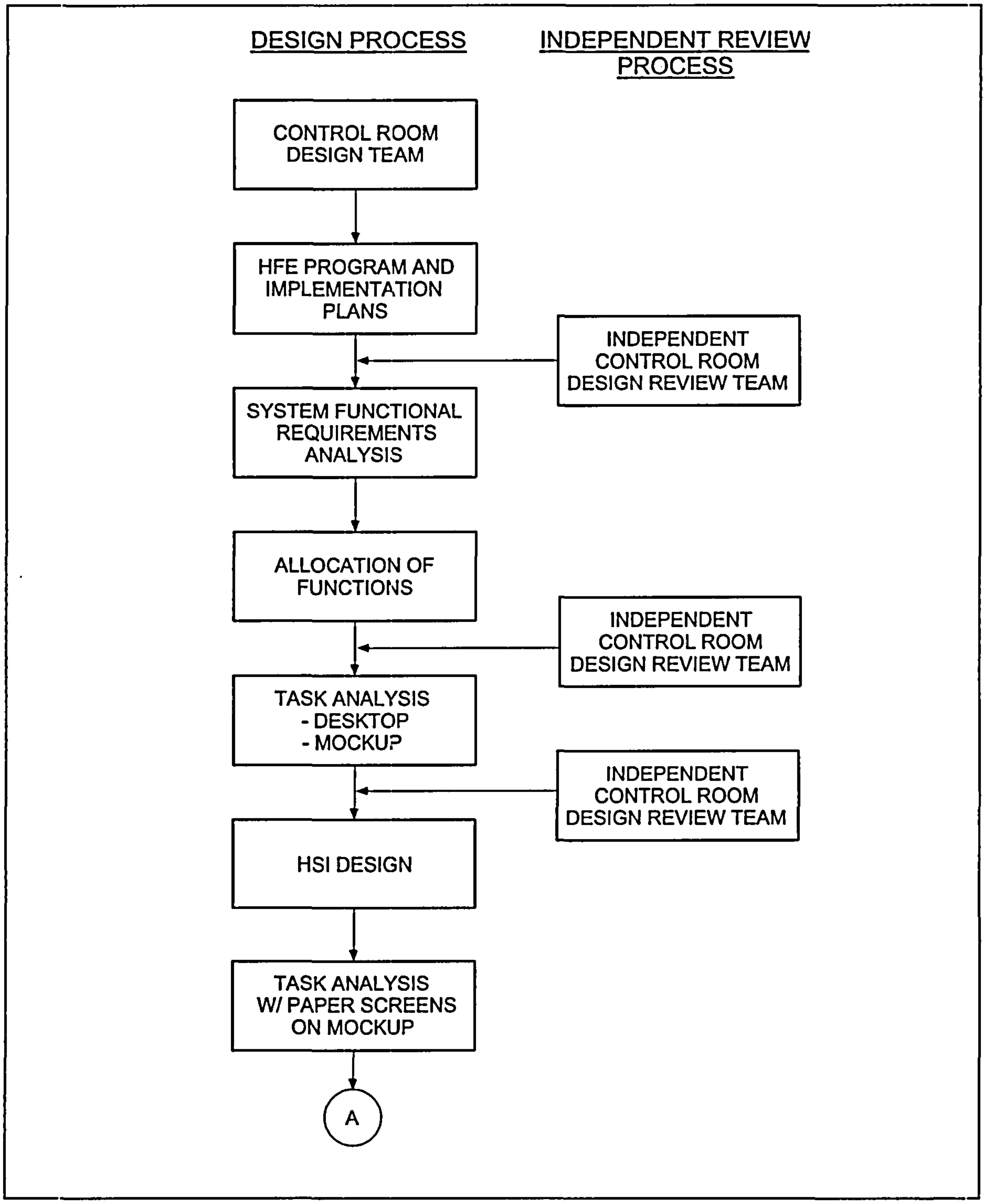


Figure 8a Human-System Design Implementation Process

