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 06-006

Docket No. 52-010

January 6, 2006

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

Subject: **NEDO-33217, Revision 1, "ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan, January 2006**

In the Referenced letter, GE submitted the subject LTR (with no Revision indication) as "Conditional Release – pending closure of design verifications." GE has completed the internal documentation required to remove the conditional release status and is submitting Revision 1 of this LTR in Enclosure 1. There are no substantive changes between the Revision 1 LTR and that submitted via the Referenced letter.

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

Sincerely,

for

David H. Hinds
Manager, ESBWR

Reference:

MFN 05-112, Letter from David H. Hinds to U. S. Nuclear Regulatory Commission, *GE Response to Results of NRC Acceptance Review for ESBWR Design Certification Application – Item 5 (TAC # MC8168),* October 22, 2005

D068

Enclosure:

1. MFN 06-006 - NEDO-33217, Revision 1, *ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan,* January 2006

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 0000-0049-5273

# ENCLOSURE 1

# MFN 06-006

# NEDO-33217, Revision 1

# ESBWR Man-Machine Interface System

# and Human Factors Engineering Implementation Plan

# January 2006

GE Energy
Nuclear

NEDO-33217
Revision 1
eDRF# 0000-0049-5273
Class I
January 2006

# Licensing Topical Report

# ESBWR
# Man-Machine Interface System And Human Factors Engineering Implementation Plan

*Copyright 2006 General Electric Company*

# NON PROPRIETARY INFORMATION NOTICE

This document, NEDO-33217, Revision 1, 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 shall be 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


**1 Introduction ..... 8**

1.1 Purpose ..... 8

1.2 Scope ..... 9

1.3 General Approach ..... 10

**2 References ..... 11**

2.1 Supporting Documents ..... 11

2.2 Human Factors Engineering References ..... 12

2.3 Hardware and Software Development References ..... 15

2.4 Definitions ..... 18

**3 HFE Program ..... 19**

3.1 Management ..... 19

3.2 HFE Team and Organization ..... 23

3.2.1 Machine Interface System (M-MIS) Design Team ..... 23

3.2.2 HFE Process and Procedures ..... 25

3.3 ESBWR M-MIS Design Bases and Goals ..... 26

3.3.1 Design Bases ..... 26

3.3.2 Design Goals ..... 28

3.4 Control Room Standard Design Features ..... 28

3.4.1 Use of Standard Plant Detailed Design Information ..... 30

3.4.2 Standardization of Components ..... 30

3.4.3 Control System Data Gathering, Transmission, and Processing ..... 30

3.5 Use of Proven Technology ..... 33

3.5.1 Criteria for Proven Technology ..... 33

3.5.2 Criteria for Unproven Technology ..... 34

3.6 Review of Operating Experience ..... 34

3.7 Human Interface to Plant Conditions ..... 37

3.7.1 Electronic Displays ..... 37

3.7.2 Testability ..... 37

3.7.3 Maintainability ..... 38

3.7.4 Constructability ..... 39

3.7.5 Alarms ..... 39

**4 Human Factors Engineering Process ..... 43**

4.1 General Requirements ..... 43

4.2 HFE Issue Tracking System ..... 45

4.3 System Functional Requirements Analysis Implementation ..... 45

4.4 Allocation of Function Implementation ....47
4.5 Task Analysis Implementation ....51
4.6 Staffing and Qualifications ....53
4.6.1 Background ....53
4.6.2 ESBWR Baseline Staffing Assumptions ....53
4.6.3 Staffing and Qualifications Plan ....54
4.7 Human Reliability Analysis ....56
4.7.1 Purpose ....56
4.7.2 HRA Requirements Development ....56
4.7.3 Methodology ....57
4.8 Human-System Interface (HSI) Design Implementation ....60
4.8.1 HSI Design Inputs ....60
4.8.2 Concept of Operations ....61
4.8.3 Functional Requirement Specification ....62
4.8.4 HSI Concept Design ....62
4.8.5 HSI Detailed Design and Integration ....62
4.8.6 HSI Tests and Evaluations ....63
4.8.7 HSI Design Documentation ....64
4.8.8 HSI Design Implementation Plan ....65
4.9 Plant Procedures ....66
4.10 Training Program Development ....67
4.10.1 Purpose ....67
4.10.2 Elements for training program development ....67
4.11 Human Factors Verification & Validation Activities ....72
4.11.1 Operational Conditions Sampling ....73
4.11.2 Design Verification (HFE) ....77
4.11.3 Integrated System Validation ....79
4.11.4 Human Factors Issue Resolution Verification ....82
4.11.5 Final Plant HFE/HSI Design Verification ....82
4.11.6 Relation to Hardware/Software V&V Process ....83
4.11.7 Integrated System Verification ....83
4.11.8 End-Users as Participants and Test Subjects ....84
4.11.9 Documentation, Reporting, and Integration of Results ....84
4.11.10 V&V Implementation ....85
4.12 Implementation of Human Factors Issue Resolution Verification ....113
4.12.2 Implementation of Final Plant HFE/HSI Design Verification ....114
4.12.3 Implementation of HFEITS ....117

**5 Design Implementation Process, HFE Infrastructure (Hardware and Software)...120**
5.1 Software Quality Program For Hardware/Software Design and Development...120
5.1.1 Software Quality Assurance Program ....121
5.1.2 Software Management Plan ....123

5.1.3 Software Development Project Plan ..... 125
5.1.4 Software Configuration Management Plan ..... 126
5.1.5 Verification And Validation Plan ..... 128
5.1.6 Software Safety Plan ..... 130
5.1.7 Software Test Plan ..... 131
5.1.8 Operational and Maintenance Manual (O&M Manual) ..... 132
5.1.9 Training Plan ..... 133
5.2 Other Required Plans and Programs ..... 134
5.2.1 Electromagnetic Compatibility (EMC) Compliance Plan ..... 134
5.2.2 Set-Point Methodology Plan ..... 136
5.2.3 Equipment Qualification Program ..... 137
5.2.4 As-Built Verification Program ..... 138
5.3 General Design Requirements ..... 138
5.3.1 Equipment Hardware and Software Performance Specification ..... 138
5.3.2 Equipment User's Manual ..... 139
5.3.3 Software Design ..... 139
5.4 Software Implementation ..... 140
5.4.1 Software Coding ..... **Error! Bookmark not defined.**
5.4.2 Software Source Code ..... 140
5.4.3 Software Module Testing ..... 141
5.5 M-MIS Integrated Factory Acceptance Test ..... 141

**6 Implementation Milestones and Responsibilities ..... 141**
6.1 Provisions for COL Applicant Involvement and Responsibilities ..... 141
6.2 Provisions for NRC Conformance Reviews ..... 142
6.3 Human Performance Monitoring ..... 143
6.3.1 Purpose ..... 143
6.3.2 HPM Strategy Development ..... 143
6.3.3 Elements of HPM process ..... 144

## Appendices

**Appendix A: Human Factors Engineering Issue Tracking System ..... 149**
HFE Issue Tracking System ..... 149

**Appendix B: ESBWR Subordinate Plan Outlines ..... 155**
Attachment A: System Functional Requirements Analysis Implementation Plan (Draft) Table of Contents ..... 155
Attachment B: Allocation of Functions Implementation Plan (Draft) Table of Contents 157
Attachment C: Task Analysis (Draft) Table of Contents ..... 159
Attachment D: Human System Interface Design Implementation Plan (Draft) Table of Contents ..... 161

Attachment E: Human Factors Verification and Validation (Draft) Table of Contents .165
Attachment F: Procedures Development Implementation Plan (Draft) Table of Contents167
Attachment G: Software Management Plan (Draft) Table of Contents.....168
Attachment H: Software Configuration Management Plan (Draft) Table of Contents .171
Attachment I: Software Verification and Validation Plan (Draft) Table of Contents ...174
Attachment J: Software Safety Plan Table of Contents.....176

## List of Tables

Table A-1 Example HFE Tracking Issue Data Sheet ..... 152

## List of Figures

Figure 1.2 ESBWR M-MIS Implementation Plan Process Flowchart .....146
Figure 4.4 Allocations of Functions to Human and Machine Resources .....147
Figure 4.7-1 The Role of Human Reliability Analysis in the HFE Program.....148
Figure A-1 HFE Issue (HED) Evaluation Process.....154

# 1 Introduction

## 1.1 Purpose

The purpose of this plan is to ensure through human-centered design, development and operational activities that the vital role personnel play in the safe efficient production of electric power at ESBWRs can be accomplished under normal and emergency conditions.

To accomplish this goal the overall structured elements of the HFE program includes:

- Developing an integrated HFE design process into the plant development, design, and evaluation.
- Providing HFE products (e.g., HSIs, procedures, and training) that provide safe, efficient, and reliable performance of operation, maintenance, test, inspection, and surveillance tasks.
- Incorporating products which reflect "state-of-the-art human factors principles"
- Satisfying all the specific regulatory requirements that support the ability of operators to perform required tasks .

As examples, developing: a safety parameter display system (SPDS) console, automatic indication of bypassed and operable status of safety systems, and monitoring capability in the control room of a variety of system parameters will be carefully considered. ESBWR will develop a plant-referenced simulator capability throughout the DCD, COL, and plant startup schedule to provide a platform for HFE design and verification activities.

ESBWR HFE will use this HFE program plan, which is implemented by a qualified HFE design team. The ESBWR "M-MIS design team" is defined in section 3.2.1.

The Man-Machine Interface System (M-MIS) implementation plan will:

1. Describe the methodology used to implement the ESBWR Human Factors Engineering (HFE) and Human Systems Interface (HSI) Design activity.
2. Describe the methodology used to implement the Hardware and Software Design Implementation activity and comply with the requirements of Chapter 7 Appendix B of the ESBWR Design Control Document (BTP 14).
3. Describe how this implementation complies with the requirements of Chapter 18 of the ESBWR Design Control Document (DCD).

4. Describe the methodology to utilize the detailed design information available from the ABWR reference plant and US standard plant design.

5. Provide a systems design approach to ensure that the overall ESBWR design is implemented, tested and constructed in an integrated manner.

## 1.2 Scope

The following design and implementation activities are covered in this plan.

1. The ESBWR Human-System Interface Design Implementation activity

2. The ESBWR Hardware and Software Design Implementation activity

3. The DCIS (Hardware and Software) QA plan and processes by which all activities associated with this plan will be executed.

The terms HSI and M-MIS are used in this Plan as defined below:

- Human-System Interface (HSI) is the means through which personnel interact with the plant, including the alarms, displays, controls, and job performance aids. Generically this includes operations, maintenance, test, and inspection interfaces.

- M-MIS is those systems that perform the monitoring, control, alarming and protection functions. This also includes the design of the facilities. The M-MIS Design Team (Design Team) is a team as described in Section 3.2.1, responsible for the design of the M-MIS systems and its HFE elements.

Engineering activities in this plan will be conducted in accordance with the ESBWR Project Management Manual (PMM) and the GE Energy Nuclear (GEEN) QA plans. The PMM define the engineering interface processes for interfaces between M-MIS design engineers and other ESBWR system design disciplines. The Plan will specifically address the requirements for COL Applicant involvement and use of mock-ups partial or prototype simulations to facilitate owner involvement and design iterations, as described in the ESBWR DCD. In addition, the Plan establishes a detailed M-MIS design and implementation process. The implementation process is represented in the flowchart form in Figure 1.2. This process flowchart includes specific milestones and will be integrated into the overall ESBWR integrated project to provide updating and tracking capability.

The selection of the design tools and databases for the M-MIS will be defined in the Software Management Plan (SMP). The SMP will define the design and evaluation tools that will be used in the design and evaluation of the M-MIS and HSI. Section 5.1.2 describes the SMP.

## 1.3 General Approach

The general approach to the implementation of the ESBWR M-MIS will be to, (a) create plans in accordance with NRC guidelines, (b) establish baseline design inputs from previous ABWR system control room designs, (c) prepare ESBWR specific gap analysis to ABWRs, including an Operating Experience Review, (d) execute the HFE plans through to turnover to the COL Applicant, (e) follow standard human factors engineering and I&C practices and processes, (f) follow the activities for HSI design and system hardware/software design, and (g) meet the commitments of ESBWR DCD Chapter 18. A full-scale ESBWR control room mockup and part-task simulator will be constructed and will serve as the focal point for integration of the HSI design development work and the developmental hardware/software work. The HSI design activity and the hardware/software development activity will be coordinated through the periodic milestones for development of the mockup/part-task simulator. The goal is to have a mockup that can be easily modified for quick evaluation of iterative design changes. The mockup will be the principle means to facilitate plant COL Applicant involvement and evaluations throughout the entire M-MIS implementation process. As development on the mockup/part-task simulator proceeds, the intention is to complete the M-MIS design process with final validation taking place using the ESBWR full-scope simulator in post COL period, but 30 months prior to plant start up.

The HSI design activity will be conducted in accordance with implementation plans for System Functional Requirements Analysis, Allocation of Functions, Task Analysis, Human-System Interface Design, and Human Factors Verification and Validation and the GEEN QA plan. The ESBWR HSI, consistent with the definition of HSI given in NUREG-0711, is the means through which personnel interact with the plant, including the alarms, displays, controls, and job performance aids.

In accordance with GEEN QA, the M-MIS design process provides for independent verification of all aspects of the M-MIS design throughout the process. This independent verification process specifically includes the verification that individual stages of the process are correct and that the transfer of information from stage to stage has been properly accomplished. The independent review process also validates that the overall M-MIS will accomplish the intended functions, and verification that the individual steps in the process of design have been properly carried out. The scope of independent verification will include any issue or area of inquiry which the reviewers or COL Applicant (at later stages) considers may affect the suitability of the M-MIS to accomplish the safety goals.

# 2 References[1]

For all references listed below, revision numbers if applicable have been omitted; the latest revision available is assumed to be the current reference.

## 2.1 Supporting Documents

1. ESBWR DCD Chapter 18 revision 0, August 2005 (GE 26A6642BX)
2. Distributed Control and Information System (DCIS) Hardware/Software Specification
3. OER Review Plan
4. System Functional Requirements Analysis Implementation Plan
5. Allocation of Functions Implementation Plan
6. Task Analysis Implementation Plan
7. Staffing and Qualification Plan
8. Human System Interface Design Implementation Plan
9. HRA Plan
10. Procedure Development Plan
11. Training Program Development Plan.
12. Human Factors Verification & Validation Implementation Plan
13. Human Performance Monitoring Plan

GEEN will be seeking a graded approach to Chapter 18 HFE and Chapter 7 Control and Instrumentation from the NRC focused on the regulatory process and design changes from the ABWR references.

[1] Within the set of documents listed, references are made to documents, which have not yet been published. These are documents, which are expected to be of potential value as guiding references. Listing of these references does not necessarily imply a commitment to apply the criteria in these future documents in total to the ESBWR. The applicable date/revision of the reference, codes, or standard is specified in the ESBWR DCD.

## 2.2 Human Factors Engineering References

1. NUREG -0700, Human-System Interface Design Review Guideline;
2. NUREG-0737, Clarification of TMI Action Plan Requirements (Item I.C.5, "Feedback of Operating Experience to Plant Staff");
3. NUREG-0899, Guidelines for the Preparation of Emergency Operating Procedures;
4. NUREG/CR-3331, A Methodology for Allocating Nuclear Power Plant Control Functions to Human and Automated Control;
5. AR602-1, Human Factors Engineering Program, (Dept. of Defense);
6. EPRI NP-3659, Human Factors Guide for Nuclear Power Plant Control Room Development, (Electric Power Research Institute);
7. ANSI/IEEE Std. 1023, IEEE Guide to the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations, (IEEE);
8. DI-HFAC-80740, Human Engineering Program Plan, (Dept. of Defense);
9. DOD-HDBK-763, Human Engineering Procedures Guide, Chapters 5-7 and Appendices A and B, (Dept. of Defense);
10. MIL-H-46855B, Human Engineering Requirements for Military Systems, Equipment and Facilities (Dept. of Defense);
11. TOP-1-2-610, Test Operating Procedure Part 1, (Dept. of Defense);
12. NUREG-0711, Human Factors Engineering Program Review Model;
13. NUREG/CR-5908, Advanced Human-System Interface Design Review Guideline;
14. NUREG/CR 6633 Advanced Information Systems: Technical Basis and Human Factors Review Guidance;
15. NUREG/CR 6634, Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance;
16. NUREG-1649Reactor Oversight Process;
17. NUREG-1764 Guidance for the Review of Changes to Human Actions;

18. EPRI NP-3448-L, A Procedure for Reviewing and Improving Power Plant Alarm Systems;

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

20. EPRI NP-3701, Computer Generated Display Guidelines (Volumes 1 and 2);

21. EPRI, NP-4350, Human Engineering Design Guidelines for Maintainability (Electric Power Research Institute);

22. ASME, "Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications," ASME RA-S-2002, ASME, April 5, 2002;

23. EPRI NP-3583, "Systematic Human Action Reliability Procedure (SHARP)," 1984;

24. EPRI NP-6560-L, "A Human Reliability Analysis Approach Using Measurements for Individual Plant Examination," 1990;

25. EPRI Report TR-100259, "An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment," 1992;

26. EPRI TP-101711 "SHARP1—A Revised Systematic Human Action Reliability Procedure, 1992;

27. Hollnagel, E., "Cognitive reliability and error analysis method, CREAM," Elsevier, Oxford, 1998;

28. IEEE Draft Standard 1574, "Best Practices for Conducting Human Reliability Analysis (HRA)," in review, expected 2006;

29. IEEE Standard 1082, "Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations," IEEE 1997;

30. Julius, J., "The EPRI HRA Calculator," EPRI, Palo Alto, CA, 2001;

31. NUREG/CR-1278, "Handbook of human reliability analysis with emphasis on nuclear power plant applications," SNL, 1983;

32. NUREG/CR-4674-V17-26, Precursors to Potential Severe Core Damage Accidents: 1992, A Status Report, Oak Ridge National Laboratory, 1992;

33. NUREG/CR-4772, Accident Sequence Evaluation Program (ASEP) Human Reliability Analysis Procedure, Sandia National Laboratories, 1987;

34. NUREG/CR-6350, "A Technique for Human Error Analysis (ATHEANA)," 1996;

35. NUREG/CR-6689: Proposed Approach for Reviewing Changes to Risk-Important Human Actions 2000;

36. NUREG/CR-6883, " The SPAR-H Human Reliability Analysis Method," Idaho National Laboratory, Office of Nuclear Regulatory Research, August 2005;

37. NUREG-0800: Standard Review Plan: Chapter 19, Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decision Making: General Guidance (NRC (2002);

38. NUREG-1560: Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance (NRC, 1997);

39. NUREG-1624, Rev. 1.: Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA) (NRC, 2000);

40. NUREG-1792, "Good Practices for Implementing Human Reliability Analysis (HRA)," Draft Report for Comment, Office of Nuclear Regulatory Research, July 2004;

41. Rasmussen, J. "Information Processing and Human-Machine Interaction," North Holland, New York, 1986;

42. Regulatory Guide 1.174: An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis, 1998;

43. EPRI NP-6209, Effective Plant Labeling and Coding (Electric Power Research Institute);

44. CN Number 02-001: NRC Inspection Manual: Chapter 2515, Light-Water Reactor Inspection Program - Operations Phase (NRC, 2002);

45. CN Number 01-015: NRC Inspection Manual: Chapter 0609, Significance Determination Process (NRC, 2001);

46. IP 71715: Sustained Control Room and Plant Observation. (NRC, periodically updated). NUREG-1649: Reactor Oversight Process (NRC, 2000);

47. Regulatory Guide 1.174: An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis (NRC, 1998);

48. DOE Order 5480.19, Conduct of Operations Requirements for DOE Facilities; and

49. INPO 85-017 Rev 2, Guidelines for the Conduct of Operations at Nuclear Power Stations.

## 2.3 Hardware and Software Development References

1. ESBWR Standard Review Plan (SRP), Section 7, Branch Technical Position HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems;

2. NUREG/CR-6082, Data Communications;

3. NUREG/CR-6083, Reviewing Real-Time Performance of Nuclear Reactor Safety Systems;

4. NUREG/CR-6101, Software Reliability;

5. NUREG/CR-6278, Survey of Industry Methods for Providing Highly Reliable Software;

6. IEEE Std. 279, Criteria for Protection Systems for Nuclear Power Generating Stations (IEEE);

7. IEEE Std. 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE);

8. ANSI/IEEE Std. 730, Standard for Software Quality Assurance Plans (IEEE);

9. ANSI/IEEE Std. 828, Standard for Software Configuration Management Plans (IEEE);

10. ANSI/IEEE Std. 829, Software Test Documentation (IEEE);

11. ANSI/IEEE Std. 830, Guide on Software Requirement Specifications (IEEE);

12. ANSI/IEEE Std. 983, Guide for Software Quality Assurance Planning (IEEE);

13. ANSI/IEEE Std. 1008, Standard for Software Unit Testing (IEEE);

14. ANSI/IEEE Std. 1012, Standard for Software Verification and Validation Plans (IEEE);

15. ANSI/IEEE Std. 1016, Recommended Practice for Software Design Descriptions (IEEE);

16. ANSI/IEEE Std. 1028, Standard for Software Reviews and Audits (IEEE);

17. ANSI/IEEE Std. 1042, Guide for Software Configuration Management (IEEE);

18. ANSI/IEEE Std. 1058.1, Standard for Software Project Management Plans (IEEE);

19. ANSI/IEEE Std. 1063, Standard for Software User Documentation (IEEE);

20. ASME NQA-2A, Part 2.7, Quality Assurance Requirements of Computer Software for Nuclear Facility Applications (ASME);

21. Regulatory Guide 1.152, Criteria.for Programmable Digital Computer System Software in Safety Related Systems of Nuclear Power Plants (US Nuclear Regulatory Commission);

22. Regulatory Guide 1.153, Criteria for Safety Systems (U.S. Nuclear Regulatory Commission)

23. ANSI/IEEE-ANS-7-4.3.2, American National Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations (IEEE);

24. EPRI TR-102348, Guideline on Licensing Digital Upgrades;

25. EPRI TR-102306, Plant Communications and Computing Architecture Plan Methodology, Vol. 1, Methodology Manual;

26. EPRI TR-102306, Plant Communications and Computing Architecture Plan Methodology, Vol. 2, Workbook;

27. EPRI TR-102303, Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants;

28. EPRI TR-102400, Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants, Vol. 1, Fundamentals of EMI Control;

29. EPRI TR-102400, Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants, Vol. 2, Implementation Guide for EMI Control;

30. EPRI TR-103291, Handbook of Verification and Validation for Digital Systems, Vol. 1, Summary;

31. EPRI TR-103291, Handbook of Verification and Validation for Digital Systems, Vol. 2, Case Histories;

32. EPRI TR-102391, Handbook of Verification and Validation for Digital Systems, Vol. 3, Topical Reviews;

33. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 1, Project Summary;

34. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 2, Survey and Assessment of Conventional Software Verification and Validation Methods;

35. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 3, Survey and Documentation of Expert System Verification and Validation Methodologies;

36. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 4, Evaluation of Knowledge Base Certification Methods;

37. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 5, Validation and Verification Guideline Packages and Procedures;

38. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 6, Selection of Validation Scenarios;

39. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 7, Users Manual for Verification and Validation Guideline Packages and Procedures;

40. EPRI TR-103331, Guidelines for the Verification and Validation of Expert System Software and Convention Software, Vol. 8, Bibliography;

41. EPRI TR-103916, Verification and Validation Guidelines for High Integrity Systems;

42. EPRI TR-104595, Abnormal Conditions and Events Analysis for Instrumentation and Control Systems, Vol. 2, Survey and Evaluation of Industry Practices;

43. EPRI NP-5652, Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications;

44. EPRI TR-102260, Supplemental Guidance for the Application of EPRI NP-5652 on the Utilization of Commercial Grade Items; and

45. EPRI TR-1002835 Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades.

## 2.4 Definitions

Chapter 7 of the ESBWR DCD defines the systems, which perform the monitoring, control, and protection functions of the plant as the Man-Machine Interface Systems (M-MIS). The M-MIS is comprised of the following functions:

1. Data gathering equipment which monitors equipment and process variables;

2. Data communication equipment which transmits equipment and process variables between data processing equipment and plant equipment;

3. Data processing equipment which manipulates data for use by plant personnel and/or automatic protection and control equipment;

4. Plant information display and control equipment which provides alarm and display media for plant personnel to access plant processes and equipment status, and controls to operate plant equipment; and

5. Output processing equipment which provides the necessary interfaces between plant controls and plant equipment actuators.

The M-MIS 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. The requirements of this chapter are directed at the Plant Designer and are applicable to all equipment supplied as part of the M-MIS. The M-MIS specifically includes:

1. Instrumentation, including sensors and local instruments, for all safety and non-safety systems throughout the plant;
2. Automatic and manual controls for all safety and non-safety systems;
3. Protection functions, including safety and non-safety systems;
4. Diagnostic systems, including loose parts monitoring, rotating machinery diagnostics, neutron noise monitoring, etc.;
5. Monitoring and control stations for the plant systems, including the main control room (MCR), remote shutdown control station, technical support center, emergency operations facility, and local control stations;
6. Instrumentation and control power supplies, grounding, and environmental compatibility;
7. Computer systems for control, data acquisition, display, storage and retrieval, monitoring and alarms, technical support, and operations support; and
8. Plant communications systems including data, visual, and voice intraplant communication associated with plant operation and maintenance;

Additionally, use of static mockups and a dynamic simulator will be used as design tools for the design of the M-MIS and verification and validation of the M-MIS.