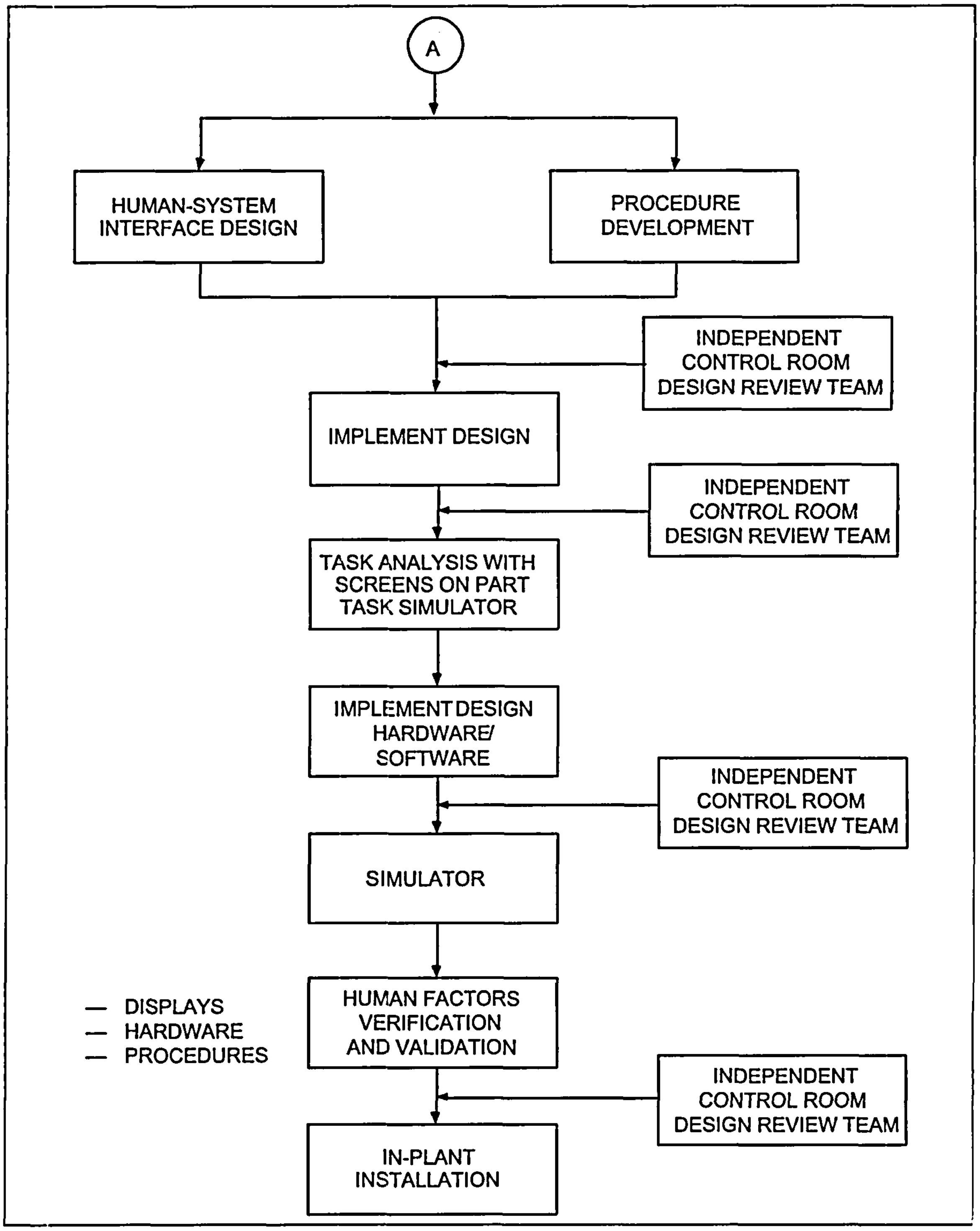


Figure 8b Human-System Design Implementation Process (Continued)