# 3 HFE Program

## 3.1 Management

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

- personnel tasks can be accomplished within time and performance criteria
- the HSIs, procedures, staffing/qualifications, training and management and organizational support will support a high degree of operating crew situation awareness
- the plant design and allocation of functions will maintain operation vigilance and provide acceptable workload levels i.e., to minimize periods of operator underload and overload
- the operator interfaces will minimize operator error and will provide for error detection and

- recovery capability

2) *Assumptions and Constraints* - An assumption or constraint is an aspect of the design will identified, such as a:

   a. specific staffing plan or the use of specific HSI technology, that is an input to the HFE program

   b. rather than the result of HFE analyses and evaluations. The design assumptions and constraints

3) Applicable Facilities - The HFE program will address the main control room, remote shutdown facility, technical support center (TSC), emergency operations facility (EOF), and local control stations (LCSs).

4) Applicable HSIs, Procedures and Training - The applicable HSIs, procedures, and training included in the HFE program will include all operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures). This includes monitoring the designs being presented by ESBWR suppliers, to ensure that supplier design are consistent with the HFE requirements of the ESBWR HFE Program.

5) Applicable Plant Personnel - Plant personnel who will be addressed by the HFE program include licensed control room operators as defined in 10 CFR Part 55 and the following categories of personnel defined by 10 CFR 50.120: nonlicensed operators, shift supervisor, shift technical advisor, instrument and control technician, electrical maintenance personnel, mechanical maintenance personnel, radiological protection technician, chemistry technician, and engineering support personnel to the extent that they perform tasks that are directly related to plant safety.

The M-MIS will employ modern digital technology to implement the majority of the monitoring, control, and protection functions for the ESBWR. Description of the technology is contained in the ESBWR system documentation prepared for the ESBWR DCD. Segmentation of major functions, separation of redundant equipment within a segment, and use of fault tolerant equipment will provide reliability and protection against the propagation of failures. Application of signal validation to selected parameters will be used to assure plant operators have data of high quality. Multiplexed data communication will be used to reduce the cost and complexity of the instrumentation and control cable runs throughout the plant. The high accuracy and drift-free operation of the digital systems will reduce the overall maintenance calibration burden. Fiber optic cables for data transmission will be used to provide high data transmission rates with electrical isolation and protection from electromagnetic interference at reduced costs.

Standardization of hardware and software, and modularity of design will be used to simplify maintenance and provide protection against obsolescence.

It is expected that the M-MIS using modern technologies will result in significant cost savings over the life of the plant through higher availability factors, lower maintenance costs, and reduced inadvertent plant trips.

The same approach to the HSI will be taken toward the design of the technical support center, emergency operations facility, remote shutdown stations, and local control stations. The NE-DCIS documentation will define the data communications and display needs of the technical support center and emergency operations facility. The Remote Shutdown System documentation will describe the capability of the remote shutdown stations to control and monitor the safe shutdown of the plant from outside the main control room.

The HSI design implementation activity will include the development of dynamic models for evaluating the overall plant response as well as individual control systems, including operator actions. These dynamic models will be:

1. Suitable for analyzing both steady state and transient behavior;
2. Used to confirm the design of the advanced alarm system concepts;
3. Used to confirm the adequacy of control schemes;
4. Used to confirm the allocation of control to an automatic system or operator;
5. Used to develop and validate plant operating procedures; and
6. Incorporated, as directly as possible, into plant general-purpose or limited use simulators.

A dynamic part-task simulator will be built to support the requirement for development of dynamic models. Using the part-task experience from the ABWR, an initial set of systems will be identified for modeling, including the development of the graphical user interfaces to be used by the operator. The part-task simulator will be used in preliminary ESBWR design and expanded to include ESBWR-unique design features. As the ESBWR design progresses, the part-task simulator will evolve through a series of iterative evaluations and will result in the development of a complete control room full scope simulator in the post COL phase. In addition, the simulator facility is intended to be the focal point for COL Applicant operator evaluations and feedback checkpoints throughout the entire M-MIS design process.

The general development of eleven key implementation plans, analyses, and evaluation of the following are identified and described in section 4:

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

ESBWR plans and execution will provide assurance that a modification to the reference ABWR to accommodate ESBWR changes will not compromise the ESBWR defense-in-depth and diversity (D-D&D) analysis for ESBWR. The D-D&D analysis will be a design input to the SFRA and will be iterated as any other engineering discipline. Important aspects of defense-in-depth are identified in RG 1.174, and will be evaluated to include:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- There is no over-reliance on programmatic activities to compensate for weaknesses in plant design. This may be pertinent to changes in credited human actions (HAs).
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.
- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed. Caution should be exercised in crediting new HAs to verify that the possibility of significant common cause errors is not created.
- Independence of barriers is not degraded.

- Defenses against human errors are preserved. For example, establish procedures for a second check or independent verification for risk-important human actions (HAs) to determine that they have been performed correctly.
- The intent of the General Design Criteria (GDC) in Appendix A to 10 CFR Part 50 is maintained. GDC that may be relevant are 3 - Fire Protection, 13 - Instrumentation and Control, 17 - Electric Power Systems, 19 - Control Room, 35 - Emergency Core Cooling System, 38 - Containment Heat Removal, and 44 - Cooling Water.

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

## 3.2 HFE Team and Organization

### 3.2.1 Machine Interface System (M-MIS) Design Team

The M-MIS implementation activities begin with the establishment of the Man-Machine Interface System (M-MIS) Design Team. Within the Design Team, the HFE group, with the support of other M-MIS staff, prepares the various implementation plans required to support the HSI design activity, and manages the activity through the remaining steps to the final validation of the implemented design. The M-MIS Design Team was originally formed during the design engineering for the reference units, was active through the ABWR Certification Program and the US Standard Plan Design (FOAKE) program. A composition of experienced individuals, whose collective expertise covers a broad range of disciplines relevant to the design and implementation activity, is maintained for the M-MIS Design Team throughout the process.

The M-MIS Design Team (referred to as the Design Team) will be comprised of at least the following areas of expertise

1. Technical Project Management;
2. Systems Engineering;
3. Nuclear Engineering;
4. Control & Instrumentation Engineering;

5. Architect Engineering;
6. Human Factors;
7. Plant Operations;
8. Computer Systems Engineering;
9. Plant Procedure Development;
10. Personnel Training;
11. System Safety Engineering; and
12. Reliability, Availability, Maintainability, and Inspection Expertise.
13. Quality Assurance

As a part of the M-MIS Design Team, a special Control Room Design Team (CRDT) will be established to coordinate the design of the Main Control Room (MCR), Remote Shutdown panels, and Local Control Stations. This CRDT will be made up of members from the M-MIS Design Team and include involvement by COL Applicant staff, including engineering and maintenance personnel and operations staff familiar with plant normal, abnormal, and emergency operating procedures. It is expected that COL Applicant will provide representatives for the CRDT.

The duties of the M-MIS Design Team will be to establish and perform the activities as defined in this Plan. The M-MIS Design Team's specific duties are to guide and oversee the design implementation activity and to assure that the execution and documentation of each step in the activity is carried out in accordance with the established program and procedures. The M-MIS Design Team will have the authority to ensure that all its areas of responsibility are accomplished and to identify problems in the implementation of the HSI design. The M-MIS Design Team will have the authority to determine where its inputs are required and to access work areas and design documentation. The M-MIS Design Team will also have the authority to control further processing, delivery, installation, or use of HSI products until the disposition of a non-conformance, deficiency, or unsatisfactory condition has been achieved and hand-over to the COL Holder is accomplished.

The M-MIS Design Team is responsible for:

- The development of all HFE plans and procedures;

- The oversight and review of SQAP's, SMP's as well as HFE design, development, test, and evaluation activities;
- The initiation, recommendation, and provision of solutions through designated channels for problems identified in the implementation of HFE activities;
- Verification that solutions to problems have been implemented;
- Assurance that HFE activities comply with the HFE plans and procedures;
- Ensure that the activities of the Quality Plan agreed to with the COL are followed; and
- The methods for reviewing M-MIS operating experience.

Independent reviews of the work of the Design Team will be conducted in accordance with GEEN QA and SQA plans to provide:

- Validation that the system and its components will perform their intended functions; and

Verification that the individual steps in the process has been properly carried out.

### 3.2.2 HFE Process and Procedures

(1) General Process Procedures - The process through which the team will execute its responsibilities is identified in the ESBWR Program Management Plan and governed by the GEEN QA. The process will address:

- assigning HFE activities to individual team members
- governing the internal management of the team
- making management decisions regarding HFE
- making HFE design decisions
- governing equipment design changes
- design team review of HFE products

(2) Process Management Tools - Tools and techniques (e.g., review forms) to be utilized by the team to verify application of HFE efforts will be identified in the individual sub-plans and the Software Management Plan.

(3) Integration of HFE and Other Plant Design Activities - The integration of design activities is established in the ESBWR program Plan, GEEN QA and herein. Figure 1.2 depicts the process that executes the integration of the engineering disciplines. It is iterative in structure and continues its process until hand-over to the COL Holder.

(4) HFE Program Milestones - HFE milestones will be identified so that evaluations of the effectiveness of the HFE effort can be made at critical checkpoints and the relationship to the integrated plant sequence of events is shown. A relative program schedule of HFE tasks showing relationships between HFE elements and activities, products, and reviews will be available for review.

(5) HFE Documentation - HFE documentation items are identified here and in the specific HFE sub-plans described in Section 4.0. Management of the documents is controlled by GEEN QA and includes retention and limited access requirements. An HFE Issue Tracking system is described in section 4.2 herein and is controlled documents within the GEEN QA Documentation system.

(6) Subcontractor HFE Efforts - HFE requirements are included in each subcontract and the subcontractor's compliance with HFE requirements are periodically verified in accordance with GEEN QA.

## 3.3 ESBWR M-MIS Design Bases and Goals

### 3.3.1 Design Bases

These design bases are adopted for the ESBWR M-MIS:

1. The proven M-MIS design of the reference ABWR plants will serve as a design basis for the ESBWR M-MIS implemented under this plan. It is recognized that different operational needs, human factors considerations, and industry standards, codes, and regulations exist between the reference plants and the ESBWR M-MIS implemented under this plan. An analysis of the design differences between the ABWR and ESBWR design will establish a Baseline Review Record.(BRR). Potential differences may lead to changes in M-MIS design, and these changes will be analyzed against the current ESBWR plans. Therefore, M-MIS design changes will be the result of ABWR-ESBWR plant differences and new requirements identified in the ESBWR specific plans.

2. From the ESBWR DCD, the preliminary staffing assumption will consist of the following assignments:

| Quantity | Qualification | Assignment |
|---|---|---|
| 1 | Senior Reactor | Provides overall supervision of control room operations |
| 2 | Reactor Operators | One is assigned to normal control actions at MCC. Second operator is assigned to maintenance activities, |

| | | |
|---|---|---|
| | | including blocking and tagging permits. |
| 1 | Senior Reactor Operator | Assigned to shift but not necessarily in the Main Control Room (MCR). Act as relief for shift SRO. |
| 1 | Reactor Operator | Assigned to shift, but not in the MCR. On call to be in MCR within 5 min. |
| 2 | Maintenance Technicians | Qualified to operate equipment in the plant. Assigned to shift qualified to provide engineering support as a shift technical adviser |
| 1 | Administration Clerk | |

3. The operator will remain in control of plant operation. The operator will be able to assume manual control of those functions that have been automated for reasons other than regulatory requirements. The operating crew's training will include manual operation an automated function that has been returned to manual monitoring and control.

4. The M-MIS will utilize only proven technology. The bases for considering M-MIS proven are defined in Section 3.5.1.

5. Safety related systems monitoring displays and control capability will be provided in full compliance with regulations regarding electrical separation and independence;

6. The M-MIS design will be highly reliable and provide functional redundancy such that sufficient display and control will be available in the main control room and remote locations to conduct an orderly reactor shutdown and to cool the reactor to cold shutdown conditions, even during the postulated ESBWR design basis equipment failures defined in the ESBWR PSAR. In addition, mean time between forced outages caused by failures of M-MIS equipment will be greater than fifty reactor-operating years. In addition, the mean time between M-MIS equipment failures which result in a reduction in plant availability will be greater than five years over the entire design life of M-MIS equipment;

7. The principal functions of the Safety Parameter Display System (SPDS) as required by Supplement 1 of NUREG-0737 will be integrated into the M-MIS and HSI design; and

8. Accepted HFE principles as applied to the needs of the ESBWR plant operators will be utilized for the M-MIS and HSI design.

### 3.3.2 Design Goals

- The design goal for the M-MIS and HSI is to facilitate safe, efficient, and reliable operator performance during all phases of normal plant operation, abnormal events, and emergency conditions. To achieve this goal, information, displays, controls, and other interface devices in the control room and other plant areas are designed and implemented in a manner consistent with good HFE practices. An integral part of the M-MIS is the HFE Program Plan.

## 3.4 Control Room Standard Design Features

As part of the ABWR design development leading to design certification and the start of construction of the reference plants, a variety of tests, studies, and evaluations were performed in a number of areas of control room equipment design. The results from these studies and evaluation form the basis for the ESBWR control room standard design features. During the performance of M-MIS and Human Factors V&V activities, the standard design features of the ESBWR control room will be evaluated further. The results of these evaluations will be reviewed and design changes will be made in accordance with the document control and quality assurance program for the ESBWR Nuclear Units. The evaluations shall be performed using scenarios and plant operating procedures modified for ESBWR. The scenarios will include all normal, abnormal, and emergency scenarios as required by the ESBWR DCD.

These eighteen standard design features of the ESBWR control room are summarized as follows:

1. A single integrated control console staffed by two operators from a seated position;

2. The use of video display units (VDU's) driven by a distributed control and information system (DCIS) for safety system monitoring and non-safety control and monitoring;

3. The use of divisionally separated, Class 1E qualified VDU's independent from the NE-DCIS for safety system control and monitoring;

4. Limited use of dedicated function switches on the control console. The dedicated function switches are used to support such functions as initiation of automated sequences or safety system operations, manual scram, reactor operating mode changes and turbine trip;

5. Operator selectable automation of pre-defined sequences;

6. The incorporation of operator selectable semi-automated mode of plant operations;

7. The capability to conduct pre-defined operations sequences in manual mode;

8. The incorporation of a wide display panel to provide the operators with a plant-overview;

9. The inclusion on the wide display panel of dedicated displays of key plant parameters and major equipment status;

10. The inclusion in the dedicated displays of both 1E-qualified and non 1E-qualified display elements;

11. The independence of the safety related dedicated displays from the NE-DCIS Computer System;

12. The inclusion within the wide display panel of a large video unit(s) driven by the NE-DCIS Computer System;

13. The incorporation of a "monitoring only" supervisors console;

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 dedicated displays located on the WDP;

15. The use of dedicated alarm tiles on the wide display panel;

16. The application of alarm prioritization and filtering logic;

17. A spatial arrangement which allows viewing of information on the wide display panel while seated at other consoles; and

18. The use of VDU's to provide alarm information in addition to the dedicated alarm tiles.

All detailed M-MIS design features of the MCR panels (MCRP), RSS, LCS and electronic display formats will conform to these standard control room design features which form the basis for the ESBWR MCR design certification.

The Main Control Room Panels (MCRP) system will describe the implementation of these standard control room design features (COL Applicant).

### 3.4.1 Use of Standard Plant Detailed Design Information

The ESBWR design will utilize the design of the ABWR reference plants and the US standard plant design. Deviations from the reference M-MIS design will be made to accommodate:

1. Regulatory requirement updates since the HFE development of ABWR reference plants;
2. Design changes identified in the BRR;
3. The results of the ESBWR specific HFE analysis; and
4. Selection of HSI Distributed Control and Information System (DCIS) equipment vendors.

### 3.4.2 Standardization of Components

In order to minimize the impact of obsolescence of M-MIS equipment throughout plant life, the M-MIS design will be modular in construction (both hardware and software) and will standardize M-MIS equipment. ESBWR will establish plans early in the project to identify what potential hardware such as VDUs, may impact the design of the MCRP over the life of the plant. ESBWR Program Plans and the Software Management Plan (SMP) will address standardization goals and requirements. Extensive use of HFE-established style guides and display primitives are incorporated.

### 3.4.3 Control System Data Gathering, Transmission, and Processing

The ESBWR plant multiplexing system Distributed Control and Information System (E-DCIS and NE-DCIS) will:

1. Minimize the plant wiring;
2. Consider the vulnerability of the M-MIS to a single component failure, which can affect more than one system or function. Single component failures and common mode failures will be analyzed in accordance with the Plans identified in section 4.2.

3. Support the plant maintenance and test requirements; and

4. Minimize the disruption to the plant database when a component, equipment, subsystem, or system failure occurs. The methodology for handling of the plant databases will be established through the SMP.

The ESBWR plant DCIS will have attributes defined which will allow each system designer to:

1. Identify the accuracy, resolution, and data rate needed to support the intended uses of each signal. Each characteristic of a signal will meet the most restrictive requirement among the systems or functions that use the signal;

2. Identify cases where the signal characteristics required for special applications (e.g., such as startup testing) require the selection of a sensor or other device with performance characteristics more restrictive than the performance characteristics applied during normal process control or monitoring. Separate special purpose sensors will be provided if the high performance requirements result in the selection of a device with lower reliability, higher drift, higher sensitivity to its environments, etc.; and

3. Determine the method of transmission of a specific signal, extent of segmentation and/or redundancy, extent of distribution of a signal, and acceptable transmission path loading. This information will be contained in the Software Management Plan.

#### 3.4.3.1 Design Flexibility

The M-MIS design will provide flexibility to accommodate design changes and the ability to replace equipment due to aging, wear, or obsolescence. The M-MIS design will include design features such as:

1. A modular design (both functionally and physically) to accommodate replacements, upgrades, and functional expansions gracefully and in a cost-effective manner; and

2. Spare capacity in instrument panels, I/O capacity, storage capacity, processing capacity, alarm and display systems, data communication (throughput loading), power supply, HVAC, etc.

#### 3.4.3.2 Data Transmission

All data on the plant-wide data buses will have signal identification information associated with them. When a signal is to be used for post event analysis where

precise timing is required, time tagging will be attached to the signal. All data will have a signal quality tag associated with it. The quality tag will contain sufficient information to support troubleshooting.

The data transmission process will provide sufficient inherent integrity and error checking to assure that random errors in the process will not degrade the availability and reliability of the systems and functions that utilize the data.

The DCIS documentation will describe the use of standard protocols and interfaces, methods of signal tagging, the data transmission process and process for data time tagging.

#### 3.4.3.3 Signal Filtering

Each data acquisition channel will be capable of filtering of the sensor output to reduce noise to acceptable levels. Filters will also reduce signal noise aliased into the pass band to acceptable levels.

#### 3.4.3.4 Signal Processing

All signal processing such as scaling, linearization, rate of change calculation, etc., will assure that:

1. The accuracy, resolution, precision, and rate of response of the results of the processing are consistent with those of the signal being processed and the applications of the signal;
2. Coefficients or other constants used in signal processing will retain their values through power interruptions and processor down time; and
3. Signal rate of change will be determined in a manner which is not unduly influenced by random noise;
4. The DCIS requirements document will describe the methods for signal processing to meet the above requirements

#### 3.4.3.5 Data Propagation Times

The propagation time for multiplexed data will be analyzed to demonstrate the prevention of significant degradation in performance of plant control and monitoring systems. The propagation time will include response degradation due to filters, the sampling rate of the signal, A/D conversion time, signal processing time, resampling rates, data transmission time, and D/A conversion times. The system design will provide operator acknowledgment of a requested action within 0.25 seconds of the

operator request. Propagation times will be modeled as a part of the DCIS safety analysis plan.

#### 3.4.3.6 Performance Margins

The DCIS documentation will demonstrate sufficient performance margin to perform its designed function under conditions of maximum stress. Conditions of maximum stress will be based on plant events that cause the highest data acquisition, data processing, and data transmission loading. The DCIS will be designed with at least 25% expansion capability. Verification of these performance margins will be demonstrated under the analyses.

#### 3.4.3.7 Reliability Models

When redundant data paths and signal selection are used, the reliability model of the data path will include consideration of the failure rate and coverage provided by the selection device or algorithm. The failure rate of the selector may be a significant contributor to overall data path reliability. The detailed reliability models will be prepared in accordance with the DCIS safety analysis plan.

#### 3.4.3.8 Use of Industry Standards

Plant-wide data highway protocols and interfaces to controllers, sensors, actuators, etc., will be based upon industry standards. Localized proprietary data highways may be used only if a clear benefit can be derived from their use; however, their interface to the plant-wide data highway will be a standard interface. Nuclear industry standards for network security will be incorporated.

## 3.5 Use of Proven Technology

Due to the advantages that currently available modern technology offers over some of the technology found at operating BWRs, the incorporation of modern technology will be used wherever possible to improve existing designs.

### 3.5.1 Criteria for Proven Technology

The proposed instrumentation, control and M-MIS systems must utilize successfully proven up-to-date technology and must be available for installation as scheduled in the COL Applicant activities. For Q-class or safety related systems, proven systems, equipment, subsystems, components, design and services are those which have been evidenced by at least one (1) year of successful operation record in existing light water reactors. For non-Q class or non-safety related systems, they are considered "proven" if they have been evidenced by at least one (1) year of successful operation record in existing light water reactors, fossil plants, or industry process plants, prior to the start up date.

### 3.5.2 Criteria for Unproven Technology

For any M-MIS component (hardware or software), which does not meet one of the proven criteria in Section 3.5.1, all of the following criteria for unproven technology will be met:

GE may make use of up-to-date modern technology and design, and understands that some designs, subsystems, systems, equipment or components proposed may not have received the required one (1) year satisfactory service prior to the start up date. For these designs, systems, and subsystems, equipment or components, if proposed, GE may develop a methodology to receive equivalent experience Such an approach will be evaluated and considered acceptable if:

1. A defined program of prototype testing which has been designed to verify their performance in the project M-MIS application, has been completed, and a detailed plan has been developed for the collection of one (1) year operation experience; and

2. Specific proven designs, systems, subsystems, equipment or components, which have been evidenced by at least one (1) year of successful operation experience startup and which can meet the basic functional requirements are considered; and

3. The needed experience data collection can be completed and assessed prior to the issuance of a Construction Permit and the determination can be made prior to the issuance of the Construction Permit as to whether the base approach (up-to-date modern technology and design) is acceptable or the back up approach must be utilized, without either of these two approaches impacting the overall project schedule.

## 3.6 Review of Operating Experience

Review of experience and identification of problems in prior M-MIS implementations, including human factors problems, will be addressed throughout the design process. In addition, the ESWBR DCD requires that a review of the industry experience with the operation of those selected M-MIS equipment technologies will be conducted for those designs, which are similar to the proposed design. The review of those M-MIS technologies will include both a review of literature pertaining to the human factors issues related to similar system applications of those technologies and interviews with personnel experienced with the operation of those systems. Any relevant HFE issues/concerns associated with the selected M-MIS equipment technologies will be entered into the HFE Issue Tracking System (HFEITS) (See Section 4.2).

Lessons learned from a review of previous nuclear plant M-MIS designs, as defined by Attachment 1 to DCD Chapter 18 Table 18E-1, will be entered into the HFEITS to assure that problems observed in previous designs will be adequately addressed in the ESBWR design implementation. Also, recognized industry HFE issues such as those documented in NUREG/CR-4600 will be addressed. .

Reviews of operating experience will be conducted for the following M-MIS and HSI design areas. The review areas will include plant operations and HFE design topics. Plant operations address normal plant evolutions, instrument failures, HSI equipment and process failures, transient, accidents and reactor shutdown periods and cooldown using a remote shutdown system. HFE Design Topics include decisions about selection of alarm and annunciation elements, displays, control and automation elements, information processing and job aids, real-time communications with plant personnel and other organizations, procedures, training, staffing/qualifications, and job design. For example, new elements of the HSI design, in which further development of the industry is expected include:

1. Use of flat panel display panels and VDU displays;
2. Use of CRTs in selected applications
3. Use of electronic on-screen controls;
4. Use of wide display panels;
5. Use of prioritized alarm systems;
6. Automation of process systems;
7. Operator workstation design integration; and
8. Any other areas where clear industry developments have been made which may address M-MIS and HFE areas.

These operating experience reviews will include review of:

- Recognized Industry HFE Issues (e.g., NUREG/CR-4600)
- Reports provided by industry organizations such as EPRI;
- Review of applicable research in these design areas;
- Proceedings published by HFE professional societies;
- Review of applicable research and experience reports published by M-MIS equipment vendors; and

- Review with actual users or industries (e.g., non nuclear power generation, process industries, aerospace, DOD, etc.) of the above six technologies.

The results of these review activities will be entered into the HFE Issue Tracking System to assure that the ESBWR implementation reflects the experience gained by the resolution of design problems in operating plants.

Events in the tracking system will be compared with the PRA/HRA for Risk-Important Human Actions that have been identified as different or where errors have occurred. Such human actions will explicitly evaluated during the design process to assess their human error probability and evaluate the impact of the HSI, and other plant features in lowering the error potential. A human action evaluation report that addresses the issue, problems, and sources of human error, and the design elements that enhance human performance will be provided for these special actions.

The M-MIS implementation process will establish quantitative reliability and availability criteria for each component part of the M-MIS within the DCIS documentation. Availability and reliability analyses and models will be prepared. The individual reliability and availability criteria will be sufficient to support an overall M-MIS availability number which meets or exceeds the requirement that mean time between forced outages caused by failures of M-MIS equipment will be greater than fifty reactor operating years over the design life of the equipment. In addition, the overall M-MIS availability will be such that the mean time between M-MIS equipment failures, which result in a reduction in plant availability, will be greater than five years over the entire design life of M-MIS equipment.

The M-MIS will also be designed so that failures or problems in one function or device will not propagate into failures of other functions or devices. The M-MIS will be designed to prevent any single random failure of M-MIS functions or devices from causing a forced outage, challenging a safety system, spuriously actuating a safety system, or causing a condition which results in the need to declare one of the plant emergency classes.

The M-MIS control and monitoring systems will be designed to protect against failures of M-MIS equipment degrading the performance of more than one major control or monitoring function. The functional and physical designs of these systems will be segmented to inhibit the propagation of failures across major functions.

An evaluation of the vulnerability of the M-MIS to common mode failures will be performed during the preparation of the DCIS documentation. After the detailed multiplexing system model is put in place, the M-MIS implementation process will explicitly consider the potential for common mode failures and their effects in

determining the architecture of the M-MIS. This process will explicitly identify failures that were considered, make a qualitative assessment of the susceptibility to each failure, and identify design measures taken to protect against these failures.

A preliminary evaluation of the reliability of the M-MIS will be performed during preparation of the DCIS. After vendor selections have been made, a detailed reliability evaluation will also be performed to provide assurance that the final system design, including all modules, performs in accordance with system requirements.

A report documenting the analysis of operating experience in the tracking system, which identifies the human performance issues, problems and sources of human error, will describe the design elements that support and enhance human performance.

## 3.7 Human Interface to Plant Conditions

### 3.7.1 Electronic Displays

An objective of the HSI design is to minimize the number of different types of displays that are used to present information and/or controls to the operators. Differences in display type and format will be related to differences in use of the information by the operators.

Position or status indications provided to the operator will be the actual component status or position where possible. The information, controls or and alarms displayed to the user will be based upon the HFE program studies. The information and controls with use plant and system state to present the correct state of a component. Using color and shape coding the displays will provide the operator with the correct valve line-up and component states. A demand indication will be used only if it provides the operator with needed information.

The design of the ESBWR electronic user interface displays will be specified and described in the NE-DCIS Hardware/Software Specification. The user interface displays shall be consistent with the requirements of NUREG-0700 [2.3(1)]. The details of the displays will be defined in a DCIS Style Guide.

### 3.7.2 Testability

The M-MIS implementation process will define the test requirements in formal test plans. These tests will be written for various test stages which exist in the M-MIS design and implementation process. These plans will, when considered as a whole, include the testing necessary to demonstrate the adequacy of the human factors of the HSI design. All testing required to validate the M-MIS design, prepare the systems for operation, and surveillance tests required after the systems are in service will be

included in the plans. Each test plan will be developed under the SQAP and Software V&V Plan, see Appendix B:

1. Identify the items to be tested, including their version or revision where appropriate;
2. Identify all features of the system under test which are not to be tested, and the reasons why;
3. Describe the overall test approach;
4. Specify relevant test case specifications;
5. Specify the acceptance criteria for pass/fail decision for each test and requirements for dispositioning and retesting failed steps;
6. Specify the test environment and test equipment;
7. Identify group responsibilities for performing the test;
8. Identify the test staffing needs and associated skill levels; and
9. Specify a test sequence and provide an estimate of the time to carry out the tests.

M-MIS equipment will be designed and configured to readily support in-service testing by use of built-in test features, including on line self-diagnostics and automated functional testing for periodic surveillance tests.

### 3.7.3 Maintainability

Although the M-MIS design must facilitate cost-effective testing and maintenance, the M-MIS design will also take into account, from the outset, full recognition of the need for maintenance and testing and inspections on the installed M-MIS equipment throughout its lifecycle. In addition, the ESBWR design will utilize the M-MIS functions as maintenance aids to optimize the operating and maintenance costs of the other power plant systems.

The M-MIS will be designed for maintenance in accordance with human factors engineering principles, References 2.3.1 and 2.3.41.

The M-MIS will be designed to simplify, and reduce the amount and difficulty of, the maintenance and testing required over the plant lifetime. Repair and replacement of

M-MIS equipment will normally be accomplished by modular replacement in the field and must be considered in the design of the components.

The M-MIS shall be designed for maintenance in accordance with good human factors engineering principles. EPRI NP-4350, Human Engineering Design Guidelines for Maintainability in Section 2.3.17, shall be utilized to assist in placing proper emphasis on human factors. The M-MIS maintenance will consider access of the components, physical location either within a panel or on a panel, and indication to the operator that the equipment is under repair.

Labeling and coding of components inside and outside of cabinets shall be unambiguous, readable and consistent with other plant labeling practices in Section 2.3.18.

The HFE Program will ensure that the maintainability requirements, including the preparation of Instruction and Maintenance Manuals prepared by GE and its suppliers are met. The maintainability group with the assistance of the HFE group will perform evaluations of the HSI designs for maintainability, including the format and content of the instruction and maintenance manuals. A software maintenance plan, which complies with IEEE Std. 828 and IEEE Std. 1042, will be established for M-MIS software. This software maintenance plan will be a revision of the currently utilized Software Management Plan for GE Plant Monitoring and Control products, revised to reflect all requirements of the ESBWR DCD and program specific plans.

### 3.7.4 Constructability

The M-MIS design will incorporate features that reduce the time and effort to fabricate and install the M-MIS equipment. The components of the M-MIS design will be designed to allow installation and functional checkout of each module separately, prior to complete system integration. Cabinets and panels will be fabricated, internally wired, and functionally tested before plant installation. The M-MIS design will contribute significantly to reducing field wiring.

### 3.7.5 Alarms

The ESBWR alarm system design will be documented as a subsection to the NE-DCIS Hardware/Software specification. The ESBWR alarm system will be designed to:

1. Alert operators to off-normal conditions which require them to take action;
2. Guide the operators, to the extent possible, to the appropriate response;

3. Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions; and

4. Minimize distraction and unnecessary workload placed on the operators by the alarm systems.

The alarm system will provide the capability for the operators to periodically confirm that it is functioning properly. Any portions of the alarm system that are not continuously checked through built-in test features will be checked through periodic functional testing by the operators.

The effectiveness of the alarm system will be verified through real-time, dynamic simulation. Simulator evaluations will include specific evaluations of the important alarm system design features, adequacy of the alarms chosen, effectiveness of audible and visual displays, and interactions between the operator and the alarm system.

#### 3.7.5.1 Selection of Alarm Conditions

A consistent approach and philosophy will be used in selecting plant conditions to be alarmed. The criteria used in selecting alarm conditions will include the following:

1. For each alarm there is a defined action the operator is to take in response;

2. The alarm conditions will be chosen based on a "dark board" concept - no alarms should be present when the plant is operating normally in any plant operating mode (STARTUP, RUN, SHUTDOWN, REFUEL), with all systems in their normal configuration for that mode of operation;

3. Each alarm set point will be chosen such that the operator will be alerted early enough that there is time to take the appropriate action, but the set point is not so close to the normal operating range as to produce unnecessary or nuisance alarms;

4. Alarms will provide alerts before a major system or component problem results in a condition which causes a loss of availability; and

5. Alarms for process deviations will be based, where possible, on validated process signals rather than individual sensor indications.

The alarm system will be designed to minimize the potential for nuisance alarms. To support elimination of potential nuisance alarms, the alarm system will incorporate:

- Capability to apply time filtering and/or time delay to the alarm inputs to allow filtering of noise or eliminate unneeded momentary alarms; and

- Capability to apply logic to alarm inputs, combining an input alarm condition with other alarms, signals, calculated conditions, and plant mode indications with flexible logic.

#### 3.7.5.2 Nuisance Alarming

Each individual alarm will be evaluated to examine its potential for nuisance alarming. The evaluation will consider:

1. All modes of operation of the plant and the associated system;
2. Maintenance of the associated system or component (e.g., the potential for many alarms to come in due to a component being shutdown for extensive maintenance);
3. Possible momentary alarm occurrences due to equipment startup;
4. System dynamic response to plant transients or upsets which induce temporary physical disturbances capable of setting off the alarm but which are not indicative of an actual alarm condition;
5. Potential sources of noise in the alarm input;
6. Unusual, but plausible, lineups for the associated system or component; and
7. Other conditions that might lead to the unnecessary occurrences of the alarm.

Alarms that are formed from the combination of more than one input condition through "OR" logic will have reflash capability. The need to implement reflash capability for multiple-input alarms will be evaluated on a case-by-case basis.

The alarm system will be designed to minimize the number of alarms that occur in plant upsets and emergencies while providing the operators with the information needed to formulate correct responses. The number and rate of occurrence of alarms will be reduced by use of filtering, conditioning logic, and prioritization logic.

The alarm system will include features or capabilities that are appropriate for dealing with alarms that are out of service, including spatially dedicated alarms on the wide display panel.

Presentation of alarms will be based upon the guidelines established in the HSI Design Implementation Plan (section 4.8)Alarms will be presented in a prioritized manner on the main control room VDU's. Priorities will be based upon relative importance and time urgency within which the operator will respond. Priorities will

be plant mode dependent; a particular alarm can change priority as the plant mode changes.

For each alarm condition, an alarm response procedure will be prepared, defining the required operator action and giving other information needed to ensure an adequate response. These alarm response procedures will be made available via hard copies and electronically (on the VDUs).

The alarm list on the VDU will be designed with the intention to display all of the plant highest priority alarms, in all credible scenarios, without display paging.

The alarm system will be capable of driving multiple audible tones or signals to annunciate alarm conditions. The types and volumes of audible tones will be chosen such that:

- The operator is alerted to the presence of the alarm condition;
- The operator can, from the specific tone or direction of sound, determine where the alarm originated (functional area of the plant, or station);
- The amount of distraction due to audible alarm signals is minimized through choice of alarms and provision for silencing audible alarms; and
- The tones used for incoming alarms are separate and distinct from tones used to signify "return to normal" alarms, and that return to normal alarms are momentary ("self-silencing").

The alarm subsystem will tag each alarm with the time of its occurrence, resolved to a maximum of 2.0 seconds. Alarms designated as sequence-of-events points will be resolved to a maximum of 4 milliseconds, except in cases where it can be demonstrated that a coarser time resolution is adequate. The operator will have capability to access at any time, via a VDU display or printed hard copy, the time sequences of alarms. The time sequence of alarms will be included as part of the permanent records of plant operation.

# 4 Human Factors Engineering Process

## 4.1 General Requirements

In application of the newer technologies to be used in the ESBWR Project, the design process provides for thorough evaluation of the design using an iterative design approach. The initial basis for the design rests in the commitments of the DCD, ABWR Reference plant data, and operating experience, results of prior research studies, and other applicable industry standards and regulatory guidelines. As the design proceeds, it will be tested at successive stages using mockups, prototypes, and simulations, and data collected to support the design decisions and specific features. Finally, the integrated design will be evaluated using full-scope simulation. The iterative testing and evaluation will specifically include the human in the loop, including operators in walkthroughs at mockups, and partial or prototype simulations on workstations and full-scope simulators. The performance criteria will be chosen based on the specific evaluations to be made, and will include such measures as error reduction, response time, and mental workload.

With respect to reducing human error potential, an HSI design plan will be developed and will emphasize:

1. Elimination of potential sources of human error - eliminating potential sources of error based on the current state of the art in human factors and behavioral science and on review of experience with existing designs, application of function and task analysis in the design, and use of mockups and simulation in verifying and validating the design;

2. Reduction in the probability of human error through careful selection and allocation of tasks, proper support of defined tasks through detailed evaluation of information and control needs, and enforcement of consistency and integration along the task analyses, the hardware and software implementation of the design, the operating procedures, the Main Control Room environment, and personnel training requirements. Reduction of human error potential will be a priority consideration in the design; and

3. Provision for detection and recovery from human errors once they occur, using data processing and display technology that automates checks and alerts to detect errors before they affect the plant. These checks and alerts will provide sufficient descriptive information to help recover from human errors that do occur.

4. Standardization and consistency in the application of HFE principles. The use of style guides, display primitives and signal processing conventions will be developed under the SMP with HFE principles and captured in HSI Implementation Plan as design input to the DCIS development. The HFE V&V and the Software V&V will assure the implementation of the conventions.

The HSI design, an activity of M-MIS development, will include the following activities:

- Allocation of functions between automatic and manual control;
- Allocation of tasks among work stations;
- Development of control and operation strategies;
- Assignment of responsibilities of the operating staff;
- Inclusion of risk important Human Actions identified in the HRA
- Assessment of operator workload, both mental and physical;
- Arrangement of work stations;
- Constraints imposed by DCIS vendor limitations;
- Selections of types of displays and their detailed characteristics;
- Selection and arrangement of alarms and their integration into the control station designs;
- Development of operating procedures and training requirements;
- Utilize data from HRA to present information, controls, or alarms that allow the operators to respond and/or perform critical tasks;
- Evaluation of the effects of credible M-MIS equipment failures; and
- Human Factors Verification and Validation (V&V) reviews.

The Functional requirements and task analysis shall be performed for the systems that the operators must monitor and control. These analyses will be performed in accordance with the requirements of the Systems Functional Requirements Analysis Implementation Plan, in Section 2.1.4, and the Task Analysis Implementation Plan, in Section 2.1.6. The purpose of these plans is to analyze operator-plant system interaction, in response to normal (startup, shutdown, and power range maneuvering), abnormal, and emergency plant, using the allocated monitoring, control, and alarm functions. These analyses will consider operator action in the main control room, remote shutdown system panel, and at local control stations as appropriate.

## 4.2 HFE Issue Tracking System

The HFE Issue Tracking System (HFEITS) will assure that HFE issues/concern and HSI that are identified throughout the development and evaluations of the M-MIS implementation are addressed. The CRDT will prepare an administrative procedure which:

1. Identifies each unique HFE issue/concern and enters each item in a log with a unique tracking number;

2. Identifies an administrative position responsible for maintaining the tracking system and tracking logs;

3. Identifies the methodology for the evaluation and documentation of the proposed solutions, implemented solutions, evaluated residual effects of the implemented solution and the evaluated criticality and likelihood of the implemented resolution of the HFE issue/concern. This methodology will follow the methodology described in NUREG-0801, "Evaluation Criteria for Detailed Control Room Design Review", and apply the content and process discussed in section 3.4;

4. Identifies individual CRDT member responsibilities for HFE issue identification, issue resolution, and issue closeout; and

5. Provides the format of the reports from the HFEITS than can be used by the Design Team and also provided to the COL for review.

Appendix A of this plan describes the detailed implementation methodology to be used for the HFEITS.

## 4.3 System Functional Requirements Analysis Implementation

Functional requirements analysis will be developed to identify functions that must be performed to satisfy plant safety objectives; that is, to prevent or mitigate the consequences of postulated accidents that could damage the plant or cause undue risk to the health and safety of the public. A functional requirements analysis is conducted to (1) determine the objectives, performance requirements, and constraints of the design, (2) define the high-level functions that have to be accomplished to meet the objectives and desired performance, (3) define the relationships between high-level functions and plant systems (e.g., plant configurations or success paths) responsible for performing the function, and (4) provide a framework for understanding the role of controllers (whether personnel or system) for controlling the plant.

The System Functional Requirements Analysis will utilize, as an input, the M-MIS functions for the ESBWR as defined in DCD and ABWR reference results summary reports and supporting documentation. The output of this analysis will be consistent with the above references.

The functional requirements analysis will use ABWR reference design documentation as the technical basis for identifying changed functions in the ESBWR design. Summary description of plant processes and detailed narrative descriptions of changed functions will form the detailed scope of SFRA and subsequent HFE activities. The System Functional Requirements Analysis Implementation Plan will establish:

1. Methods and criteria for conducting the System Functional Requirements Analysis in accordance with accepted human factors principles and practices;

2. That system requirements will define the system functions and those system functions will provide the basis for determining the associated HSI performance requirements;

3. That functions critical to safety will be identified using HRA techniques as well as deterministic evaluations; and

4. Descriptions will be developed for each of the identified functions and for overall system configuration design. A description of the functions and systems should be provided along with a comparison to the reference plants/systems, i.e., the previous plants or plant systems on which the new system is based. This description should identify differences that exist between the proposed and reference plants/systems. Safety functions (e.g., reactivity control) include functions needed to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant system configurations or success paths that are responsible for or capable of carrying out the function should be clearly defined. Function decomposition should start at "top-level" functions where a very general picture of major functions is described, and continue to lower levels until a specific critical end-item requirement emerges (e.g., a piece of equipment, software, or HA). The functional decomposition should address the following levels

   - high-level functions [e.g., maintain reactor coolant system (RCS) integrity] and critical safety functions (e.g., maintain RCS pressure control)
   - specific plant systems and components

5. Each function will be identified and described in terms of inputs (observable parameters which will indicate system status), functional processing (control process and performance measures required to achieve the function), functional operations (including detecting signals, measuring information, comparing one measurement with another, processing information, and acting upon decisions to produce a desired condition or result such as a system or component operation actuation or trip), outputs, feedback (how to determine correct discharge of function), and interface requirements so that subfunctions are related to larger functional elements. Interim and Results Summary of this analysis is input to Allocation of Functions and as recorded in the HFE ITS for iteration through systems engineering process. Refer to Figure 4.3, the SFRA plan will be submitted to the NRC. The Results Summary Report will be confirmed in the DAC analysis. *See also Appendix B for a draft outline of this plan.*

## 4.4 Allocation of Function Implementation

Function allocation is based on analysis of the requirements for plant control and the assignment of control functions to (1) personnel (e.g., manual control), (2) system elements (e.g., automatic control and passive, self-controlling phenomena), and (3) combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup). Plant safety and reliability are enhanced by exploiting the strengths of personnel and system elements, including improvements that can be achieved through the assignment of control to these elements with overlapping and redundant responsibilities. In addition to technological and economic considerations, function allocation will be based on HFE principles using a structured and well-documented methodology that seeks to provide personnel with logical, coherent, and meaningful tasks.

A procedure for an allocation process will be developed and applied by the HFE team according the ESBWR project plan. The process will include identification of the functions to be performed drawing on previous BWR designs and differences in the ESBWR design. The process will link the high level and critical safety function with its purpose, conditions for activation, parameters that indicate the function is available, operating, achieving its purpose, and when it should be terminated. This allocation analysis process will be documented for reviews, verification and updating.

The Allocation of Function activity in the HSI design activity is intended to evaluate each monitoring, control, and protection function as part of the design activity and determine the appropriate level of automation for each with due consideration of operator workload, including potential failures of automatic equipment. This evaluation is to include considerations of system response requirements, complexity of operation, operator burden, and level and duration of attention required. When

selecting the level of automation, the evaluation will address the need to maintain the operators in the loop, cognizant of the plant status so that the operators remain alert and vigilant and can intervene in plant operations as required. The evaluation will also recognize that the operator role changes from one of direct operation to one of management or supervision as the level of automation increases and that this, in turn, changes the type and level of plant data which will be provided to the operators. The effect of failures of automatic control systems will be addressed as part of the process of selecting automated or manual controls. Where manual controls are required, the allocation of functions will establish where soft (VDU-based) controls are appropriate, where hard switches are appropriate, and where both are appropriate .

Decisions on the use of automatic versus manual control or monitoring will be based upon evaluations, which specifically include consideration of:

- Performance demands such as:
  - Operator workload (including parallel or potentially concurrent emergency activities);
  - Operator capability, including time to respond, skill, and precision;
  - Operator vigilance and the need to keep the operator involved and knowledgeable as to the plant status;
- Past operating experience with automatic or manual controls or monitoring in similar applications as determined by the OER plan interim summary and results;
- Technical feasibility, amount and complexity of the M-MIS hardware and software, and the resulting maintenance or testing burden;
- The consequences of and potential for malfunctions of the automatic equipment and for operating errors; and
- Regulatory requirements.

Decisions on the use of remote versus local control and monitoring will be based upon evaluations, which include consideration of:

- Operator workload, including the effect of the time to access local equipment and the other parallel or potentially concurrent operator tasks;
- Operator capability, including the need for feedback or monitoring as a control action is taken;
- The local environmental conditions, such as access difficulty, temperature, radiation and contamination level, leaks, and other personnel hazards;

- The amount and complexity of M-MIS and plant system equipment and the resulting maintenance and testing burden;
- The consequences of malfunctions of remote equipment; and
- Past experience with remote or local controls in similar applications.
- The Allocation of Functions Implementation Plan, in Section 2.1.5, will establish:
- That all changed functions identified in the System Functional Requirements Analysis have been properly considered for functional allocation, through use of a Function/Functional Allocation cross-reference matrix or equivalent means;
- OER and SFRA interim and final results summary reports and supporting documentation;
- The methods and criteria for the execution of function allocation in accordance with accepted human factors practices and principles;
- That aspects of system and functions definition will be analyzed in terms of resulting human performance requirements based upon the user population;
- That the allocation of functions to personnel, system elements, and personnel system combinations will reflect:
  - Sensitivity, precision, time, and safety requirements;
  - Reliability of system performance;
  - The number and the necessary skills of the personnel required to operate the system;
- That the operator's role remains consistent with HFE objectives and ESBWR design basis.
- That allocation criteria, rationale, analyses, and procedures will be documented; and
- That analysis will confirm that the personnel can perform tasks allocated to them while maintaining operator situation awareness, acceptable personnel workload, and personnel vigilance.
- That the technical basis for all function allocations is documented including the allocation criteria, rationale, and analyses method
- That the technical basis for functional allocation can be any one or combination of the evaluation factors, see Fig 4.4. This would establish a basis for automation (assuming acceptability of other factors, such as technical feasibility or cost).

- The allocation of functions activity will confirm that the M-MIS design will not require the operators to perform tasks, which over-burden their capabilities, especially during emergency or upset conditions. The M-MIS simulation facility will be used to confirm compliance with this requirement.

The SFRA interim and results summary reports will include description of the functions and systems will be provided along with a comparison to the reference plants/systems, i.e., the previous plants or plant systems on which ESBWR system is based. This description will identify differences that exist between the proposed and reference plants/systems. Safety functions (e.g., reactivity control) include functions needed to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety function, the set of plant system configurations or success paths that are responsible for or capable of carrying out the function will be defined. Function decomposition will start at "top-level" functions where a very general picture of major functions is described, and continue to lower levels until a specific critical end-item requirement emerges (e.g., apiece of equipment, software, or HA). The functional decomposition will address the following levels:

- High-level functions [e.g., maintain reactor coolant system (RCS) integrity] and critical safety functions (e.g., maintain RCS pressure control)
- Specific plant systems and components

The HSI design will include features that facilitate operator activities that tend to maintain the operators alert and attentive. These features will be based upon available information on methods that have been proven to be effective in assuring operator vigilance.

The functional requirements analysis and function allocation will be verified in accordance with GEEN QA and ESBWR Project Plans:

- All the high-level functions necessary for the achievement of safe operation are identified.
- All requirements of each high-level function are identified.
- The allocations of functions result in a coherent role for plant personnel

Interim and results summary reports will be design input to the task analysis and changes identified to the systems engineering process,see to Fig. 1.2

*See also Appendix B for a draft outline of this plan.*

## 4.5 Task Analysis Implementation

Results of Allocation of the Function Plans form the input to the Task Analysis along with HFE developed risk-important human actions (HA). The functions allocated to plant personnel define their roles and responsibilities. Human actions (HAs) are performed to accomplish these functions. HAs can be further divided into tasks. A task is a group of related activities that have a common objective or goal. Task analysis is the identification of requirements for accomplishing these tasks, i.e., for specifying the requirements for the displays, data processing, controls, and job support aids needed to accomplish tasks. As such, the results of task analysis are identified as inputs in many HFE activities; e.g., it forms the basis for:

- Staffing, qualifications, job design, and training
- HSIs, procedures, and training program design
- Task support verification criteria definition.

The objective of this analysis is to identify the specific tasks that are needed for function accomplishment and related information, control and task-support requirements. Results are captured in the results summary reports and provided to the engineering disciplines to iterate the design as well as perform the HFE V&V activities.