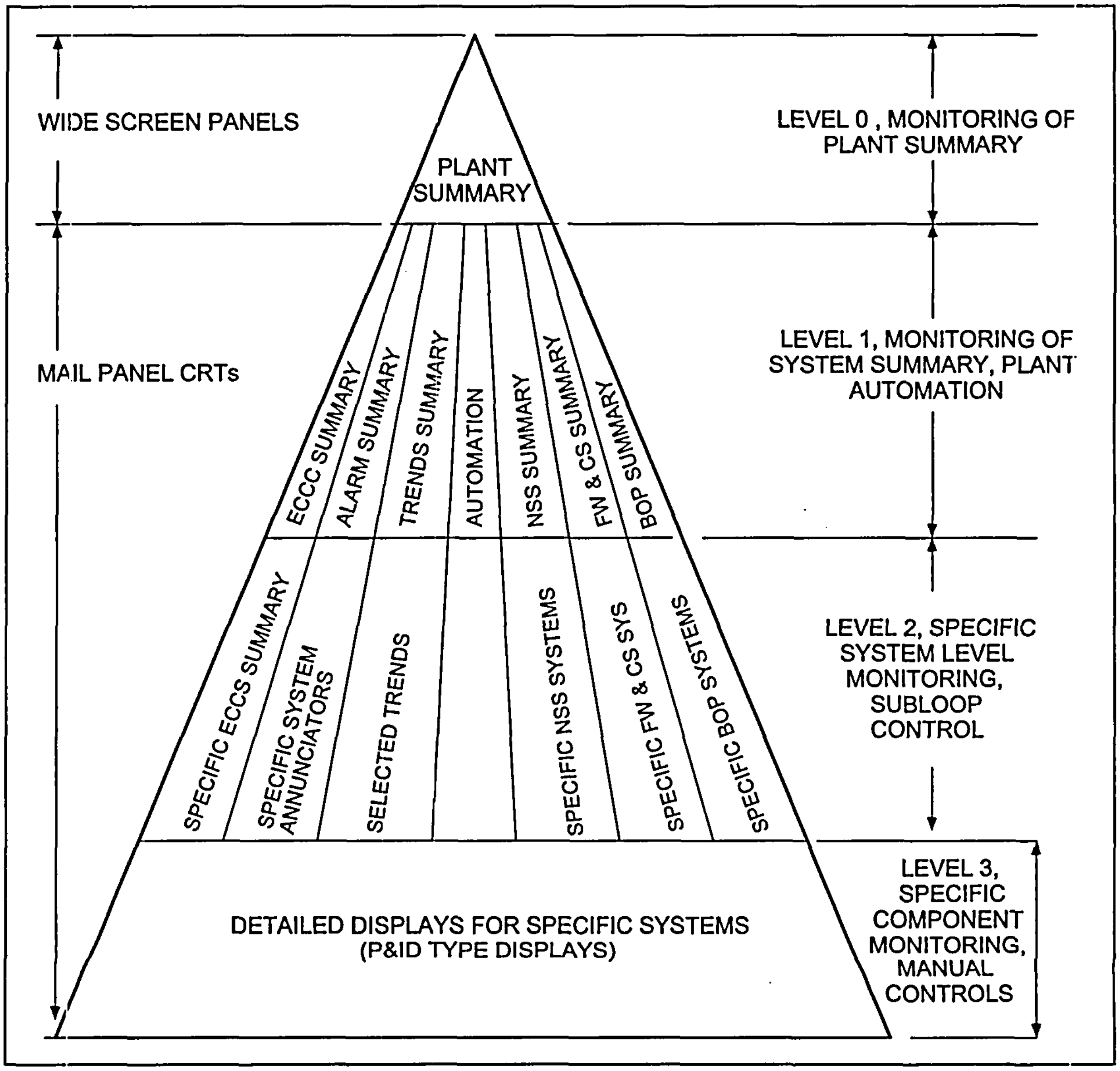


Figure 9 ESBWR Display Hierarchy for VDUs