(1) The scope of the task analysis includes:

- selected representative and important tasks from the areas of operations, maintenance, test, inspection, and surveillance;
- full range of plant operating modes, including startup, normal operations, abnormal;
- emergency operations, transient conditions, and low-power and shutdown conditions;
- HAs that have been found to affect plant risk by means of PRA importance.
- ESBWR employs extensive use of automated safety (passive) functions. ESBWR analyses will consider all human tasks including monitoring of the automated system and execution of backup actions if the system fails.

(2) Tasks are linked using operational sequence diagrams.

(3) The task analysis is iterative and became progressively more detailed over the design cycle. It identifies information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls for human task accomplishment.

(4) The task analysis addresses issues such as:

- the number of crew members
- crew member skills
- allocation of monitoring and control tasks to the (a) formation of a meaningful job and
- management of crew member's physical and cognitive workload.

The task analysis results will be used to define a minimum inventory of alarms, displays, and controls necessary to perform crew tasks based on both task and instrumentation and control requirements.

The task analysis results will provide input to the design of HSIs, procedures, and personnel training programs.

The Task Analysis activity will result in the explicit identification of the individual tasks, mental and physical, necessary to support the functions allocated to the plant operator. The plan will provide for interactive analysis and validation of the tasks through techniques such as walk-throughs in control room mockups, dynamic modeling and simulation, and a full-scope plant simulator (post DCD).

The communications requirements of the operators will be included in the task analyses and the needed communications equipment will be integrated into the main control room.

Local control stations will be considered in the task analyses and will be consistent with the integrated design of the M-MIS. The task analysis will be performed in accordance with the Plan and those tasks that may need to be performed at Local Control stations as identified in the analysis. The availability and arrangement of indicators and displays, lighting, access, communications, and special equipment needs of the operator will be considered during the design stage by analysis of the functions and tasks of the station.

The Task Analysis Implementation Plan, see figure 4.7-1, will establish:

1. That all functions allocated to the plant operator in the Allocation of Functions are considered in the task analyses, through use of a Function/Task Analysis cross-reference matrix or similar means;

2. The methods and criteria for conduct of the task analyses in accordance with accepted human factors practices and principles;

3. The scope of the task analyses will include operations performed at the operator interface at the MCR and at the Remote Shutdown System (RSS). The task analyses will be directed to the full range of plant operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, low power and shutdown conditions. The task analysis shall identify the need for information, controls and alarms. The task analyses will also address operator interface operations during periods of maintenance and test of plant systems and equipment, including M-MIS equipment;

4. That the analysis will be used to identify which tasks are critical to safety;

5. That task analysis will develop narrative descriptions of the personnel activities required for successful completion of the task;

6. That task analysis will identify requirements for alarms, displays, data processing, and controls. Where possible and applicable, a single task will be associated with a single VDU display; and

7. That task analysis results will be made available as input to the procedures and personnel training development programs.

Interim and results summary reports will be design input to the HRA analysis and changes from the Reference ABWR identified to the systems engineering process, see Fig. 1.2. Task Analysis results requiring HSI design changes from the Reference ABWR will be iterated as described in the HFE V&V Plan.

*See also Appendix B for a draft outline of this plan.*

## 4.6 Staffing and Qualifications

### 4.6.1 Background

Plant staff and their qualifications are important considerations throughout the design process. Initial staffing level is established based on experience with ABWR Reference plants, staffing goals (such as for staffing reductions), initial analyses, and government regulations. ESBWR staffing and qualifications plans will systematically re-examine the ABWR assumptions and consider staffing reductions warranted by the use of passive safety systems.

### 4.6.2 ESBWR Baseline Staffing Assumptions

From the ESBWR DCD Chapter 18, the preliminary staffing assumption for reactor control and monitoring will consist of the following assignments:

| Quantity | Qualification | Assignment |
|---|---|---|

| | | |
|---|---|---|
| 1 | Senior Reactor | Provides overall supervision of control room operations |
| 2 | Reactor Operators | One is assigned to normal control actions at MCC. Second operator is assigned to maintenance activities, including blocking and tagging permits. |
| 1 | Senior Reactor Operator | Assigned to shift but not necessarily in the Main Control Room (MCR). Act as relief for shift SRO. |
| 1 | Reactor Operator | Assigned to shift, but not in the MCR. On call to be in MCR within 5 min. |
| 2 | Maintenance Technicians | Qualified to operate equipment in the plant. Assigned to shift qualified to provide engineering support as a shift technical adviser |
| 1 | Administration Clerk | |

The licensed operator will remain in control of plant operation during all states of operation. During normal operations the operator will monitor the automated control functions. The operator will be able to assume manual control of those functions that have been automated for reasons other than regulatory requirements. The operating crew's training will include manual operation of an automated function that has been returned to manual monitoring and control.

### 4.6.3 Staffing and Qualifications Plan

The HFE team will develop a staffing analysis plan to perform an iterative HFE process in accordance with Figure A-1 herein. The basis for staffing and qualifications plan will address these issues:

#### 4.6.3.1 Operating Experience Review

- operational problems and strengths that resulted from staffing levels in ABWR Reference systems
- initial staffing goals and their bases including staffing levels of ABWR Reference plants

- systems and a description of significant similarities and differences between ABWR Reference systems and ESBWR systems( See Baseline Review Record)
- staffing considerations described in NRC Information Notice 95-48, "Results of Shift Staffing Study"
- staffing considerations described in NRC Information Notice 97-78, "Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times"

#### 4.6.3.2 Functional Requirements Analysis and Function Allocation

- mismatches between functions allocated to personnel and their qualifications
- changes the roles of personnel due to plant system and HFE modifications

#### 4.6.3.3 Task Analysis

- the knowledge, skills, and abilities needed for personnel tasks addressed by the task analysis
- personnel response time and workload
- personnel communication and coordination, including interactions between them for diagnosis, planning, and control activities, and interactions between personnel for administrative, communications, and reporting activities
- the job requirements that result from the sum of all tasks allocated to each individual both inside and outside the control room
- decreases in the ability of personnel to coordinate their work due to plant and HFE modifications
- availability of personnel considering other activities that may be ongoing and for which operators may take on responsibilities outside the control room (e.g., fire brigade)
- actions identified in 10 CFR 50.47, NUREG-0654, and procedures to meet an initial accident response in key functional areas as identified in the emergency plan
- staffing considerations described by the application of ANSI/ANS 58.8-1994, "Time Response Design Criteria for Safety-Related Operator Actions"

#### 4.6.3.4 Human Reliability Analysis

- the effect of overall staffing levels on plant safety and reliability
- the effect of overall staffing levels and crew coordination for risk-important HAs
- the effect of overall staffing levels and the coordination of personnel on human errors associated with the use of advanced technology

#### 4.6.3.5 HSI Design

- Staffing demands resulting from the locations and use (especially concurrent use) of controls and displays
- coordinated actions between individuals
- decreases the availability or accessibility of information needed by personnel due to plant system and HFE modifications
- the physical configuration of the control room and control consoles
- the availability of plant information from individual workstations and group-view interfaces

#### 4.6.3.6 Procedure Development

- staffing demands resulting from requirements for concurrent use of multiple procedures
- personnel skills, knowledge, abilities, and authority identified in procedures

#### 4.6.3.7 Training Program Development

The training program will address crew coordination concerns that are identified during the development of training

## 4.7 Human Reliability Analysis

Human reliability analysis (HRA) is a required activity of a probabilistic risk assessment (PRA) for both pre- and post-initiator human actions [ASME, 2002].

### 4.7.1 Purpose

This section describes how the HRA information and tools are used to support the HSI HFE design goals. An initial "design level" ESBWR PRA/HRA will be submitted in support of NRC licensing requirements using the ABWR reference HFE design documentation. The HRA will address the impact of human-error mechanisms on the HSI design. . Human error identified and quantified in the PRA will be analyzed to determine if new or modified HSI design features are needed to reduce the likelihood and impact of errors. The HRA activity will quantitatively integrate the HFE program into the PRA and risk analysis. In addition, the results will be design input to the software safety plan activities described in section 5.1.6.

### 4.7.2 HRA Requirements Development

The specific requirements for the HRA implementation plan will be developed by the M-MIS design team following the iterative links with the HFE program shown in Figure 4.7-1, which leads to an "as designed PRA/HRA" at the completion of design. The HRA will be performed iteratively as the design progresses. The PRA and HRA will be performed early in the design process to provide insights and guidance both

for systems design and for HFE purposes. The robustness of the HRA depends, in large part, on the analyst's understanding of personnel tasks, the information related to them, and the factors, which influence human performance.

Accordingly, the HRA will be carried out interactively as the design progresses. At the very least, the initial PRA/HRA phase will be finalized when the plant design and HFE are complete.

The HRA is conducted to screen for important human actions and evaluate their potential for and mechanisms of human errors that impact the frequency of key accident scenarios for the PRA. Thus, HRA is an essential tool for identifying, screening and evaluating specific human actions based on the impact of potential errors on plant safety. The HRA also supports the HFE design goal of minimizing personnel errors, detecting errors when they do occur, and recovering from errors and hardware failures through careful design of the HSI. HRA is expected to provide valuable insight into desirable characteristics of the HSI design as the design evolves. Consequently, the HFE design effort will give special attention to those plant scenarios, risk- important human actions, and HSIs that have been identified by PRA/HRA as being important to plant safety and reliability.

The HRA will interact with the verification and validation program by designing test scenarios and updating quantitative evaluations based on validation results. The HRA models will establish a basis for future human performance monitoring and help prioritize corrective actions.

### 4.7.3 Methodology

The specific methodology and modeling approaches will be established by the design team using information from HRA reports on data, models and methods [e.g. from sources such as NUREG/CR-1278, 1983, EPRI NP-3583, 1984, NUREG/CR-4772, 1987, EPRI NP-6560-L 1990, EPRI TR-100259, 1992, NUREG/CR-6350, 1996, Hollnagel, 1998, Julius, 2001, NUREG-1792, Draft 2004, and NUREG/CR-6883, 2005]. Standards include ASME RA-S-2002, IEEE Std. 1082-1997, and IEEE Draft Std 1574, which is in development.

The HRA inputs will include descriptions and analyses of operator functions and task requirements, previous PRA identified actions and errors, performance factors associated with the operational characteristics of HSI design, procedures for normal, startup, shutdown and emergency operations as well as training programs.

Although there are many different approaches for conducting HRAs, there are several analysis components that increase the quality of the HRA. These include:

- Performing a design specific PRA/HRA to identify significant risk reduction improvements relating to the reliability of core and containment heat removal systems that can be practically implemented during the plant design.

  The PRA will include both internal and external events to the extent possible during the design phase. The main output will be a listing of potentially risk-important human actions from the PRA/HRA.

  Risk important human actions from the PRA/HRA will be used as input to the HFE design effort (i.e., to support function allocation analyses, task analyses, HSI design, procedure development, and training). The design effort will demonstrate how these human actions are well supported by the HSI design and that there is suitable crew availability and time to accomplish the action given that the need is detected.

- Using a multidisciplinary team to analyze human actions within the context of the PRA.

  For some actions the level III requirements in ASME, 2002 may be applied to support quantification of the risk important human actions in dominant accident sequences. The HRA assumptions involving diagnosis, decision-making, and planning and implementation strategies during accident responses may be validated by event simulations using experienced crews, walkthrough analyses using personnel with operational experience to apply procedures for conditions in plant-specific control room mockup or simulator. Such reviews may be conducted to support final quantification of the PRA.

- Obtaining design information related to those factors that affect human performance.

  These include: accident analyses from design basis events, operational experience, and PRAs to define quantification elements such as the time available for action, HSI design details that indicate the cue for an action and the feedback of the effects of taking the action, task analyses to determine the steps, timing and special tools required to carry out the sub steps of the human action, and the applicability of general or specific written procedures.

- Evaluating the effects of HSI advanced technology on human performance and the potential to change the human error mechanisms due to advanced technology. The evaluation of new design features will assess at a minimum the following effects on the existing HRA:
  - The original HRA assumptions and assessed error mechanisms are valid for the modified design
  - The human errors analyzed in the existing HRA are still relevant

- New error mechanisms may become important that were not modeled by the existing HRA/PRA
- The probability of errors by operators and maintenance personnel may change, which may require use of a different modeling construct and
- The consequences of errors, established in the existing HRA, may change.

- Analyzing human actions with an emphasis on human error mechanisms.

  The likelihood of operator error will be minimized for risk-important HAs by identifying key error mechanisms and then providing means for error detection and recovery capability within the HSI design, procedures, and training elements under the HFE program.

- Obtaining appropriate sources of human error data for the types of human actions and associated error mechanisms that are modeled including human to human dependencies and dependencies between human actions and hardware failures.

  Performing sensitivity and uncertainty analyses on the human success and error probability estimates within the PRA sequences to evaluate the impact of human errors on the plant systems.

  These analyses will use a variety of importance measures and HRA sensitivity analyses assumptions to ensure that risk important actions are not overlooked.

- Integrating the PRA and HRA activities into plant design activities by defining safety important actions, supporting HIS design, procedures and training element development to ensure that HRA performance factor assumptions are met in the design.

- Providing a thorough documentation of the HRA process, integration with the HFE elements, methods used, assumptions made and the database for the human error probabilities that feed into the PRA. Such document will support evaluation of future COL applicant changes to the HSI design.

## 4.8 Human-System Interface (HSI) Design Implementation

The HSI design process represents the translation of function and task requirements into HSI characteristics and functions. The HSI will be designed using a structured methodology that will guide 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 HFE guidelines that are tailored to the unique aspects of the ESBWR design, (e.g., a style guide to define the design-specific conventions).

An HSI design methodology will be developed under the SMP and establish standardization and consistency in applying HFE principles. The process and the rationale for the HSI design will be documented and managed under GEEN QA and ESBWR specific Program Plans.

Issues related to the detailed design of specific aspects of the HSIs are resolved during HSI design activities rather than at 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.

### 4.8.1 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 HSIs. These analyses include:

- Operational experience review - Lessons learned from other complex human-machine systems, especially ABWR Reference designs and designs involving similar HSI technology are used as an input to HSI design.
- Functional requirement analysis and function allocation - The HSIs support 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 be 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.

(4) As the design progresses the HFE team may identify other requirements that will become inputs to the HSI design

### 4.8.2 Concept of Operations

The HFE team will develop a concept of operations indicating crew composition and the roles and responsibilities of individual crew 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 will be identified is the allocation of task to the main control room 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 will be displayed to the entire crew.

The concept will address the coordination of crew member activities, such as the interaction with auxiliary operators and coordination of maintenance and operations will be addressed.

### 4.8.3 Functional Requirement Specification

The HFE team will develop functional requirements for the HSIs to address the concept of operations, personnel functions and tasks, and requirements for a safe, comfortable working environment. The requirements will address the various types of HSIs, e.g., alarms, displays, and controls.

### 4.8.4 HSI Concept Design

The HFE team may use several approaches for developing a concept design. 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, and ABWR reference designs. Human performance issues identified from previous operating experience with the 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 will be identified for components of the selected HSI concept design. These requirements will be based on the functional requirement specifications but will be 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.

### 4.8.5 HSI Detailed Design and Integration

(1) Design-specific HFE design guidance (style guides) are developed. HFE Guidelines are utilized in the design of the HSI features, layout, and environment.

(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 HSIs (e.g., window manipulation, display selection, display system navigation). High-level HSI design review principles reflect NUREG-0700 guidelines.

(3) For risk-important HAs, the design seeks to minimize the probability that errors will occur and maximize the probability that an error will be detected if one should be 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
- feedback local environment
- inspection, test, and maintenance
- importance to safety

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

(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. 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) The HSIs is designed to support inspection, maintenance, test, and repair of (1) plant equipment and (2) the HSIs. The HSIs should be designed so that inspection, maintenance, test, and repair of the HSIs do not interfere with other plant control activities (e.g., maintenance tags should not block the operators' views of plant indications).

### 4.8.6 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 and evaluations. The methodology used for testing will be reviewed applying criteria provided below. Note the types of tests and evaluations performed will vary depending on the specific point in the design process.

#### 4.8.6.1 Trade-Off Evaluations

To adequately consider human performance the HFE team will use the example factors when performing trade-off 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 various design alternatives. .

#### 4.8.6.2 Performance-Based Tests

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

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

### 4.8.7 HSI Design Documentation

(1) The HSI design is captured within the GEEN QA Documentation system to include:

- The detailed HSI description including its form, function and performance characteristics
- The basis for the HSI requirements and design characteristics with respect to operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations records of the basis of the design changes

(2) The outcomes of tests and evaluations performed in support of HSI design should be documented.

### 4.8.8 HSI Design Implementation Plan

The HSI Design Implementation Plan will establish:

1. The methods and criteria for HSI design in accordance with accepted human factors practices and principles;

2. That the HSI design will implement the information and control requirements:

   a. Developed through the task analyses, including the displays, controls, and alarms necessary for the execution of those tasks identified in the task analyses as being critical tasks and;

   b. Includes the fixed position alarms, displays, and controls;

   c. Limit errors associated with risk important HAS;

   d. Identify human errors when feasible.

3. The methods for comparing the consistency of the HSI human performance, equipment design and associated workplace factors with that modeled and evaluated with in the completed task analysis;

4. The HSI design criteria and guidance for control room operations during periods of maintenance and test; and

5. The 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.

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

The HSI design will include features, which facilitate operator activities that tend to maintain the operators alert and attentive. Features of the HSI will be designed based upon methods that are 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 shall be a part of the documented design.

As described in the HSI Design Implementation Plan, the design of the information and controls located at the operator sit-down workstation will be integrated with the

design of the mimics displayed on the wide display panel (WDP) for consistency in nomenclature, symbols, and color.

Human factors principles will be followed and the color-coding, mimics, labeling and demarcation will be applied consistent with the main control room consoles. The task analysis will assume that ESBWR plant operators will not be color-deficient.

*See also Appendix B for a draft outline of this plan.*

## 4.9 Plant Procedures

Procedures are essential to plant safety because they support and guide personnel interactions with plant systems and their response to plant-related events.

The HFE team will develop a process for procedure development using applicable requirements from NUREG-0800 Section 13.5. The plant normal operating, abnormal operating, alarm response, and emergency operating procedures for the ESBWR will be developed as an integral part of the M-MIS and HSI development. The ESBWR procedure modifications from previous plants will address all personnel tasks that are affected by the changes in plant systems and HSIs. The procedures will be developed or modified to reflect the characteristics and functions of the plant improvements. The same human factors principles will be applied to both aspects of the interface to verify complete integration and consistency.

The procedures will be provided in their final form as part of the overall M-MIS Implementation Process. The M-MIS implementation will include steps, which provide verification that all functions and tasks assigned to the plant procedures are included in the operating procedures. The M-MIS implementation process will include validation of the operating procedures using the mockup/part-task and full-scope simulator facility.

In addition to the standard hard paper (laminated) copies, the plant procedures will be presented electronically on the video display units in the main control room. Electronically displayed procedures will conform to the following requirements unless simulation reveals deficiencies and a need for different implementation requirements:

1. Procedures will be in the form of logic or flow charts;

2. Procedures will normally provide on the same display as the procedure the parameters necessary for the operator to make each decision required. This will include checklists of prerequisites or interlocks to steps where applicable;

3. Procedures will provide the capability for the operator to access those controls needed to carry out the tasks directly from the procedure display;

4. Procedures will provide for the verification of operator decisions, with the operator retaining final control and authority whether or not to proceed. Automatic logging of those cases of disagreement will be provided;

5. Plant parameters and status presented as part of the procedure displays will be continuously updated; and

6. Procedures displayed in the HSI shall conform to industry and regulatory guidelines regarding HFE principles.

## 4.10 Training Program Development

Training of plant personnel is an important factor in ensuring safe and reliable operation of nuclear power plants. The training program applied by the COL applicant will help to provide reasonable assurance that plant personnel have the knowledge, skills, and abilities to properly perform their roles and responsibilities. Training program development will be coordinated with the other elements of the HFE design process by including, for example, a systematic analysis of job and task requirements.

### 4.10.1 Purpose

The aim of an implementation plan for training program development is to systematically incorporate information from the other HFE design tasks to support implementation of an ESBWR personnel training by the COL applicant. As a minimum, the training program will include the following five activities:

- A systematic analysis of the tasks and jobs that are triggered by cues from the HIS or procedures.
- Development of learning objectives derived from an analysis of desired performance through the training program
- Design and implementation of training based on the learning objectives
- Evaluation of trainee mastery of the objectives during training
- Evaluation and revision of the training based on the performance of trained personnel in the job setting.

### 4.10.2 Elements for training program development

The following elements will be supported by the HFE design team to be further developed by the COL applicant: General Approach, Organization of Training,

Learning Objectives, Content of Training Program, Evaluation of Training, and Periodic Re-training.

#### 4.10.2.1 General Approach

A systems approach to the training of plant personnel will be developed.

The approach will follow applicable guidance in NUREG-0800 Section 13.2 ("Training"), as defined in 10 CFR 55.4, and as required by 10 CFR 52.78 and 50.120. An overall scope of training will be defined by the COL applicant and supported by the HFE design team. It will include the following elements:

- Categories of personnel will be defined (e.g., senior reactor operator) to be trained
- Specific plant conditions (normal, upset, and emergency) will be defined using information from normal startup and shutdowns, expected transients, design basis events and key PRA/HRA sequences.
- Specific operational activities (e.g., operations, maintenance, testing and surveillance) will be defined from procedures, technical specifications and pre-initiator actions in the PRA/HRA.
- Key actions will be defined as required by cues from the HSIs (e.g., in the main control room, emergency operations facility, remote shutdown panel, local control stations).

The COL applicant training program plan will provide reasonable assurance that personnel have the qualifications commensurate with the performance requirements of their jobs. Training will address:

- Specific training will be provided for a full range of positions of operational personnel including licensed and nonlicensed personnel whose actions may affect plant safety.
- The training program will address a full range of plant functions and systems including those that may be different from those in predecessor plants (e.g., passive systems and functions)
- The training program will address the full range of relevant HSIs (e.g., main control room, remote shutdown panel, local control stations) including characteristics that may be different from those in predecessor plants (e.g., display space navigation, operation of "soft" controls) as is appropriate for each job classification.

The training program will address a full range of plant conditions as defined above.

#### 4.10.2.2 Organization of Training

The specific roles of the COL applicant and the HFE team for development of training requirements, development of training information sources, development of training materials, and implementation of the training program will be defined in a training plan. The initial role for the HFE team is expected be to provide input materials to the COL training program and if requested to conduct specific training modules.

The qualifications of organizations and personnel involved in the development and conduct of training will be defined in the training plan.

The COL applicant and the HFE team will define the facilities and resources to be used during different phases of the design and operation. The facilities may include a plant-reference simulator and part-task training simulators. The plan for these facilities will follow the guidance contained in ANSI 3.5 and Regulatory Guide 1.149.

#### 4.10.2.3 Learning Objectives

Learning objectives for each job description will be derived from the COL applicant analysis and information from the HFE team that describes desired performance after training. This analysis will include but not be limited to training needs identified in the following elements:

- Licensing Basis - Final Safety Analysis Report, system description manuals and operating procedures, facility license and license amendments, licensee event reports, and other documents identified by the COL applicant staff and HFE team as being important to training
- Operating Experience Review - previous training deficiencies and operational problems that may be corrected through additional and enhanced training, and positive characteristics of previous training programs. Such information is available through industry owner groups, and may also come from the COL applicant.
- Function Analysis and Allocation - functions identified as new or modified will come from the HFE design team.
- Task Analysis - tasks identified through the HFE process as posing unusual demands including new or different tasks, and tasks requiring a high degree if coordination, high workload, or special skills are expected to be provided by the HFE team to the COL training program.

- Human Reliability Analysis – This analysis as part of the PRA/HRA provided by the HFE design team is expected to be used to define coordinated roles for the operational crew to reduce the likelihood and/or consequences of human error associated with risk-important HAs and the use of advanced technology. Generic design PRA/HRA models will be made plant specific by the COL applicant.
- HSI Design – The HFE design team will identify HSI features whose purpose or operation may be different from the past experience or expectations of personnel. This is vitally important in the areas where an expanded role for passive safety systems has been incorporated into the defense in depth safety functions.
- Plant Procedures – The basic BWR symptom based emergency procedures will be updated to address the impact of passive safety systems by the HFE team and modified by the COL applicant to address plant specific issues. The HFE team will address specific tasks that have under gone extensive revision during past procedure development to address plant safety concerns.
- Verification and Validation (V&V) –The HFE design team will provide scenarios and information to the COL applicant to support V&V testing. The COL applicant will be responsible for identifying training concerns identified during V&V. Issues for training improvement are expected to arise from V&V of the HSI usability with the procedures for specific scenarios that lead to operator performance errors (e.g., misdiagnoses of plant event).

Learning objectives for personnel training that address the knowledge and skill attributes associated with all relevant topics and dimensions of a trainee's job will be initially developed by the HFE design team and enhanced by the COL applicant. Table 4.10, illustrates generic learning objectives for interactions with the plant, the HSIs, and other personnel.

**Table 4.10 Example Knowledge and Skill Dimensions for Learning Objectives Identification**

| Topic | Knowledge | Skill |
|---|---|---|
| Plant Interactions | Understanding of plant processes, systems, operational constraints, and failure modes. | Skills associated with monitoring and detection, situation awareness, response planning and implementation. |
| HSI and Procedure Interactions | Understanding of procedures and HSI structure, functions, failure modes, and interface management | Skills associated with interface management tasks. |

| | | |
|---|---|---|
| Interactions | tasks (actions, errors, and recovery strategies). | |
| Personnel Interactions (In the CR and in the plant) | Understanding information requirements of others, how actions will be coordinated with others, policies and constraints on crews' interaction. | Skills associated with crew's interactions (i.e., teamwork) |

#### 4.10.2.4 Content of Training Program

The COL applicant will provide a training program design based on the HFE team plan for training. The training plan will define specifically how learning objectives will be conveyed to the trainee. The plan will include:

- How lectures, simulators, and on-the-job training will be used to convey particular categories of learning objectives.
- The HFE design process is expected to define an initial listing of specific plant conditions and scenarios for training. The COL applicant and the owner groups are expected to upgrade specific training scenarios by incorporating lessons learned during the operational period.
- The HFE team will develop a training implementation plan. It will consider the order and schedule of training segment building blocks. The COL applicant will adopt and update the schedule leaving room for special scenario development and simulations to challenge well trained crews.
- The COL training program will use factual knowledge developed by the HFE design team. The COL applicant plan is expected to teach the knowledge and skill elements within the context of actual job tasks so that trainees learn to apply knowledge and skill training in the work environment. For example, the COL applicant plan is expected to integrate theory topic training with training in using procedures.

The COL applicant plan is expected to structure training programs for developing skills so that the training topics build upon the level of skill already mastered. For example the order of training will master the manipulation of control devices through the HIS, before developing coordination skills among crew members that require knowledge of how to manipulate the control system.

The COL training program will use the symptom-based procedures developed by the HFE team to support rules for decision-making related to plant systems, HSIs, and

use of the procedures. The symptom-based procedures will include rules for identifying cues, confirming, and interpreting information. The COL training program will cover acquiring new decision-making rules for interpreting symptoms of failures of systems, HSIs, and procedures that are a direct result of the passive design. The training will also eliminate existing "rules of thumb" from current BWRs that are not appropriate to the ESBWR passive design.

#### 4.10.2.5 Evaluation and Modification of Training

The COL applicant training program plan will include methods for evaluating the overall effectiveness of the training programs and trainee mastery of training objectives. The methods may include written and oral tests and review of personnel performance during walkthrough, simulator exercises, and on-the-job checking. Evaluation criteria for mastery of training objectives during individual training modules will be defined in the COL applicant training program plan. Methods for assessing overall proficiency will be defined and coordinated with regulations, where applicable for licensed personnel.

The COL applicant training program plan will define methods for verifying the accuracy and completeness of training course materials.

The COL applicant training program plan will establish procedures for refining and updating the content and conduct of training. The plan will include provisions for tracking training course modifications.

#### 4.10.2.6 Periodic Retraining

The COL training program plan will address how often and which job classifications need to undergo periodic retraining. The COL training program plan will provide for evaluating whether any changes or increases in retraining are warranted following plant upgrades and other modernization programs.

## 4.11 Human Factors Verification & Validation Activities

This section provides an overview of the integrated HF V&V activities with their associated inputs and outputs that will be included in the HFE plan. The main activities of HF V&V (in order of occurrence) are:

1. Operational Conditions Sampling (per NUREG 0711r2),
2. Design Verification,
    a. Inventory and Characterization,
    b. Human-System Interface (HSI) Task Support Verification,

c. Human Factors Engineering (HFE) Design Verification,

3. Integrated System Validation,

4. Human Factors Issue Resolution Verification (HED Resolution), and

5. Final Plant HFE/HSI Design Verification.

Additional special topics discussed are:

- Relationship Between HF V&V and Hardware/Software V&V,
- HF V&V Team,
- End-Users as Participants and Test Subjects, and
- Documentation, Reporting, Performance Measurement, and Integration of Results.
- V &V Implementation in areas of HSI task support. HFE design, Integrated System Validation and Documentation

### 4.11.1 Operational Conditions Sampling

This section addresses the range of dimensions for HSI evaluation.

#### 4.11.1.1 Human Factor Sampling Dimensions

The following sampling dimensions are addressed below: plant conditions, personnel tasks, and situational factors known to challenge personnel performance.

(3) The following plant conditions are included:

- normal operational events including plant startup, plant shutdown or refueling, and significant changes in operating power failure events, e.g.,
  - instrument failures [e.g., safety-related system logic and control unit, fault tolerant controller, local "field unit" for DCIS system, DCIS controller, and break in DCIS line] including I&C failures that exceed the design basis, such as a common mode I&C failure during an accident
  - HSI failures (e.g., loss of processing and/or display capabilities for alarms, displays, controls, and computer-based procedures)
- transients and accidents,
  - transients (e.g., turbine trip, loss of off-site power, station blackout, loss of all feedwater, loss of service water, loss of power to selected

buses or main control room (MCR) power supplies, and safety and relief valve transients);

- accidents (e.g., main steam line break, positive reactivity addition, control rod insertion at power, anticipated transient without scram, and various-sized loss-of coolant accidents[GWH80])
- reactor shutdown and cooldown using the remote shutdown system

- reasonable, risk-significant, beyond-design-basis events, which will be determined from the ESBWR specific PRA
- consideration of the role of the equipment in achieving plant safety functions and the degree of interconnection with other plant systems. (A system that is interconnected with other systems could cause the failure of other systems because the initial failure could propagate over the connections. This consideration is especially important when assessing non-class 1E electrical systems.)

(4) The following types of personnel tasks will be included:

- *Risk-significant HAs, systems, and accident sequences* - All risk-important HAs are included in the sample. Additional factors should be sampled that contribute highly to risk, as defined by the PRA, including:
  - dominant human actions (selected via sensitivity analyses)
  - dominant accident sequences
  - dominant systems (selected via PRA importance measures such as Risk Achievement Worth or Risk Reduction Worth)
- *OER-identified difficult tasks* - The sample will include all personnel tasks identified as problematic during the applicant's review of operating experience.
- *Range of procedure guided tasks* - These are tasks that are well defined by normal, abnormal, emergency, alarm response, and test procedures. The operator will be able to, as part of rule-based decision-making, understand and execute the specified steps. Regulatory Guide 1.33, Appendix A, contains several categories of "typical safety-related activities that will be covered by written procedures." The sample will include appropriate procedures in each relevant category:
  - administrative procedures
  - general plant operating procedures

- procedures for startup, operation, and shutdown of safety-related systems
- procedures for abnormal, off normal, and alarm conditions
- procedures for combating emergencies and other significant events
- procedures for control of radioactivity
- procedures for control of measuring and test equipment and for surveillance tests, procedures, and calibration
- procedures for performing maintenance chemistry and radiochemical control procedures

- *Range of knowledge-based tasks* - these are tasks that are not as well defined by detailed procedures. Knowledge-based decision-making involves greater reasoning about safety and operating goals and the various means of achieving them.
- *Range of human cognitive activities* -The sample will include the range of cognitive activities performed by personnel, including:
  - detection and monitoring (e.g., of critical safety-function threats)
  - situation assessment (e.g., interpretation of alarms and displays for diagnosis of faults in plant processes and automated control and safety systems)
  - response planning (e.g., evaluating alternatives for recovery from plant failures)
  - response implementation (e.g., in-the-loop control of plant systems, assuming manual control from automatic control systems, and carrying out complicated control actions)
  - obtaining feedback (e.g., of the success of actions taken)
- *Range of human interactions* - The sample will reflect the range of interactions among plant personnel, including tasks that are performed independently by individual crew members and tasks that are performed by crew members acting as a team. These interactions among plant personnel will include interactions between:
  - main control room operators (e.g., operations, shift turnover walkdowns) main control room operators and auxiliary operators
  - main control room operators and support centers (e.g., the technical support center and the emergency offsite facility)

- main control room operators with plant management, NRC, and other outside organizations
- Tasks that are performed with high frequency.

(5) The sample will reflect a range of situational factors that are known to challenge human performance, such as:

- *Operationally difficult tasks* - The sample will address tasks that have been found to be problematic in the operation of NPPs, e.g., procedure versus situation assessment conflicts. The specific tasks selected will reflect the operating history of the type of plant being validated (or the plant's predecessor).
- *Error-forcing contexts* - Situations specifically designed to create human errors will be included to assess the error tolerance of the system and the capability of operators to recover from errors if they occur.
- *High-workload conditions* - The sample will include situations where human performance variation due to high workload and multitasking situations can be assessed.
- *Varying-workload situations* - The sample will include situations where human performance variation due to workload transitions can be assessed. These include conditions that exhibit (1) a sudden increase in the number of signals that must be detected and processed following a period in which signals were infrequent and (2) a rapid reduction in signal detection and processing demands following a period of sustained high task demand.
- *Fatigue and circadian factors* - The sample will include situations where human performance variation due to personnel fatigue and circadian factors can be assessed.
- *Environmental factors* - The sample will include situations where human performance variation due to environmental conditions such as poor lighting, extreme temperatures, high noise, and simulated radiological contamination can be assessed.

#### 4.11.1.2 Identification of Sampling Scenarios

(1) The results of the sampling will be combined to identify a set of event scenarios to guide subsequent analyses. A given scenario may combine many of the characteristics identified by the operational event sampling.

(2) The scenarios will not be biased in the direction of over representation of the following:

- scenarios for which only positive outcomes can be expected
- scenarios that for integrated system validation are relatively easy to conduct administratively (scenarios that place high demands, data collection or analysis are avoided)
- scenarios that for integrated system validation are familiar and well structured (e.g., which address familiar systems and failure modes that are highly compatible with plant procedures such as "textbook" design-basis accidents)

#### 4.11.1.3 Special Considerations for Plant Modernization Programs

When evaluating plant modifications, the following factors will be addressed when identifying operational conditions:

(1) The operational conditions will reflect tasks that involve the modification, rather than the entire range of topics discussed above for Personnel Tasks.

(2) For integrated system validation, the operational conditions will address the transfer of learning effects on personnel performance when a modification replaces an old HSI or procedure. (Negative transfer of learning effects may occur when the new and old components are different and impose different demands on personnel.)

(3) For integrated system validation, when both old and new versions of the same HSI components with different means of presentation and methods of operation are permanently present in the HSI, evaluations will provide reasonable assurance that personnel can alternate their use of these HSI components without degrading their performance.

(4) Where old HSI components that are to be deactivated and left in place in the HSI, conditions will be identified for integrated system validation that would test the potential for task interference.

### 4.11.2 Design Verification (HFE)

The inventory of all HSI components associated with the personnel tasks identified from the operational conditions will provide a basis for HFE design verification. The inventory will include aspects of the HSI that are used for interface management such as navigation and display retrieval in addition to those that control the plant.

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

HSI Task Support Verification begins with a relatively narrow scope verification (compared to HFE Design Verification described in the next section). Initial HSI

Task Support Verification is a document-based, static evaluation process that includes independent verification in accordance with the GEEN QA requirements.

Task Analysis, PRA/HRA, and emergency operating procedure analysis, identify tasks critical to safety in terms of importance for function achievement, potential for human error, and impact of task failure. Where critical functions are automated, the analyses address the human tasks including the monitoring of the automated functions and the backup manual actions which may be required if an automated function fails. The initial HSI Task Support Verification confirms that the inventory of HSI components (controls, displays, alarms, procedures, and data processing) provides for personnel tasks as defined by these analyses.

More detailed HSI Task Support Verification confirms, for various operational tasks, that each HSI component meets the operability (task execution and information access) requirements specified for the end user (e.g., response time, accuracy, precision, etc.).

A process for identifying and addressing deficiencies during the V&V will be established and captured in the HFEITS. HSI components are considered deficient if, for example, there are:

- Unsupported tasks where a required control, display or alarm is missing (e.g., absence of on-screen pushbuttons)
- Partially supported tasks where HSI characteristics do not fully meet the operability requirements (e.g., poor real-time response and feedback when using a manual/auto controller, or inadequate pushbutton tactile feedback).
- HSI components that are not required for personnel tasks (e.g., extraneous, nonfunctional, or purely decorative objects in graphical displays).

#### 4.11.2.2 HFE Design Verification

HFE Design Verification is a form of verification that is broader in scope than HSI Task Support Verification. It is evaluation of the HSI with respect to a particular end user population, and not an evaluation of the end users. Individual HSI components are checked against plant engineering criteria, human engineering criteria, and operating and functional requirements. The verification is performed in accordance with ESBWR GEEN QA include requirements for independent verification.

HFE Design Verification verifies that each HSI component design meets personnel task requirements and operational considerations, and reflects HFE guidelines, standards, and principles. HFE Design Verification covers design aspects such as:

- HSI characteristics (e.g., coding, conventions, input devices, dialog, display navigation, etc.)
- Inter-personnel communication systems that support users of the HSI (e.g., functional capabilities, equipment performance, ease of use, etc.)
- Hardcopy procedures and electronically displayed ("on-line") procedures
- Room layouts and panel configurations (e.g., anthropometrics, ergonomics, grouping, labeling, etc.)
- Work environment (e.g., lighting, space, air conditions, floor design, noise mitigation)

Designs are compared to HFE guidelines to determine whether they account for human characteristics and capabilities. Deviations from accepted HFE guidelines, standards, and principles are documented for resolution/correction and acceptably justified on the basis of documented rationale such as trade study results, literature-based evaluations, demonstrated operational experience, and tests and experiments.

### 4.11.3 Integrated System Validation

Integrated System Validation is a performance-based evaluation of the integrated HSI design and human task performance to ensure the HSI is operable within all performance requirements, and that it supports safe operation of the plant. Integrated System Validation is performed using dynamic HSI prototypes and high-fidelity simulators that can facilitate regulatory reviews and witnessing.

The HFE team will develop a validation process by establishing detailed "Test Objectives" for specific "Validation Test beds." The testing process will include: "Plant Personnel" that are licensed for the activities in the test and different from the design team; realistic "Test Scenarios" will be defined that are different from the design scenarios; good quality "Performance Measurements" will be selected to evaluate the HSI. Measurement characteristics will include construct validity, diagnosticity, impartiality, objectivity, reliability, resolution, sensitivity, simplicity, and unintrusiveness.

The performance measures will be used to measure performance of the plant personnel (i.e., personnel tasks, situation awareness, cognitive workload, and anthropometric/physiological factors). Some of these measures will help identify deficiencies in the HIS, training and procedures. For primary (e.g., start a pump), and secondary (e.g., access the pump status display) tasks the personnel task measurements will consider observable measures such as time, accuracy, frequency, errors (omission and commission), amount achieved or accomplished, consumption or quantity used. More subjective measures, which can be obtained from reports of

participants, behavior categorization by observers, will address issues such as situation awareness, cognitive workload, anthropometric and physiological factors.

Performance criteria will be established to support decisions as to whether the design is validated or not. The basis for criteria will be defined, (e.g., requirement-referenced, benchmark referenced, normative referenced, or expert-judgment referenced). The emphasis of the validation is on HSI effectiveness more so than understandability and compatibility of the HSI with respect to the end user. Integrated System Validation confirms

- Adequacy of the entire HSI configuration for achieving HFE program goals consistent with HFE practices and principles
- Allocation of functions and the degree of task dependence on procedures
- Adequacy of the HSI to support plant crews in accomplishing critical functions and tasks
- Human performance assumptions in PRA/HRA
- Tolerance to human error and system faults
- HSI facilitates efficient search and retrieval of information and controls
- The effect of HSI characteristics on operator workload
- Adequacy of staffing
- Adequacy of procedures

Procedure validation confirms that the procedures

- Are consistent with the HSI in terms of controls, displays, alarms, and data processing
- Are useable
- Function as intended in the integrated HSI design

Validation can lead to design changes and design changes are handled as part of the formal design change control process. The following are taken into account during the design change process:

- HSI Task Support Verification and HFE Design Verification for minor design changes.
- Extensive or significant changes may require re-verifying that functional uses of the original design have been addressed, evaluating the change once it has been

implemented and integrated into the overall HSI, and evaluating the change with respect to impact on procedures and training.

- Major design changes require re-validation to confirm that the change corrected the deficiency.

Integration concerns integration/interfacing of HSI elements (controls, displays, alarms, communication devices, etc.) and integration/interfacing of system functions and dynamic performance. Validation of dynamic and time-dependent performance typically involves at least a fully functional thread of the total system. DCIS is the total, fully integrated system and final, complete validation can only be achieved with the entire DCIS. However, validation is a progressive, cumulative activity. Hence validation at any stage in the overall V&V process is partial validation, using integrated subsystems of DCIS. For instance, the non-safety portion of DCIS is an integration of different process system controls and several HSIs (displays, mimic, alarms, large variable display, switches). It is testable and it can be partially validated separately of other DCIS portions, including safety-related portions. Each of the following are therefore treated as an "Integrated System" in the context of this plan document:

1. The entire DCIS
2. The non-safety related portion of DCIS
3. The safety-related portion of DCIS (i.e., DCIS Essential Controls) consisting of:
   a. Safety System Logic and Control (SSLC) Reactor Trip and Isolation Functions (RTIF) subsystem ,and
   b. SSLC Engineered Safety Features (ESF) subsystem
4. The RSS
5. An LCS critical to plant safety
6. Any "HSI thread" (i.e., operationally useful HSI function) of the above.

To ensure consistent testing the HFE team will develop a test design protocol to balance coupling of crews with scenarios, to standardize test procedures, to define elements for training of test conductors and test participants, and to conducting of pilot tests studies. Approaches for implementation are discussed in section 4.11.10.

The HFE team will develop a plan for systematic analysis and interpretation of the data. The analysis will use both quantitative and qualitative methods link the

observed performance data to established performance criteria. If performance measures do not pass established levels, they may be resolved by adjusting the design and retesting or by using the HED evaluation process. Systematic scientific processes will be used to verify the analysis validity and margin of error.

The conclusions of the testing and analysis process will be clearly documented. This will include the statistical and logical bases for determining that performance of the integrated system is validated. The Validation limitations will be considered in terms of aspects of the tests that were not well controlled, potential differences between the test situation and actual operations, and potential differences between the validated design and plant as built.

### 4.11.4 Human Factors Issue Resolution Verification

The ESBWR Man-Machine Interface System (M-MIS) Design Implementation Plan establishes that HFE issues (Human Factors Engineering Discrepancies, HEDs) are tracked with a Human Factors Engineering Issue Tracking System (HFEITS) consistent with NUREG-0711 and NUREG-0700, see Section 4.2. The HFEITS facilitates resolution of human factors issues by providing the means to record and track issues throughout the process ("life cycle") of HFE/HSI design, development, and evaluation. Tracking by the M-MIS designer ends when HFE V&V is completed and tracking is transferred to the COL Applicant.

Human Factors Issue Resolution Verification is the process of verifying that HFE issues are identified, evaluated and documented in the HFEITS. If human error discrepancies are identified, they will be justified, analyzed, prioritized, documented, so that design solutions can be developed and evaluated. Then the modification can be adequately addressed in the design. Issues that cannot be resolved until the plant is built are specifically identified and incorporated into Final Plant HFE/HSI Design Verification. Human Factors Issue Resolution Verification is complete when all validation issues have been resolved, implemented and verified.

### 4.11.5 Final Plant HFE/HSI Design Verification

Final Plant HFE/HSI Design Verification is a check of the final, actual HSIs against design description document(s) that include performance criteria and the requirements for verification that the "as built" design is the design resulting from the HFE design process. It verifies aspects of the design that may not have been evaluated previously with a simulator (e.g., lighting, environmental control, floor design, sound powered communication, noise mitigation, display changes based on pre-operation and startup testing, etc.). It also verifies resolution of open items from the HFEITS. Developing a document that describes the final installed design and its performance criteria is part of the Final Plant HFE/HSI Design Verification process.

### 4.11.6 Relation to Hardware/Software V&V Process

HF V&V is a process for assuring HFE-related quality of the HSI and operating procedures. Among other things, HF V&V identifies, documents, and facilitates resolution of defects in the HSI. Resolution could impact hardware/software design (e.g., component type or technology, graphic display performance) depending on the specific nature of the defect. Likewise, the hardware/software V&V process could impact HSI design (e.g., component dimensions, graphic display layout). The relationship between the two V&V processes is a process interface whereby resolution of V&V findings are integrated into the design and implementation phases of HSI, hardware, and software.

#### 4.11.6.1 HF V&V Team

There is no single HF V&V team responsible for all of the activities in this plan. The term "HF V&V Team" is used herein as a general term to refer to the persons that conduct an HF V&V activity. Those persons may be from a single organization or more than one organization. For example, HSI Task Support Verification of operator display image specifications known as HSI Design Reports is performed by one responsible design organization (RDO). A team member may contribute a combination of expertise and qualifications.

The HFE Lead is responsible for defining, managing, leading, and executing the HF V&V program. The program is the composite of all HF V&V activities for ESBWR project. The HF V&V Activity Lead and HF V&V Activity Director are those persons responsible for a given HF V&V activity (or set of activities), such as the HF V&V activities performed during testing (referred to as HFE-Phase 2). They may be persons other than the HFE Lead and CRDT Chairperson.

### 4.11.7 Integrated System Verification

The HF V&V Activity Lead is responsible for the following:

- Overall administration and review of the activities
- Approving HF Verification & Validation Test Plans
- Planning and coordinating the HF V&V activity with the activity of another group if the two activities require shared used of the mockup or simulator
- Reviewing and approving HFE issues
- Report documentation
- Maintaining records

The HF V&V Activity Director is responsible for the following:

- Lead representative and spokesman while conducting the HF V&V activity
- Scheduling the HF V&V activity and managing personnel assignments
- Producing timely, accurate records
- Support reviews of test plans to ensure consistent objectives within the scope of HF V&V
- Reviewing and approving HFE issues

### 4.11.8 End-Users as Participants and Test Subjects

Participants conduct an HFE V&V activity jointly with GE. COL Applicant personnel are participants in the following HF V&V activities:

- Human-System Interface (HSI) Task Support Verification
- Human Factors Engineering (HFE) Design Verification
- Integrated System Validation
- Final Plant HFE/HSI Design Verification

The training programs administered by GE and COL Applicant will include personnel participating in V&V activities. Test Subjects are evaluated as part of an HF V&V activity. COL Applicant personnel are test subjects in the Integrated System Validation activity.

### 4.11.9 Documentation, Reporting, and Integration of Results

Documentation facilitates identifying HFE-related deficiency categories in terms of HSI components and the level of task support. Results of the HF V&V activities are documented in reports that address the following:

- Objectives
- Participants (name, position, experience/qualifications, relevant demographics)
- Descriptions of HSIs involved (or references to applicable documents)
- Test Conditions
- Personnel performance issues (if any) as applicable to the activity
- Methods and procedures used (by reference to this plan document)
- Deviations (if any) from test methods, procedures, and acceptance criteria
- Documentation and administration of deviations (i.e., recorded, assessed for impact, resolved, justified, etc.).

- Presentation and discussion of test data (e.g., performance measurements), test results, and findings
- HFE issues (if any), including training-related issues to be examined with respect to learning objectives and post-training performance
- Conclusions
- Recommendations such as design changes or corrective actions (e.g., by reference to corresponding HFEITS record)

The final ("as built") design is documented in accordance with the QA requirements. Proceedings and results of the HF V&V program are recorded and in accordance with GEEN QA

### 4.11.10 V&V Implementation

This section prescribes implementation of the five main HF V&V activities and the HFEITS. The following are addressed for each HF V&V activity, to the extent applicable:

- Scope, e.g.,
  - Items to be tested and evaluated (T&E'd), including justification for features of the item not to be T&E'd (i.e., the scope of HSI that the respective HF V&V activity applies to)
- Objectives
- Participants, Test Subjects, and Observers, e.g.,
  - Staffing needs and personnel skills/experience
  - Personnel roles and responsibilities
  - Provisions for audits and witnessing
- Methods and Procedures, e.g.,
  - Task Performance Diagrams
  - Interviews and Questionnaires
  - Checklists
  - Walkthroughs and talkthroughs
- Test and Evaluation (T&E) Conditions
  - Test environment, test equipment and tools (including any requiring development and qualification)

  - Test sequencing and T&E time estimates

- Acceptance Criteria (for making pass/fail/retest decisions for each test) for each performance measure (e.g., safe operating ranges, alarm conditions, and personnel response times per plant Technical Specifications)
- HSI Equipment Performance Measures, e.g.,
  - dynamic response
  - display navigation
- Operator Performance Measures (qualitative and quantitative)
  - Operational performance relevant to plant safety (e.g., error avoidance, avoiding alarm conditions and Technical Specification violations)
  - Crew primary task performance (e.g., response time, task completion times, procedure violations)
  - Crew errors (e.g., intention errors related to assessing the plant's condition, and execution errors related to using the HSI)
  - Situation awareness (e.g., proper assessment of implications of alarm states)
  - Workload (cognitive and physical) and provide justification for their use
  - Crew communications and coordination (e.g., information sharing and coordinated control actions)
  - Dynamic anthropometry evaluations (e.g., reach and dexterity)
  - Physical positioning (e.g., physical motion between panels and workstations)
- Data Collection and Analysis
  - Simulator recording of chronological event logs (operator actions, alarms, disturbances, etc.) and process variables
  - Video recordings of walkthroughs and talkthroughs
  - Recording of observations, notes, and commentary
  - How to conduct root cause analysis of findings
  - Dispositioning the findings
- Documentation and Integration of Results

#### 4.11.10.1 Implementation of HSI Task Support Verification

##### 4.11.10.1.1 Scope

Initial HSI Task Support Verification applies to:

- Panel drawings (covering fixed-position controls, indications, and alarms)
- Room layout/arrangement drawings
- Computer-generated displays (providing controls, indications, and alarms)

##### 4.11.10.1.2 Objectives

The objectives of initial HSI Task Support Verification are to verify:

- That the HSI inventory is consistent with the HFE analyses (SFRA, AOF, TA, HSI Design)
- That, in addition to initial TA results, the HSI design accommodates operator tasks as confirmed through emergency operating procedure analysis and PRA/HRA of critical operator actions

The objective of detailed HSI Task Support Verification is to verify:

- That each HSI component meets the user operability requirements associated with a given task

##### 4.11.10.1.3 Participants, Test Subjects, and Observers

COL Applicant participation with GE is expected in these areas:

- Panel drawings
- Room layout/arrangement
- Computer-generated displays

##### 4.11.10.1.4 Methods and Procedures

The HSI design during initial HSI Task Support Verification is preliminary and based upon Task Analysis and initial versions of issued specifications such as System Design Descriptions (SDDs), P&IDs, Logic Diagrams, and Hardware/Software Specifications (HSSs). More detailed HSI Task Support Verification applies to the HSI components. Mockups can be used for HSI Task Support Verification if, in lieu of panel drawings and room layout drawings (i.e., the two-dimensional form), they mock the HSI components in three-dimensional form.

PRA/HRA determines risk profiles using best-estimate Human Error Probabilities (HEPs) that are based on analysts' understanding of the HSI design and its operability. PRA/HRA identifies critical operator actions and their error probabilities. PRA/HRA models the role of operators and other personnel in response

to accident sequences. Task Analysis and HSI design account for PRA/HRA results. Design changes required based on PRA/HRA, Task Analysis, and HSI design, are propagated throughout the plant design and systems designs via the normal engineering, design change, and verification processes. Documented PRA/HRA assumptions about the HSI design and procedures are available for implementation considerations by designers and procedure developers.

Task performance requirements (e.g., HSI Design Implementation Plan , Style Guide for Graphical User Interfaces , and Display Primitives Design Specification) are imposed on the various HSI hardware and software components. These requirements are included (directly or by reference) in hardware and software specifications (e.g., DCIS Hardware/Software Specification. Verification equivalent to detailed HSI Task Support Verification concerning task performance requirements occurs during DCIS factory acceptance tests. These tests are performed in accordance with test specifications (e.g., Software Test Plan and Acceptance Criteria).

#### 4.11.10.1.4.1 Panel and Room Layout/Arrangement Drawings

Several groups and organizations achieve HSI Task Support Verification of panel drawings through an iterative process of reviews. The groups and organizations include the CRDT, individual system designers, independent verifiers, HFE analysts, procedure developers, and COL Applicant. The results of HSI analyses for individual plant systems are checked for consistency with the drawings. Collaborative reviews by these groups and organizations during the development of the ESBWR Safety Analysis Report provide additional accountability for critical operator actions in the panel designs. HSI Task Support Verification of layouts for the MCR, RSS, and LCSs are accomplished in a similar manner.

#### 4.11.10.1.4.2 Computer Generated Displays

The HSI inventory is analyzed and specified (on a per-system basis) in HSI Design Reports. The analyses and documentation are done in accordance with GEEN QA and QA program that includes independent verification. This process includes reviews by the respective system engineering discipline to ensure the analyses support, and are supported by, the system design specifications (SDD, Logic Diagrams, P&IDs, etc.). In some cases, COL Applicant members also review selected reports.

### 4.11.10.1.5 Test and Evaluation (T&E) Conditions

Test conditions are defined in test plans and test specifications.

### 4.11.10.1.6 Acceptance Criteria

The Acceptance Criteria is that the objectives are met.

#### 4.11.10.1.7 Performance Measures

There are no performance measures associated with initial HSI Task Support Verification because the verification concerns completeness of the HSI inventory. Performance measures associated with detailed HSI Task Support Verification are the performance requirements (e.g., from applicable hardware/software design specifications) and HFE design guidelines (e.g., Style Guide for Graphical User Interfaces. These requirements cover quantitative parameters, limits, tolerances, etc., concerning performance such as completion time, range, accuracy, precision, frequency, and percent completion.

#### 4.11.10.1.8 Data Collection and Analysis

The document reviews and analyses discussed above (Methods and Procedures) constitute the data collection and analysis portion of HSI Task Support Verification.

#### 4.11.10.1.9 Documentation and Integration of Results

Deficiencies identified by evaluators are documented. A deficiency is logged into the HFEITS if it matches at least one of the HFE issue entry criteria.

### 4.11.10.2 Implementation of HFE Design Verification

#### 4.11.10.2.1 Scope

HFE Design Verification applies to:

- HFE analyses (SFRA, AOF, TA, HSI Design)
- Panel anthropometrics
- Operating procedures
- HSI components (e.g., controls, displays, alarms, data processing, communications equipment) required to accomplish human tasks and actions (as defined by the TA, EOP analysis, and PRA/HRA critical operator actions).
- Industrial Television (ITV) equipment in the MCR
- Work environment and workplace layout (MCR, RSSL, MCRBP)

#### 4.11.10.2.2 Objectives

The objectives of HFE Design Verification are to verify that:

- HFE analyses (including documentation) meet QA requirements
- HFE analyses are accomplished in accordance with the implementation plan requirements for the respective analyses
- HSI component design specifications incorporate applicable HFE requirements (guidelines, standards, criteria)

- HSI components are implemented per the specified HFE requirements

HFE Design Verification is comprehensive enough to provide objective evidence that the following are addressed:

- Operator tasks under normal, abnormal, and emergency conditions
  - Status monitoring and situation awareness of automatic safety functions
  - Surveillance testing and maintenance (e.g., equipment blocking, tagging, and bypass)
  - Alarm monitoring, analysis, and response
  - Fault detection, analysis, diagnosis, and mitigation
  - Override of automated systems and their direct control
  - Risk-significant interactions as defined by PRA/HRA
- Operator tasks guided by procedures of varying complexity
  - Rule-based tasks (procedure intensive)
  - Knowledge-based tasks (requiring judgment, planning, analysis, and reasoning based on observed symptoms)
- Operator tasks involving the different types of interactions with the HSI
- Particular operator tasks, if any, identified from operating experience reviews (OERs)
- Crew interactions
  - During operations, shift turnovers, walkdowns, maintenance, etc.
  - With the Technical Support Center during accident management
  - With management and other outside organizations during emergency management (e.g., from the EOF)

#### 4.11.10.2.3 Participants, Test Subjects, and Observers

Participation is as follows:

- Performs and verifies HFE analyses
- COL Applicant participates with GE in verifying partially dynamic graphic display images (i.e., displays not connected to a simulator)

#### 4.11.10.2.4 Methods and Procedures

##### 4.11.10.2.4.1 HFE Analyses

SFRA, AOF, TA, and HSI analyses (and associated reports) for individual plant systems are developed in accordance with the developer's QA program. Each report is reviewed by the respective RDO for that system, and review comments are documented in the preparer's GEEN QA Documentation system.

##### 4.11.10.2.4.2 Panel Anthropometrics

Verification of the anthropometrics is accomplished as an integral part of the NUREG-0700 (Volume 2 - Reviewer's Checklist) evaluations performed with mockups and simulator versions of the MCRP and RSSL.

##### 4.11.10.2.4.3 Operating Procedures

Operating procedures include the following:

1. Integrated Operating Procedures (IOP)
2. System Operating Procedures (SOP)
3. Abnormal Operating Procedures (AOP)
4. Emergency Operating Procedures (EOI)
5. Annunciator Response Procedures (ARP)
6. Surveillance Test Procedures (STP)

EOIs are based upon the ESBWR Plant Specific Technical Guidelines (PSTGs) that, in turn, are derived from the BWR Owners' Group Emergency Procedure and Severe Accident Guidelines (EPGs/SAGs), Revision 1, dated July 1997 (See ESBWR Chapter 18 DCD Appendices A, B, and C). The EOIs consist of EOI Support Procedures and EOI Flowcharts (estimated to be 1.2m high by 0.75m wide, but producible to any preferred size). The EOI Support Procedures may consist of certain SOPs and AOPs containing detailed instructions for abnormal system operation or abnormal overrides of interlocks. EOI flowcharts (estimated quantity of 8) address the four main controls (RPV Control, Primary Containment Control, Secondary Containment Control, and Radioactivity Release Control) and the five contingencies (Alternate Level Control, Emergency RPV Depressurization, Steam Cooling, RPV Flooding, and Level/Power Control). The flowcharts also include EOI graphs.

Verification of written procedures is performed in accordance with the procedure writer's approved QA program. Procedures are checked for

- Compliance with the Procedure Development Implementation Plan, ESBWR Procedure Writer's Guide and other requirements and guidelines (e.g., BWR Owners Group Emergency Procedure Guidelines and Severe Accident Guidelines, BWROG EPG/SAG)
- Technical accuracy and format quality
- Correct references to HSI components

#### 4.11.10.2.4.4 HSI Components

Verifications of HSI component designs and implementations are checks that the components are built as specified. Design specifications (e.g., P&IDs, Logic Diagrams, Display Control Tables (DCTs) and associated Change Descriptions (CDs), and unincorporated Engineering Change Notices) are consulted as needed for understanding component operation, design changes, and investigation of findings.

For example, display image specifications (part of HSI reports and display building specifications (DCTs), are developed in accordance with the HSI Implementation Plan. The simulator display builder uses these to build partially dynamic graphic display images (i.e., displays not yet connected to a simulator). The images are verified through a collective effort by GE, COL Applicant, and subcontractors, to ensure display readiness for validation. Partially dynamic displays are verified for consistency and correctness as follows:

- Visually checking whether or not the Flat Panel Display (FPD) image replicates the DCT image
- Visually checking for compliance with the Style Guide for Graphical User Interfaces and the Display Primitive Design Specification
- Dynamically checking that each Display Primitive on an FPD image correctly assumes each of its states in accordance with the DPDS and the DCT.

Other HSI components subjected to HFE Design Verification include the following:

- Fixed-position (hard) switches
- Fixed-position (hard) indicators such as meters and status lights
- Labeling
- Alarm tiles
- Alarms displayed via 42-inch diagonal Flat Panel Display (FPDs)
- FPDs (15-inch and 18-inch diagonal)
- Large (70-inch diagonal) variable display

- Mimics (on WDP and RSS)
- Communication systems
- Data and video interfaces necessary to link the TSC to the MCR and the plant computer system
- Equipment to duplicate or to link the EOF to the plant process database used to support the MCR and the TSC

Verification of MCR and RSS HSI components (i.e., switches, indicators, labeling, alarm tiles and displays, FPDs, large variable display, mimic, communication systems) occurs as part of the normal course of engineering design in accordance with ESBWR QA requirements that include requirements for independent verification.

The functionality of data and video interfaces with the TSC, and equipment to duplicate or link the EOF to the plant process database, are verified during factory acceptance tests. Verification of these components is completed during integration testing at the site as part of the Final HFE/HSI Design Verification activity.

#### 4.11.10.2.4.5 Industrial Television

Industrial Television (ITV) System is a stand-alone system with a user console adjacent to the Shift Supervisor Console and two television units mounted in the Wide Display Panel (WDP). The ITV system is verified in accordance with ESBWR GEEN QA include requirements for verification. HFE Design Verification confirms that the console designs, and televisions at the WDP, meet user requirements, exhibit prudent HFE design practices, and effectively integrate with the MCR arrangement and work environment. The HSI at the ITV user console is not subjected to HFE V&V because it is an off-the-shelf product that does not perform process control and monitoring functions.

#### 4.11.10.2.4.6 Work Environment

HFE design verification of MCR, RSS, and MCRBP work environment aspects (e.g., lighting, space, air conditions, floor design, noise mitigation) is part of the normal engineering, design change, and verification process. Final verification against HFE guidelines such as those in NUREG-0700 occurs at the site as a COL holder responsibility.

#### 4.11.10.2.4.7 Workplace Layout

HFE design verification of MCR, RSS, and MCRBP workplace layout is part of the normal engineering, design change, and verification process. Final verification against HFE guidelines such as those in NUREG-0700 occurs at the site.

#### 4.11.10.2.5 Test and Evaluation (T&E) Conditions

##### 4.11.10.2.5.1 Mockup

A full-scale, foam core mockup of the MCR panels is staged to facilitate design, verification, and evaluation activities. The staging area is large enough that portable partitions can be used to mock up the boundaries and layout of Control Building walls of the MCR. Full-scale panel arrangement drawings are attached to the mockup. The mockup is not populated with any HSI hardware.

##### 4.11.10.2.5.2 General Electric Test System (GETS)

The GETS is a partial-scope ESBWR simulation and test system for developing, testing, verifying, and partially validating the following:

- Plant simulation models
- Control systems
- Operator displays
- Procedures

GETS hardware includes:

1. Flat Panel Displays (FPD) with capacitive touchscreens
2. Workstations to store and display the graphics for the FPDs
3. Simulation computers
4. Ethernet network controllers and node bus interface units that interconnect the workstations

GETS simulation software includes:

1. Graphical Interface for Process Simulation for process modeling of hydraulic and thermal networks (P&ID equivalents)
2. Logic Implementation and Documentation (LIDO) for modeling of analog and binary control logic schemes (Logic Diagram equivalents)
3. Transient Analysis Code (TRAC) for modeling core kinetics and NSSS for the reactor pressure vessel

The initial GETS configuration does not include:

1. Hardware switches (but they are emulated at the Instructor Station to facilitate display evaluations using operating procedures)
2. Alarms

3. On-line procedures
4. Maintenance/test/surveillance/diagnostic displays
5. Wide Display Panel
6. Simulator sequence-of-events recording/playback

GETS is used to HFE design verify operator displays.

#### 4.11.10.2.5.3 Baseline Simulator (BS)

The Baseline Simulator (BS) ESBWR is the earliest available ESBWR simulator that establishes a baseline of an ANSI/ANS-3.5-1998 compliant simulator. It is characterized by the following HSI:

1. Fully prototypic MCR panels (excluding communication equipment and closed-circuit television equipment)
2. Fully prototypic RSS panels
3. Some fully prototypic LCSs (e.g., RCIS)
4. Operator displays covering at least 48 plant systems, inclusive of all necessary safety-related systems
5. Prototypic operator displays for Safety Parameter Display System (SPDS)
6. General Displays
   *This includes Operator Aid displays (e.g., Near-Criticality Trends, Low-Power Water Level Control, Power Flow Map, Reactor Heat Up Rate, Safety Systems Bypassed and Inoperable Status Indication, Post Scram Status, and ECCS Summary)*
7. Balance of necessary displays available in non-prototypic, yet animated form
8. Representation of the alarm system with static alarm prioritization

The BS is updated with more recent design input data prior to operator training at the site.

The BS is used to verify the following HFE design:

- Panels (MCR, RSS, LCSs)
- Displays
- Alarms
- Procedures

#### 4.11.10.2.5.4 Full Scope Simulator (FSS)

The FSS contains the full functionality of the MCR and RSS HSIs that is not available in the BS. It is used to verify the fully integrated HSIs including any changes to procedures and training. FSS functions that are not in the BS include the following :

1. Plant Automation System
2. OLPS (a "job performance aid")
3. Dynamic alarm prioritization
4. Graphic Displays for 40 plant systems
5. Group Point Displays (part of Transient Recording and Analysis function)
6. Sequence of Events (SOE) monitoring

#### 4.11.10.2.6 Acceptance Criteria

The HFE guidelines of Part 2 of NUREG-0700 are used for HFE Design Verification. The guidelines are criteria for verifying the design and their applicability depends on the specific design feature being verified. NUREG-0700 Appendix B is considered when developing design-specific HFE guidelines documents and checklists. Design-specific HFE guidelines documents are identified whenever such documents are used as criteria for HF V&V activities.

#### 4.11.10.2.7 Performance Measures

Performance measures concern performance of the HSI. The measures are embodied in requirements contained in design specifications.

#### 4.11.10.2.8 Data Collection and Analysis

Verifications using the BS are recorded on checklists.

#### 4.11.10.2.9 Documentation and Integration of Results

Deficiencies identified by evaluators are documented. A deficiency HED is logged into the HFEITS if it matches at least one of the HFE issue entry criteria.

### 4.11.10.3 Implementation of Integrated System Validation

#### 4.11.10.3.1 Scope

Integrated System Validation applies to:

- Panel layouts (anthropometrics) and labeling
- HSI components (controls, displays, alarms, data processing, communications equipment) that include:

  - Operator displays and their associated FPDs (15-inch and 18-inch diagonal)
  - Fixed-position (hard) switches
  - Fixed-position (hard) indicators such as meters and status lights
  - Alarm tiles
  - Alarms displayed via 42-inch diagonal FPDs
  - Large variable display (70-inch diagonal)
  - Mimics
  - Electronic (on-line) procedures. [*Joint GE and COL Applicant responsibility*]
  - Phone, radio, page party, and public address devices
- Hardcopy procedures [COL Applicant responsibility]
- Portable utility board for EOP flowcharts (and perhaps shift turnover information) [COL Applicant responsibility]
- Portable cart for hardcopy procedures [COL Applicant responsibility]
- The standard design features of the ESBWR Main Control Room HSI (see ESBWR DCD Chapter 18).

#### 4.11.10.3.2 Objectives

The objectives are to confirm:

- HFE-adequacy of the integrated HSI configuration
- Automation (allocation of functions and the degree of task dependence on procedures)
- Adequacy of the HSI (equipment performance, dynamic and time-dependent aspects) to support the crew in accomplishing critical functions and tasks (e.g., evaluating plant status, diagnosing transients, performing control actions to maintain safety)
- Human performance assumptions in PRA/HRA
- Tolerance to human error and system faults
- That the HSI facilitates efficient search and retrieval of information and controls
- The effect of HSI characteristics on operator workload
- Adequacy of staffing
- Adequacy of procedures

#### 4.11.10.3.3 Participants, Test Subjects, and Observers

##### 4.11.10.3.3.1 Validating Displays Using GETS

The HF V&V teams performing qualitative validation of display usability with GE include *COL Applicant* personnel (operations, maintenance, training, QA, etc.), and GE subcontractors.

##### 4.11.10.3.3.2 Validations Using BS and FSS

The HF V&V teams performing validations with BS or FSS include GE personnel, GE subcontractors, and *COL Applicant/Holder* personnel.

##### 4.11.10.3.3.3 Methods and Procedures

Performance evaluations cover human performance and integrated HSI performance. Performance is evaluated on the basis of whether the acceptance criteria are met. The following outlines typical steps to be taken to prepare, and produce evaluation procedures, for HF V&V activities using the simulators:

- Define the evaluation team (participants)
- Identify the operating crew (test subjects) and support staff to operate simulators and recording apparatus (e.g., video cameras)
- Identify required witnesses and authorized observers
- Train (or rehearse with) the evaluation team and operating crews (as necessary)
- Obtain operating crew biographical information (age, anthropometrics, qualifications, experience, age, license held, etc.)
- Define the scenarios (including initial conditions)
- Define evaluation criteria
- Document assumptions (e.g., concerning plant operating conditions, tasks such as tagouts performed by other plant staff personnel, automation, etc.)
- Brief the evaluation team and operating crew on purpose, objectives, and how evaluations are to be conducted
- Explain the scenarios and test conditions to the evaluation team and operating crew
- Acquire the materials and resources for data collection methods (interview guides, questionnaires, observation forms, recording equipment and user manuals, etc.)

- Identify source documents (e.g., procedures, PRA/HRA, Technical Specifications, etc.) that delineate expected operator responses and expected plant behavior
- Schedule the evaluation

#### 4.11.10.3.3.4 Evaluating Operational Safety and Task Performance

Operator crews are subjected to a set of test scenarios run on the simulator. The test scenarios have predefined initial conditions, applicable symptoms, and expected system responses and plant behavior. Each crew is subjected to a given scenario at least twice. Each crew is also subjected to the same set of scenarios for purposes of comparing crew performance under similar uses, and conditions, of the HSI. Test subjects are not told what particular scenario is going to be simulated. The evaluation team observes the simulated exercise and documents crew performance. Debriefings and structured interviews are held after the simulated scenarios. Evaluators take notes on these discussions to supplement video recordings and visual observations.

It is recognized that simulator testing environments cannot fully replicate the influence that Performance Shaping Factors (PSFs) such as stress and noise have on operator human performance in real situations. Simulator testing environments can also bias operator behavior. For example, during a simulator test scenario, the operator anticipates an abnormal situation occurring. The anticipation heightens the operator's attention and alertness to an abnormal event. Operator responses are also shaped by adherence to procedure and the absence of potential conflicts between rote procedure compliance and economic demands (e.g., maximizing the unit's capacity factor).

Validation is a progressive, cumulative activity. Applicable ESBWR specific procedures, if available, are used as necessary when simulating validation scenarios. Non-ESBWR procedures and/or the experience of test subjects and participants can also be used. Some Integrated System Validation can be conducted without operating procedures. For example, validation of display navigation and validation of HSI component layouts on consoles are not dependent on operating procedures and scenario simulations.

A standard design feature of the ESBWR is the Safety Parameter Display System (SPDS) function integrated into the MCR HSI as displays and fixed-position indicators at the Wide Display Panel. Validation demonstrates that the ESBWR SPDS aids operators during abnormal and emergency conditions in (a) determining the unit safety status, (b) assessing whether abnormal conditions warrant corrective actions by operators to prevent core damage, (c) monitoring the impact of engineered

safeguards or mitigation activities, and (d) executing symptom-based emergency operating procedures.

#### 4.11.10.3.3.5 Detecting Human Error

Errors are detected by comparing operator actions (observed and recorded) to reference (predefined) responses. Observed and recorded actions include crew communications and test subjects describing their observations and intended actions during the testing.

Documented PRA/HRA assumptions regarding operator performance and the HSI are validated. The assumptions relate to the tasks definition, time allowed for each task, and the probability of operator success to perform the task in the allowed time. The following are samples of assumptions:

1. Intentional deviation from standard operating procedures is due to misdiagnosis or misleading indication and operator discretionary decision to deviate.
2. Procedures exist for providing backup DC power to ADS valves under station blackout conditions.
3. Per-control-room staffing is:
   (a) Unit MCR Shift Supervisor (available within 10 minutes)
   (b) Unit MCR Senior Reactor Operator
   (c) Unit MCR Reactor Operator
   (d) Unit Auxiliary Operator
   (e) Unit Equipment Operators (two)
4. Procedures are available in a clear written form.
5. Information is available to help operators diagnose events and carryout mitigating actions for those credited in the PRA.
6. Accessibility of control is available for successful action in an appropriate time frame.

#### 4.11.10.3.3.6 Evaluating Situation Awareness

The HSI is an integration of proven technologies based on human factors principles and human-centered automation. Validation to confirm situation awareness does not require defining or developing a cognitive model. Instead, simulated operator test scenarios inherently involve many features of the HSI that reinforce situation awareness. Operator situation awareness is qualitatively evaluated based on acquired test data (recordings and observations). Test data is expected to provide evidence regarding whether or not (a) mental and physical tasks are within operator performance capabilities, (b) situation awareness and vigilance is acquired and

maintained, and (c) potentially new types, and possibilities, of human error are not being introduced.

Situation awareness is evaluated using a method similar to the Situation Awareness Control Room Inventory (SACRI) method developed by OECD Halden Reactor Project of Institutt for Energiteknikk. The SACRI method is based on the Situation Awareness Global Assessment Technique (SAGAT) used in the aviation industry. A simulated scenario is suspended at selected points unbeknown to the operators. Operators are requested to turn away from displays and answer questions (about process parameters) deemed highly relevant to situational awareness. The questions concern the qualitative status of each parameter (e.g., increasing, decreasing, no change) over time (past, present, and future). Examples of questions: Compared to initial water level, how has water level changed? Compared to expected water level under normal conditions, how has current water level changed? Compared to the current water level, what do you expect to happen to water level? Supplementary information to support the assessments is obtained by questioning the operators (during the suspended scenario) on how they perceive the different situations with respect to their task objectives. Operators can be "walked back through" the scenario at a slower pace. The recorded operator responses are compared to time-tagged simulator data logs to assess correctness, gauge operator situational awareness, and critique crew performance.

Equally important (as HSI design) to situation awareness (and reliable operator performance in general) are training and procedures. The following are undertaken to promote and maintain situation awareness:

- Using simulators to test for overdependence on automation (i.e., identify conditions when operators are reluctant to act despite being certain about abnormal conditions). The goal of such tests is to encourage operator discretion, reinforce the operator being "in the loop", promote learning from potential mistakes, and motivate operators to learn by giving them the opportunities to experiment.
- Training operators on what the automation does, both well and not well, and what the automation does not do. This includes understanding the operator's supervisory, or mission manager, decision-making role.
- Confirming adherence to procedures expressly developed for effective transfer and communication of unit information during shift changeovers.

#### 4.11.10.3.3.7 Assessing Operator Workload

Workload (physical and cognitive) concerns the magnitude of task loading placed on operators during operational conditions (normal and abnormal). Operator

performance could be adversely impact if processing and response task demands of the system exceed operator capacity to perform the tasks. Workload is a function of:

- Time available to complete the tasks
- The number of tasks
- Task duration
- Task difficulty

Workload assessment methods are discussed in the Task Analysis Implementation Plan.

#### 4.11.10.3.3.8 Evaluating Crew Communication and Coordination

Crew communication and coordination are subjectively evaluated on the basis of the crews' demonstrated performance during training exercises (e.g., emergency response drills).

Inoperable communication equipment (phone, radio, page party, public address) is installed in the simulator at the site. This is the first opportunity to evaluate the equipment for effective integration with the MCR panel arrangement and work environment. Operable communication equipment is installed in the Unit 1 MCR panels at the site. Evaluating use of the operable equipment with plant staff outside the MCR is part of the Final HFE/HSI Design Verification activity.

#### 4.11.10.3.3.9 Validating Anthropometrics

Anthropometrics are validated as part of the performance evaluations using test scenarios. Additional, predefined scenarios and tasks are used (as necessary) to ensure coverage of all HSI components. The validation relies on detecting problems (during use of the HSI) that may not have been evident when HSI components were verified without reference to specific tasks.

#### 4.11.10.3.3.10 Evaluating Automation

Automation is evaluated for human-centered automation principles as part of the performance evaluations using test scenarios. Additional, predefined scenarios and tasks are used (as necessary) to ensure coverage of automation features and modes.

#### 4.11.10.3.3.11 Validating Operating Procedures

Initial validation of hardcopy SOPs is performed with the GETS. The validation is partial because it is limited to examining consistency between operator display content and those procedure steps involving use of displays.

Validation of hardcopy procedures continues with the BS and the FSS. The validation is more structured and comprehensive because it is conducted under defined test conditions (scenarios or situations) and it includes other procedures (i.e., IOP, AOP, EOP, ARP) and the remaining HSI components (hard switches, alarm tiles, mimic, etc.). Validation of procedures (hardcopy and electronic) is completed during operator training phases on the BS and FSS. The procedures are adapted and finalized for implementation in the MCR and the simulator procedure computerized system (i.e., in OLPS) before plant start up.

Validation confirms that a portable cart for hardcopy procedures and a portable utility board for EOP flowcharts effectively integrate with the MCR arrangement and work environment. The top surfaces of the Main Control Console and Shift Supervisor Console are purposely designed for layout of multiple drawings and procedures. However, a portable (e.g., wheeled), dual-sided utility board is one option considered for mounting EOP flowcharts in the MCR. The side not used for mounting flowcharts can be a whiteboard for shift turnover information purposes. This option can be validated during procedure validation activities with the BS and the FSS.

#### 4.11.10.3.3.12 Validating Displays Using GETS

The qualitative validation of display usability is referred to as a Dynamic Walkthrough. Initial Dynamic Walkthroughs are one-system-at-a-time evaluations for normal operational sequences using the respective System Operating Procedure (SOP) as a guide for task execution. These initial walkthroughs do not address integrated system operation or abnormal operations.

#### 4.11.10.3.3.13 Validating Displays Using BS and FSS

Display validation with the BS is similar to previous Dynamic Walkthroughs except that the displays are evaluated under use simulator exercises (Normal Evolutions, Malfunctions, Surveillances, Transients, and Automatic actions).

#### 4.11.10.3.3.14 Validating Displays Without Simulation

The simulator will not have prototypic operator displays for the certain site-specific systems until ESBWR displays are available for installation in the simulator:

Auxiliary Fuel Pool Cooling & Cleanup
BOP Liquid Sampling and Analysis
Reactor Building Sampling
Filter/Demin Resin Transfer
Breathing Air
Flammability Control
Switchgear Building HVAC
Hot Machine Shop HVAC

Radioactive Waste Tunnel HVAC
Auxiliary Fuel Building HVAC
Pump House HVAC
Electrochlorination Building Ventilation
Circulation Water Pump House Ventilation
Electrochlorination

Once installed in the simulator, the Unit 1 displays for these systems are driven with "dummy" variables. Validation of systems that are not simulated therefore occurs after the systems are installed at the site and testable. The scope of validation may be strictly limited to features conducive to reasonable and necessary modification at that stage.

#### 4.11.10.3.4 Test and Evaluation (T&E) Conditions

Scenario selections are based upon the requirements specified in Section 4.1. Specific HSI equipment failure scenarios consider input from PRA/HRA and supporting reliability analyses.

##### 4.11.10.3.4.1 GETS

The T&E conditions are one-system-at-a-time evaluations against normal operational sequences.

##### 4.11.10.3.4.2 BS

The T&E conditions are those of the normal evolutions, malfunctions, surveillances, transients, and automatic actions, for the simulator testing program.

##### 4.11.10.3.4.3 FSS

[ To be included in a future revision of this document. ]

#### 4.11.10.3.5 Acceptance Criteria

##### 4.11.10.3.5.1 Operational Safety and Task Performance

Acceptable human performance is based, in part, on success with the measures for operational safety and task performance.

##### 4.11.10.3.5.2 Human Error

Acceptable human performance is partly based on successful operator performance with respect to human error performance measures. Acceptable HSI performance is partly based on the HSI not being a root cause of operator failure with respect to human error performance measures.

##### 4.11.10.3.5.3 Situation Awareness

An acceptable level of situation awareness is based, in part, on operator success with the performance measures for situation awareness.

#### 4.11.10.3.5.4 Operator Workload

An acceptable workload would be the result of:

- Positive ratings by crews
- Successful accomplishment of needed operator tasks in time and precision
- Adequate situation awareness (as more workload implies less situation awareness or less time available to assess plant situations)

The Task Analysis Implementation Plan cites 50% to 75% as a "rule of thumb" acceptable average physical workload [(time occupied / task time) * 100]. Meister notes that, although supporting empirical data is lacking,

- Physical workloads of 75-100% are undesirable
- Physical workloads <75% are acceptable provided the operator remains reasonably occupied
- Inaccuracy of most physical workload estimates is +/- 20%
- Physical workload estimates are to be used to investigate potential improvements (e.g., to HSI, to procedures, to training, etc.) rather than reject the design.

#### 4.11.10.3.5.5 Crew Communications and Coordination

Acceptable human performance is based, in part, on operator success with the performance measures for crew communication and coordination.

#### 4.11.10.3.5.6 Anthropometrics

The acceptance criteria are the same as those used for HFE Design Verification.

#### 4.11.10.3.5.7 Automation

Human-centered automation is automation to any extent provided that safe, economic plant operation and maintenance remain within the capabilities of the operators and maintainers. Acceptance of the integrated HSI is based, in part, on the HSI exhibiting the following general human-centered automation design principles:

| OPERATOR (or MAINTAINER) | AUTOMATION |
|---|---|
| • Retains ultimate authority and decision-making responsibility | • Facilitates control and operation in appropriate modes (full auto, semi-auto, manual) and at appropriate levels (plant, system, component) |
| • Remains involved and is able to accomplish tasks within time, performance, and workload criteria | • Provides quality, timely information. |

| | |
|---|---|
| • Is well-informed | • Provides task-relevant information, and explains actions (taken, pending, anticipated) |
| • Is able to effectively anticipate problems | • Supports a high degree of operator vigilance and "situation awareness" (e.g., monitors trends, aids operator decision-making, and provides fault detection, identification, verification, and recovery) |
| • Understands the automation | • Is human-engineered for simple, cognitive, and intuitive operation (i.e., low probability of human error) |
| • Is able to manage task support resources | • Effectively integrates task support resources and the HSIs for NSSS, BOP, and T/G |

#### 4.11.10.3.5.8 Operating Procedures

Acceptance criteria for operating procedures includes:

- Correct execution of the procedure meets the intended purpose of the procedure
- Procedures are conveniently accessible and retrievable
- EOPs can be navigated effectively
- ARPs meet the criteria of NUREG-0700, Section 4.9
- Electronic procedures aid the operator
- User acceptance

#### 4.11.10.3.5.9 Validating Displays Using GETS

The acceptance criteria for operator displays on the GETS is:

The displays enable normal operating procedure tasks to be accomplished effectively, and

Displays are complete.

- There is good 1-to-1 correspondence with operating procedure tasks and information, and
  - System process images correlate well with P&IDs, PFDs, and DCTs.

Displays are compatible with operators (and other applicable end users).

- Readable

- Touchscreens work effectively
- Active touch areas are suitably sized
- Easy to navigate
- Multiple FPDs can be used simultaneously

Displays are understood by the operator (and other applicable end users).

- Consistent "look and feel"
- Colors and color coding scheme are effective
- Dynamic behaviors are easily recognized and understood
- Appropriate units, number of significant digits, decimal places
- Easy to learn

Displays are not a cause of human error.

Display operability is validated and includes aspects such as;

- Effective control using on-screen Manual/Auto (M/A) stations
- Clear status feedback (e.g., valve open/closed, pump on/off, etc.) from color coding and labeling
- Ability to abort actions or retract inputs without adverse effects
- Navigation features function effectively
- Touch screen responsiveness and ease of selecting touch points correctly

#### 4.11.10.3.5.10 Validating Displays Using BS and FSS

The acceptance criteria for operator displays on the BS and FSS is the same criteria as displays on the GETS with the additional criteria that the displays enable abnormal and emergency procedure tasks to be accomplished effectively.

Acceptance criteria for SPDS displays is compliance with Paragraph 3.8a of NUREG-0737 (Supplement 1) including incorporation of applicable results of ESBWR PRA/HRA, and that SPDS is addressed in training programs for abnormalities and emergencies.

### 4.11.10.3.6 Performance Measures

Performance measures cover human performance and HSI performance.

#### 4.11.10.3.6.1 Operational Safety and Task Performance

Human performance measures include:

- Error avoidance
- Avoiding alarm conditions
- Avoiding technical specification violations
- Response time
- Task completion time
- Procedure compliance

#### 4.11.10.3.6.2 Human Error

Human errors in various industries (e.g., power generation, aerospace, naval, communication) fit six general categories as follows:

1. Observing the state of the unit or system
2. Diagnosis (making hypotheses, judgments, assumptions, guesses)
3. Testing their diagnosis
4. Deciding on their goal/objective
5. Selecting a procedure
6. Executing a procedure (adhering to instructions and executing the tasks)

The errors are errors of commission (i.e., doing what should not have been done) and errors of omission (not doing what should have been done). Failures to perform the tasks listed in the situation awareness section are examples of errors.

#### 4.11.10.3.6.3 Situation Awareness

Situation awareness is subjectively evaluated partly on the basis of the correctness of test subject responses to questions asked during test scenarios. Situation awareness is also subjectively evaluated on the basis of how well crews exhibit the following skills and capabilities:

- Locating and interpreting information correctly and efficiently to ascertain vital symptoms and system status
- Properly assessing the implications of alarm states
- Demonstrating an understanding of how the plant, systems, and components were operating, and the status of key setpoints, interlocks, and automatic actions
- Demonstrating an understanding of how their actions (or inaction) affected the plant and individual systems (including discretionary decisions to assume manual control)

Measures of performance are the operator's effectiveness at tasks that include:

Observing the state of the unit or system

- Recognizing off-normal trends before the onset of a significant upset condition

Diagnosis (making hypotheses, judgments, assumptions, guesses)

- Classifying symptoms and events correctly
- Diagnosing conditions in a timely and accurate manner
- Use of information and reference material (drawings, books, charts, emergency response procedures, etc.) appropriately and effectively

Testing a diagnosis

- Informing others of intended action and executing appropriate if-then-else steps in abnormal operating procedures

Deciding on a goal/objective

- Making decisions correctly (e.g., while following emergency procedures)

Selecting a procedure

- Referring to, and transitioning between, the appropriate procedures in a timely manner

Executing a procedure (with or without OLPS)

- Strict adherence to procedures, cautions, and limitations (i.e., no deviating even if the deviation appears to have no detrimental consequences)
- Executing procedural steps in correct sequence
- Locating and accessing controls and information correctly and efficiently
- Using controls in a timely and effective manner

#### 4.11.10.3.6.4 Operator Workload

Data acquired from test scenarios is analyzed to determine physical workloads that are *average* workloads per task over defined task time periods. Cognitive workload is evaluated qualitatively using a rating method that considers operator views of task loading and difficulty, and actual operator performance during test scenarios.

Workload is assessed from test scenarios by means of:

- Evaluating navigation, which includes all actions indicating that the operator actively searches and answers demands from the system, or follows procedure logic.
- Evaluating information gathering, which includes the monitoring of plant parameters to evaluate plant status, depending on the plant situation.
- Evaluating plant operations, which include all actions that have a direct effect on the simulated process (opening or closing valves, or switching on/off automatic programs.
- Evaluating alarm interaction, which involves acknowledging incoming alarms.
- Analyzing the information that is needed to assess plant situation and step logic while performing other activities per task over defined task time periods
- Analyzing the memory demands to perform operational tasks
- Evaluating the crew's subjective ratings (an output from questionnaires and interviews concerning task loading, difficulty, and operator performance during test scenarios)
- Evaluation of results using crew ratings that are composed of six factors: mental demand, physical demand, temporal demand, own performance, own effort and own frustration

#### 4.11.10.3.6.5 Crew Communications and Coordination

Crew communication and coordination are subjectively evaluated on the basis of how well crews exhibit the following:

- Effective leadership and clear chain of command. Cooperation and composure under supervisor's direction without micromanagement.
- Well-defined roles and responsibilities
- Teamwork. The crew performs as an integrated unit and interacts effectively (i.e., everyone contributing, supporting and backing each other up as needed, ease of task delegation, using a consensus approach to problem solving and decision making, informing key personnel outside the control room)
- Open dialogue (sharing information and knowledge)
- Use of same information (displays, alarms, procedures)
- Clear directions and repeatbacks (confirmations, acknowledgements)
- Correct, accurate, concise, and relevant information exchange (e.g., always designating the specific unit, division, train, etc.)

- Proactive monitoring and observation (for situation awareness and progress assessment)
- Efficient movement between panels and workstations

#### 4.11.10.3.6.6 Anthropometrics

The performance measure primarily concerns reachability and operability of controls, and viewability of indicators, from the expected user position(s). Variability of the task execution envelope is investigated if interference among users occurs.

#### 4.11.10.3.6.7 Automation

Performance measures include:

1. Operability (i.e., effective operator use) of PAS during automation modes (startup from cold shutdown or hot shutdown conditions to rated power operation, power maneuvers in the normal operating range, and shutdown from rated power level to shutdown of the turbine gland sealing system).
2. Operator cognition (e.g., mode awareness)
3. Correct confirmations during pre-programmed automation break points

#### 4.11.10.3.6.8 Operating Procedures

Refer to operator performance measures regarding situation awareness.

#### 4.11.10.3.6.9 Display Validation

There are no performance measures for graphical displays because the behavior of the graphics is a function of software programming, hardware performance, and overall system throughput and response.

### 4.11.10.3.7 Data Collection and Analysis

Validation activities with the BS and the FSS use the following:

- Videotaping and data collection forms
- Interviews using the NASA Task Load Index (TLX) to supplement analytic data.
- Questionnaires
- Simulator recording of chronological event logs (e.g., operator actions with screen displays and hard controls, occurrence of alarms, etc.)
- Simulator recordings (logs) of process variables
- Written observations, notes and commentary

Validation activities with the FSS also use the following:

- Operator activity timelines of expected operator tasks (developed in advance based on TA and PRA/HRA to identify periods of overloading and underloading). The timelines show phasing, frequency, durations, and time limits for tasks. Other actions (reactions to secondary effects, diagnostic actions), if defined, can be included in the timeline. These timelines become baselines for expected operator task execution.
- Expected operator movement pattern diagrams (developed following validations with the BS) to establish a baseline movement pattern for each scenario. Only the most essential key actions are reflected in these movement pattern diagrams.

Time data (measured, calculated and estimated) includes:

- Elapsed time from occurrence of first alarm to awareness of that alarm
- Elapsed time from first significant alarm to first manual safety-related action
- Time used to navigate to the appropriate screen display
- Time used to find and access the correct procedure (hardcopy and electronic)

Timelines and movement pattern diagrams for each crew are developed for each simulated scenario. Movement pattern diagrams are constructed from video recordings and visual observation records. Timelines and movement pattern diagrams are compared against baseline timelines and movement pattern diagrams to assess correctness, timeliness, and completeness of responses to scenarios. Findings are compared to performance criteria and requirements. Tests subjects support the evaluation team by interpreting videotaped sessions and interrelating recorded events with test data.

Human errors are analyzed for root cause.

#### 4.11.10.4 Documentation and Integration of Results

1. Design specifications, procedures, training, etc., are revised accordingly, if necessary, to reflect the validation results.
2. Results can be used to modify baseline timelines and movement pattern diagrams for use as operator training tools and baseline Human Performance monitoring.
3. Reports include discussion of the type and frequency of human errors detected, error consequences, root cause analysis of errors, and corrective measures to address the errors.
4. Multimedia records are retained in accordance with GEEN QA.
5. Deficiencies identified by evaluators are documented (HEDs). A deficiency is logged into the HFEITS if it matches at least one of the HFE issue entry criteria.

## 4.12 Implementation of Human Factors Issue Resolution Verification

### 4.12.1.1 Scope

The verification applies principally to significant issues in the HFEITS requiring resolution (i.e., those with potential for risk-significant human error and adverse impact on plant safety or performance).

### 4.12.1.2 Objectives

The objective is to ensure that issues are acceptably resolved and corrections are implemented (if applicable).

### 4.12.1.3 Participants, Test Subjects, and Observers

GE, as custodian of the HFEITS, performs verification for the issues that are resolved prior to plant start-up. *COL Holder* performs verification of any issues thereafter. The HFEITS is expected to support a wide variety of plant upgrades. Such modernization upgrade programs may implemented in a wide range of ways including: many small modifications at one time, large modifications during multiple outages, both old and new equipment left in place, and new non-functional HSIs are in place in parallel with old functional HSIs. .

### 4.12.1.4 Methods and Procedures

Verifications by GE are performed in accordance with the GEEN QA requirements.

### 4.12.1.5 Test and Evaluation (T&E) Conditions

Not applicable.

### 4.12.1.6 Acceptance Criteria

Acceptance is obtained through formal design change and verification processes in accordance with QA requirements and program requirements specified in Section 3. For significant issues, the criteria for acceptance includes

- Reducing, or eliminating, the potential for risk-significant human error and adverse impact on plant safety or performance
- Engineering independent review determines the resolution to be adequate
- Approval by licensee and licensor

### 4.12.1.7 Performance Measures

Not applicable.

### 4.12.1.8 Data Collection and Analysis

Not applicable.

#### 4.12.1.9 Documentation and Integration of Results

HFEITS contains traceable references to resolutions and implementation.

### 4.12.2 Implementation of Final Plant HFE/HSI Design Verification

#### 4.12.2.1 Scope

The scope of Final Plant HFE/HSI Design Verification includes the following:

- MCR facility layout/arrangement
- RSS facility layout/arrangement
- MCR facility layout/arrangement
- Tagout facility
- Communication equipment (phones, radios, intercoms, etc.)
- Lighting (normal and emergency)
- Habitability systems (HVAC, noise mitigation features, etc.)
- Floor design
- Peripherals (e.g., printers, utility tables)
- Training manuals
- Staffing and room occupancy [*COL Applicant responsibility*]
- Shift rotation [*COL Applicant responsibility*]
- Data and video interfaces with the TSC, and equipment to duplicate or link the EOF to the plant process database

#### 4.12.2.2 Objectives

The objectives are to verify

- Those aspects of the design that are either partially verified or not verified at all prior to the FSS becoming operational at the site
- That the "as built" HSI designs are consistent with final design specifications, user/trainee manuals, and procedures (operating, maintenance)
- The final MCR, RSS, and LCS layouts
- Any design modifications (e.g., display changes) resulting from pre-operation and startup testing
- Resolution of any open HFE issues
- That the final installed design and its performance criteria are described and documented

#### 4.12.2.3 Participants, Test Subjects, and Observers

[To be included in a future revision of this document. ]

#### 4.12.2.4 Methods and Procedures

##### 4.12.2.4.1 MCR Facility Layout/Arrangement

Facility layout and arrangement are verified against HFE guidelines such as those in NUREG-0700, Section 7.2, taking into account maximum occupancy (e.g., during shift turnovers).

##### 4.12.2.4.2 RSS Facility Layout/Arrangement

Facility layout and arrangement are verified against HFE guidelines such as those in NUREG-0700, Section 7.2, taking into account maximum expected staffing (e.g., for a control room evacuation scenario or an emergency shutdown scenario).

##### 4.12.2.4.3 MCRBP Facility Layout/Arrangement

Facility layout and arrangement are verified against HFE guidelines such as those in NUREG-0700, Section 7.2, taking into account maximum expected staffing (e.g., during startup, outages, transient and emergency situations).

##### 4.12.2.4.4 Tagout Facility

Facility layout and arrangement are verified against HFE guidelines such as those in NUREG-0700, Section 7.2, taking into account maximum expected staffing (e.g., during startup, outages).

##### 4.12.2.4.5 Communication Equipment

Communication equipment is verified against HFE guidelines such as those in NUREG-0700, Section 6 and Section 8.4.

##### 4.12.2.4.6 Lighting

Lighting is verified against HFE guidelines such as those in NUREG-0700, Section 7.3 and Section 8.5.

##### 4.12.2.4.7 Habitability Systems

Habitability is verified against HFE guidelines such as those in NUREG-0700, Section 7.3 and Section 8.5.

##### 4.12.2.4.8 Floor Design

Floor design is verified against HFE guidelines such as those in NUREG-0700, Section 7.3.7.

#### 4.12.2.4.9 Peripherals

Peripherals are verified against HFE guidelines such as those in NUREG-0700, Section 7.2. The verification confirms that peripherals effectively integrate with the arrangement and work environment.

#### 4.12.2.4.10 Training Manuals

Verification of training manuals is a check that HSI component descriptions/discussions in the manuals are consistent with the as-built design.

#### 4.12.2.4.11 Main Control Room Staffing and Occupancy

Verifications are made of the adequacy of MCR staffing under different conditions (i.e., nominal and minimal staffing levels during startup/shutdown, outages, transient and emergency situations) and the ability of the main control area to accommodate a larger operating staff when necessary (e.g., shift turnovers). The ESBWR shift composition provided in Table 6 is considered for defining the validation test conditions.

#### 4.12.2.4.12 RSS Staffing and Occupancy

Staffing and occupancy are verified based on a maximum expected staffing (e.g., for a control room evacuation scenario or an emergency shutdown scenario).

#### 4.12.2.4.13 Shift Rotations

[To be included in a future revision of this document. ]

#### 4.12.2.4.14 Interfaces with the TSC and EOF

HSI-related interfaces with the TSC and EOF are verified during integration tests at the site. The verification checks that the interfaces support the plant's emergency response plan as follows:

1. Interfaces with the MCR functionally support the plant's emergency rotation procedure.
2. Data interfaces support display of important rotation parameters.
3. Communication systems work effectively with other emergency response operation sites.
4. Interfaces with the MCR facilitate storage of related document data.
5. The interfaces support TSC functions prior to completion of mobilization of other operation sites.

### 4.12.2.5 Test and Evaluation (T&E) Conditions

[To be included in a future revision of this document. ]

#### 4.12.2.6 Acceptance Criteria

The acceptance criteria are satisfactory compliance with HFE guidelines such as those in NUREG-0700.

#### 4.12.2.7 Performance Measures

Performance measures are embodied in requirements contained in design specifications.

#### 4.12.2.8 Data Collection and Analysis

Verifications are recorded on checklists.

#### 4.12.2.9 Documentation and Integration of Results

Deficiencies identified by evaluators are documented. A deficiency is logged into the HFEITS if it matches at least one of the HFE issue entry criteria.

### 4.12.3 Implementation of HFEITS

The HFEITS tool is a Microsoft Access database. Records within the database include the following (as fields within a record). An example of an HFEITS database record is:

1. HFE Issue tracking identifier
2. Design lifecycle process (or activity thereof) that led to the issue being identified
3. Area (of MCR, RSS, Simulator, or LCS) affected by the issue
4. HFE principle or guideline pertinent to the issue (e.g., workspace, legibility, screen content, etc.)
   - 4a. Plant system(s) affected
   - 4b. Control panel(s) affected
   - 4c. Component(s) or feature affected (e.g., switch, mimic, display, lighting)
   - 4d. Operator task(s)/function(s) affected
   - 4e. Human performance characteristic affected (e.g., vision, hearing, cognitive, motor skill, etc.)
5. Date that the issue was identified
6. Brief description of the issue
7. Name of person (or group, or organization) identifying the issue
8. Qualified evaluator's "Yes/No" designation that the issue requires corrective action
9. Qualified evaluator's justification statement if no corrective action is needed

10. Date when the need for corrective action was evaluated
11. Name of the qualified evaluator
    11a. Significance Category (*Clarification noted below*)
12. Description of the proposed corrective action
13. Date that the corrective action was proposed
14. Name of engineering discipline responsible for proposed corrective action
15. Organization responsible for evaluation of proposed corrective action
16. Date that the evaluation was completed
17. Statement (and/or summary of findings) confirming completion of corrective action
18. Name of person confirming completion of corrective action
19. Date of confirmation statement
20. Name of HFE Group Member authorized to signify that the issue has been closed
21. Date of closure

Significance Category is a temporary field for potentially future HED compilation, ranking and screening purposes. It is a methodology to rank or prioritize new and unresolved in terms of their significance and potential impact on plant safety and performance. The intent is to facilitate evaluation and resolution of in a manner consistent with the guidelines of NUREG-0700 and NUREG 0711. The Significance Category methodology is depicted in Figure 10. It is modeled after a methodology described in Section 4.2 of NUREG-0801 (Evaluation Criteria for Detailed Control Room Design Review (DCRDR), Draft Report for Comment, October 1981, USNRC).

The Human Factors Verification & Validation Plan, in Section 2.1.128, will establish:

1. The methods and criteria for conducting the Human Factors V&V in accordance with accepted human factors practices and principles;

2. That scope of the evaluations of the integrated M-MIS will include:

    a. The HSI (including both the interface of the operator with the M-MIS equipment hardware and the interface of the operator with the M-MIS equipment software functions)

    b. The Plant and Emergency Operating Procedures

c. The HSI work environment

3. That evaluations of the HSI equipment will be conducted to confirm that the controls, displays and data processing functions identified in the task analyses are provided;

4. That integration of M-MIS equipment with each other, with the operating personnel and with the Plant and Emergency Operating Procedures will be evaluated through the conduct of dynamic task performance testing. The dynamic task performance tests and evaluations will have as their objectives:

   a. Confirmation that the identified critical functions can be achieved using the integrated M-MIS and HSI design;

   b. Confirmation that the M-MIS and HSI design and configuration can be operated using the established MCR staffing levels;

   c. Confirmation that the Plant and Emergency Operating Procedures provide direction for completing the identified tasks associated with normal, abnormal, and emergency operations;

   d. Confirmation that the time dependent and interactive aspects of the HSI equipment performance allow for task accomplishment;

   e. Confirmation that the allocation of functions is sufficient to enable task accomplishment;

5. That dynamic task performance test evaluations will be conducted over the range of operational conditions and upsets;

6. The HFE performance measures to be used as the basis for evaluating the dynamic task performance test results. These performance measures will address:

   a. Operating crew primary task performance characteristics, such as task times and procedure compliance;

   b. Operating crew errors and error rates;

   c. Operating crew situation awareness;

   d. Operating crew workload;

   e. Operating crew communications and coordination;

f. Anthropometry evaluations;

g. M-MIS equipment performance measures;

7. The methods to confirm that HFE issues identified and documented have been resolved in the integrated M-MIS design;

8. The methods and criteria to be used to confirm that critical human tasks, as defined by the task analysis, have been addressed in the integrated M-MIS design.

*See also Appendix B for a draft outline of this plan.*

# 5 Design Implementation Process, HFE Infrastructure (Hardware and Software)

Both GE and the COL Applicant carry out the design implementation. The implementing organizations execute their responsibilities under the plans described herein. The design implementation, startup and operation duties of the COL Holder include aspects of these plans which are transferred to the COL holder under their license obligations to ensure the integrity of the HFE infrastructure is maintained throughout the life cycle of the plant.

## 5.1 Software Quality Program For Hardware/Software Design and Development

Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7 4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," provides guidance for complying with requirements for safety systems that use digital computer systems. Branch Technical Position HICB-14 (BTP-14) outlines the many activities to be considered when constructing a software development program for software-based control and instrumentation (C&I) system, herein refers to as software-based product. BTP-14 divides these activities into 11 separate software development plans. The overall requirement is that the essential elements of each of the 11 development groups are addressed and documented. GE has developed and accumulated the experiences and documentation of various aspects of the software development plans called out in BTP-14, in GE's design work of software-based products in current products including that of advanced reactor. The ESBWR software development program will be developed using GE's current software development plans as bases. The development of the plans will address various aspects of the software development and quality addressed in the guidance documents of various related industry standards and regulatory guides. While deviations may be

taken from the detailed requirements described in those guidance documents, the process outlined herein will be followed. The development activities to be implemented for ESBWR safety-related software-based products with documentation in the following subject areas:

The described development work and available documentation demonstrate how the ESBWR safety-related software development process intends to meet the requirements of BTP-14.

- Software Quality Assurance
- Software Management Plan
- Software Development Project plan
- Software Configuration Management Plan
- Verification and Validation Plan
- Software Safety Plan (SSP)
- Software Test Plan (SVTP)
- Operations and Maintenance Manual

*See also Appendix B for draft outlines of representative plans.*

### 5.1.1 Software Quality Assurance Program

The Software Quality Assurance Program (SQAP) outlined below describes a systematic approach to the development and use that will be implemented for ESBWR software development. It also identifies the documentation to be prepared during the software development, verification, validation, use, and maintenance phases conforms to the requirements of 10 CFR 50, Appendix B and is consistent with the requirements specified in IEEE-730, "IEEE Standard for Quality Assurance Plans".

The SQAP outline in conjunction with other plans described herein addresses the various elements described in the related guidance documents including IEEE-730. The SQAPdefines the quality assurance management of the software-based product including:

(1) The organizational structure that influences and controls the quality of the software. The SQA organization shall maintain independence from the development organization.

(2) The organizational boundaries between the software QA organization and other company organizations.

(3) The responsibilities and authority of the software quality organization, and identify the specific organizational elements responsible for each task (i.e., configuration management, V&V, safety analysis, etc).

(4) Tasks to be performed, with special emphasis on software quality assurance activities for each software life cycle phase (described in the Software Management Plan) include:

- Defining the documentation governing the development, verification and validation, use, and maintenance of the software-based product and stating how these documents are to be checked for adequacy, and identifying the documentation needed to ensure that the software implementation satisfies requirements.
- Defining the standards, practices, conventions and metrics to be applied and how compliance with these requirements is to be monitored, and how traceability is maintained and assured through all phases of the software life cycle.
- Defining the reviews and audits to be conducted and accomplished, such as but not limited to: software requirements review, software design review, managerial reviews, functional audits and in-process audits and if applicable, defining further actions required and how they are to be implemented and verified.
- Describing the practices and procedures to be followed for reporting, tracking, and resolving problems identified in both software development and maintenance process.
- Identifying the special software tools, techniques, and methodologies that support SQA.
- Defining the methods used to control and secure the software source code and software media.
- Defining the provisions for assuring that software provided by suppliers through purchase meet the established requirements; and assuring SQAP covers the proper methods used to assure the suitability of previously-developed software.
- Identifing the SQA documentation to be retained, the retention period, and the methods and facilities to be used to assemble, safeguard, and maintain this documentation.

### 5.1.2 Software Management Plan

The Software Management Plan (SMP) outlined below describes the management of the software development in accordance with Reg. Guide 1.173, "Development Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants". This outline in conjunction with other plans described herein addresses the various elements described in the related guidance documents including Reg. Guide 1.173.

The SMP defines:

(1) The Organizational Structure describing the boundaries, interfaces and responsibilities for development of the software design.

(2) The Management Plan activities in:

a. Software developed by subcontractors;

b. Procedures to be used in the software development

c. The interrelationships between software design activities;

d. Security to provide assurance that the integrity of the software product is maintained, and to provide methods to be used to prevent contamination of the developed software by viruses;

e. Adaptation of previously developed software;

f. Use of commercial off-the-shelf software (COTS);

g. System for collection of software metrics and using them to improve processes and software quality.

(3) The software engineering process, which is composed of the following life-cycle phases:

a. The Planning Phase. The planning phase design activities address the following system design requirements and software development plans and review report:

- Software Management Plan
- Software Development Project Plan
- Software Configuration Management Plan
- Verification and Validation Plan
- Equipment design requirements

- Disposition of design and/or documentation of non-conformances identified during this phase

b. The Design Definition (Requirements) Phase. Design Definition (Requirements) Phase design activities address the development of the following equipment design and configuration requirements in accordance with Reg. Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." The design and review activities are documented in the following documents and drawings, analysis and review reports:

- System Requirements Specification
- Equipment schematic, if necessary
- Equipment hardware and software performance specification
- Equipment user's manual (Operation and Maintenance Manual)
- Data communications protocol
- Safety analysis of the developed design definition
- Disposition of design and/or documentation of non-conformances identified during this phase

c. The Software Design phase. The Software Design phase addresses the design of the software architecture and program structure elements, and the definition of software module functions. The design and review activities are documented in the following documents, analysis and review reports:

- Software Design Specification
- Safety analysis of the software design
- Disposition of design and/or documentation of non-conformances identified during this phase

d. The Software Coding phase. The Software Coding phase activities address the implementation and testing of software design. The implementation and review activities are documented in the following documents, analysis and review reports:

- Software source code listings
- Software module test reports
- Safety analysis of the software coding

- Disposition of non-conformances identified in this phase's design documentation and test results

e. The Integration Test Phase. Integration test phase describes the integration process and addresses the equipment testing activities that evaluate the performance of the software being installed in prototype hardware. The installation shall be performed in accordance with defined methods and procedures. The test and review activities are documented in the following analysis and review reports:

- Installation and Integration test reports
- Safety analysis of the integration test results
- Disposition of non-conformances identified in this phase's design documentation and test results

f. The Validation Test Phase. Validation test phase activities address the V&V testing activities that demonstrate that the software-based product is operational and conforms to all functional and performance requirements as defined in the Design Definition phase. The test and review activities are documented in the following analysis and review reports:

- Validation test plans and procedures
- Validation test reports
- Description of as-tested software
- Safety analysis of the validation test results
- Disposition of non-conformances identified in this phase's design documentation and test results

g. The Change Control Phase. The Change Control phase begins with the completion of validation testing. It provides a controlled path through the design process (operation) that may be invoked when software modification is required.

### 5.1.3 Software Development Project Plan (SDPP)

Software Development Project Plans outlined below define the managerial processes necessary to accomplish the design and development of the ESBWR software-based products. Software Development Project Plans are developed as a supplemental document to the SMP. This outline in conjunction with other plans described herein addresses the various elements described in the related guidance documents including IEEE-1058.1. Software Development Project Plans are used as a tool to aid, as a

minimum, the following project management activities and as such may be updated throughout the course of the project:

The SDPPs:

(1) Establish the project goals, deliverables and principle work packages;

(2) Establish schedules and milestones for each project deliverable and work package;

(3) Coordinate between ESBWR project team and interfacing organizations including subcontractors responsible for software development;

(4) Develop constraints and mechanisms to track and report progress;

(5) Establish plans of resources and staffing, qualifications, and training of project personnel;

(6) Establish a description of the methods, techniques, and tools used;

Software Development Project Plans use the format specified in IEEE 1058.1, "Standard for Software Project Management Plans."

### 5.1.4 Software Configuration Management Plan

The Software Configuration Management Plan (SCMP) outlined below defines the organizational responsibilities for software configuration management, and methods to be applied to create a plan to establish and maintain the integrity of the products of the software project throughout the projects software life cycle. This outline in conjunction with other plans described herein addresses the various elements described in the related guidance documents including Reg. Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." The SCMP describes:

(1) The SCM organization with a description of responsibilities of each individual for carrying out each SCM activity, and identifies the individual with authority to authorize release of any software, data, or document for revision.

(2) A list of documents to be placed under configuration control.

(3) The SCM activities, which include:

a. A process to manage changes to design interface documentation and software design documentation;

b. A process to designate and control software revision status. Such methods shall require that software code listings present direct indication of the software code revision status;

c. Baseline reviews of the software development process to be conducted during each phase of the software development life cycle, and the scope and methods to be used in the baseline reviews to evaluate the implemented design, design documentation, and compliance with the requirements of the Software Management Plan and Configuration Management Plan;

d. Configuration management of tools (such as compilers) and software development procedures;

e. Configuration review and audits;

f. Control of vendor(s) responsible for software development;

g. Methods for error tracking and analysis of failures during software development, such as the use of software metrics;

h. Evaluate and track commercial off-the-shelf (COTS) software in accordance with EPRI TR-106439 and CR-G421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications", and method of tracking tool history and errors.

(4) The procedures to be used in configuration management and as a minimum includes:

a. Naming conventions and procedures for placing items under configuration control;

b. Procedures for managing software libraries;

c. Procedures to manage the change process, reporting procedures, change approval procedures;

d. Procedures for maintaining status of design interface documentation and developed software design documentation, change histories, backup and recovery;

e. Tracking and synchronization procedures, and procedures for protecting configuration management records, including controlling source and object code during and after the project development process;

f. Procedures for managing corrective actions to resolve deviations identified in software design and design documentation, including notification to end user of errors discovered in software development tools or other software;

g. Methods for design record collection and retention;

h. Methods for tracking error rates during software development, such as the use of software metrics and actions taken on recommendations to improve operation.

### 5.1.5 Verification And Validation Plan

The Verification and Validation Plans (V&VP) outlined below define the verification and validation process to assure the following:

(1) V&V shall be performed as a controlled and documented evaluation of the conformity of the developed design to the documented design requirements at each phase of baseline review;

(2) Software outputs of each life cycle phase are in compliance with the requirements defined in the previous phase;

(3) Final software product meets the system requirements and applicable established standards.

The Verification and Validation Plans, in conjunction with other plans described herein, address the various elements and are intended to meet the requirements specified in Reg. Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems for Nuclear Power." The V & V Plan provides:

(1) Description of the organization supporting the software V&V effort. This includes:

a. V&V staff qualification and responsibilities of individuals carrying out each V&V task and personnel assignments for performing the V&V tasks;

b. Approval authority reporting channels;

c. Organizational interfaces;

d. Training requirements.

(2) A description of the degree of independence between the development team and V&V Team.

(3) Description of how the V&V effort will be managed, including:

a. Reporting procedures;

b. Management reviews and audits. Design verification reviews shall be conducted as part of the baseline reviews of the design material developed during the Planning through Integration phases of the software development life-cycle, and that validation testing shall be conducted as part of the baseline review of the Validation phase of the software development life-cycle;

c. Methods of carrying out the different V&V activities

d. Ensuring that validation testing shall be conducted per documented test plan and procedure;

e. Completion criteria for the V&V activities. Software development is not complete until the specified verification and validation activities are complete and developed software is consistent with design documentation;

f. Evaluation of commercial software and commercial development tools for safety-related applications;

g. V&V requirements for non-conformance tracking and closure.

(4) Schedule, milestone and resources plans needed to support the V&V activities.

(5) A description of the V&V activities, including:

a. Verification and Validation Methods and Test Tools;

b. Acceptance criteria for each activity;

c. Relationships with the product development life cycle tasks;

d. Coordination with SCM activities.

(6) A description of all required testing and test documentation requirements, including error reporting and methods for identification, closure, and documentation of design and/or design documentation non-conformances and anomaly resolution procedures.

(7) A description of V&V documentation and reporting requirements, including:

a. The individual and/or team conducting the V&V;

b. Activities during the V&V, including the V&V inputs and outputs, traceability matrix (forward and backward direction), evaluation criteria and non-conformances identified during the V&V.

c. The products which shall result from the baseline reviews conducted at each phase of the software development life cycle. The products of the baseline reviews and the V&V Plan shall be documented and maintained under configuration management;

d. Use of commercial software and commercial development tools for safety-related applications is a controlled and documented procedure.

### 5.1.6 Software Safety Plan

This Software Safety Plan (SSP) outlined below establishes the processes and activities intended to be used to ensure the safety of the safety related software for the software-based product and to address the potential software risks. This outline in conjunction with other plans described herein, addresses the various elements described in the related guidance documents including the guidelines described in IEEE 1228, "Software Safety Plans." The Software Safety Plan:

(1) Specifies the purpose and scope of the software safety activities.

(2) Defines the responsibilities and authority of the software safety organization (i.e., specify a person or group responsible for software safety tasks). The designated individual shall have a clear authority for enforcing safety requirements in the software-based products being designed and developed. The software safety organization shall have the authority to reject the software, including previously developed software, support software, and third party software if the software cannot be shown to be adequately safe.

(3) IdentifiesPlan the resources required for the software safety organization, including qualification and training requirements.

(4) Describes the management of software safety activities, including how the safety activities are integrated and coordinated between the development team and other organizations (i.e., software safety organizations, Quality Assurance, Configuration Control Management, vendors).

(5) Describes the safety analyses to be performed and documented on each of the principle design documents for software life cycle phases defined in the Software Management Plan.

(6) Describes the documentation requirements for software safety analysis, including configuration management of the software safety documents.

(7) Describe any safety related tests that are not included in the Software Verification and Validation Plan.

### 5.1.7 Software Test Plan

The Software Test Plan outlined below describes the software test activities to be carried out during the development process of the software product. This test plan outline, in conjunction with other plans described herein, addresses and is intended to meet the requirements specified in Reg. Guide 1.170, "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants", and Reg. Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." The test plan:

(1) Describes the test organization, which includes description of responsibilities of each individual for carrying out each test activity;

(2) Describes test management, such as (but not limited to) schedule, resources, security, risks and contingency planning, anomaly and problem reporting, and training needs;

(3) Describes of the scope of the equipment to be tested;

(4) Defines the Software Test Guidelines for:

a. Test preparation to assure that the required test activities can be properly carried out within the project schedule. This is accomplished by identification of resources, including applicable tools and environmental conditions required to support the development, execution, and the documentation of the test.

b. Test design to specify the test strategies (acceptance criteria, test techniques and test approaches) to assure completeness of the test coverage.

c. Test execution to analyze the test item in order to evaluate each identified feature or combination of features to determine if the feature or combination of features have passed or failed based on the defined acceptance limits.

d. Test summary to summarize the results of the designated testing activities and to provide evaluations based on these results.

(5) Defines the test methods such as:

a. Module (unit) testing. Module testing is the verification of the internal structure of individual software modules, or group of modules, to ensure that each software function allocated in the Software Design Specification (SDS) performs as intended.

b. Integration testing. Integration testing is an orderly progression of testing to uncover errors associated with software and hardware interfaces. Integration testing is performed to verify that all software modules perform

as intended and conform to requirements (such as but not limited to interfaces, stress, security, and self test) after being installed in the hardware.

c. System validation testing. System validation testing relies entirely on black-box testing techniques and is executed using formally prepared test procedures to assure the system is operational and conforms to all functional and performance requirements specified in the System Requirements Specification (SRS).

(6) Definition of all required test documentation, such as testing plans, specifications, procedures and cases, and summary and anomaly reports.

(7) Measurement system for error tracking and resolution, and to assess the success or failure of the test effort.

### 5.1.8 Operational and Maintenance Manual (O&M Manual)

The Software Operations and Maintenance Plan (O&M Manual) outlined below, which complies with the software maintenance guidelines specified in IEEE Std. 828, "IEEE Standard for Software Configuration Management Plans", and IEEE Std. 1042, "IEEE Guide to Software Configuration Management", will be established for software-based products.

The O&M Manual describes the instruction and guideline to operate and maintain the software product. The O&M Manual:

(1) Describes the organization supporting the software product operations and maintenance effort. This includes:

a. The qualification and responsibilities of individual carrying out each operations and maintenance task;

b. Personnel assignments for performing the operations and maintenance tasks;

c. Security measures to limit access to information, use of critical functions, and changes to critical functions;

d. Organizational interfaces;

e. Training requirements.

(2) Defines the procedures to allow responsible personnel to:

a. Initiate and perform normal system operational activities;

b. Perform required maintenance;

c. Perform troubleshooting when abnormal conditions for system operation occur;

d. Develop a problem reporting channel, and a resolution path of those problem reports.

(3) Specifies the methods, techniques and tools use to accomplish the maintenance function.

(4) Includes the required system documentation such as (but not limited) to elementary diagram, schematic, system guides to assist operations and maintenance personnel in operating and maintaining the software-based product.

(5) Defines the procedures on failure detection during operation, correction of faults that have caused those failures, and if applicable, regression testing to be conducted.

(6) Defines procedures to shut down and restore the software-based product to normal operation.

(7) Provides a list of recommended spare parts so that an appropriate site plan can be implemented for obtaining spare parts and performing replacement if needed to assure continued, reliable and safe operation.

(8) Develops a system for collecting metrics and using them to assess the success or failure of the operating and maintenance procedures.

### 5.1.9 Training Plan

The training plan outlined below describes the management, implementation, and resource characteristics of the training program. The training plan defines the organization supporting the software-based product training effort. This includes:

(1) Organizational interfaces and responsibilities; the qualification and responsibilities of individual carrying out each training module and personnel assignments for performing the training. The qualified trainers must be knowledgeable in the operation of software product.

(2) Overall objectives, describing the training needs of appropriate plant staff, including operators, I&C engineers, and technicians.

(3) The methods, techniques, tools and facility used to accomplish the training function.

(4) Written test or assessment that demonstrates the student's knowledge as it relates to the objectives or subject material presented to the student.

## 5.2 Other Required Plans and Programs

### 5.2.1 Electromagnetic Compatibility (EMC) Compliance Plan

The electrical and electronic components of the systems listed below will be qualified for the anticipated levels of electrical interference at the installed locations of the components according to an established plan:

1. Safety System Logic and Control; and
2. DCIS (both essential and non-essential portions).

The EMC compliance plan will be structured on the basis that electromagnetic compatibility (EMC) of I&C equipment is verified by factory testing and site testing of both individual components and interconnected systems to meet EMC requirements for protection against the effects of:

- Electromagnetic Interference (EMI);
- Radio Frequency Interference (RFI);
- Electrostatic Discharge (ESD); and
- Electrical surge (Surge Withstand Capability) (SWC).

The EMC compliance plan will require, for each system qualified, system documentation that includes confirmation of component and system testing for the effects of high electrical field conditions and current surges. As a minimum, the following information will be documented in a qualification file:

- Expected performance under test conditions for which normal system operation is to be ensured;
- Normal electrical field conditions at the locations where the equipment will perform as above;
- Testing methods used to qualify the equipment, including:
  - Types of test equipment;
  - Range of normal test conditions;
  - Range of abnormal test conditions for expected transient environment;
  - Location of testing and exact configuration of tested components and systems, including interconnecting cables, connections to electrical power distribution

system, and connections to interfacing devices used during normal plant operation; and

- Test results that show the component or system is qualified for its application and remains qualified after being subjected to the range of normal and abnormal test conditions specified above.

The EMC compliance plan will establish separate test programs for each element of EMC, using the following approaches:

- EMI and RFI protection. An EMC compliance plan for each component or system identified in the design commitment will include tests to ensure that equipment performs its functions in the presence of the specified EMI/RFI noise environment, including the low range of the EMI spectrum, without equipment damage, spurious actuation, or inhibition of functions. As part of the pre-operational test program, the EMC compliance plan will call for each system to be subjected to EMI/RFI testing. Tests cover potential EMI and RFI susceptibility over four different paths:
  - Power feed lines
  - Input signal lines
  - Output signal lines
  - Radiation
- The test program will include sensitivity of components identified in the design commitment to radiation from plant communication transmitters and receivers.
- Test procedures will be prepared for the safety and non-safety systems, ensuring the unique EMC requirements are applied to the test programs applied by the respective suppliers.
- ESD Protection. An EMC compliance plan for each component or system identified in the design commitment will include tests to ensure that equipment performs its functions in the presence of the specified ESD environment without equipment damage, spurious actuation, or inhibition of functions. The plan will be structured on the basis that ESD protection is confirmed by factory tests that determine the susceptibility of instrumentation and control equipment to electrostatic discharges.
- The EMC compliance plan includes standards, conventions, design considerations, and test procedures to ensure ESD protection of the plan instrumentation and control equipment. The plan requires test documentation

confirming that, for each component tested, the following conditions have been met:

- No change in output signal status was observed during the test
- The equipment performed its normal functions after the test

- SWC Protection. An EMC compliance plan for each component of system identified in the design commitment will include tests to ensure that equipment performs its functions for the specified SWC environment without equipment damage, spurious actuation, or inhibition of functions. The EMC compliance plan will include standards, conventions, design considerations, and test procedures to ensure SWC protection of the plan instrumentation and control equipment.

The plan will document the level of compliance of each system with standard grounding and shielding practices.

### 5.2.2 Set-Point Methodology Plan

The setpoint methodology plan will establish requirements for:

1. Documentation of data, assumptions, and methods used in the bases for selection of trip setpoints;
2. Consideration of instrument channel inaccuracies (including those due to analog-to-digital converters, signal conditioners, temperature compensation circuits, and multiplexing and demultiplexing components), instrument calibration uncertainties, instrument drift, and uncertainties due to environmental conditions (temperature, humidity, pressure, radiation, EMI, power supply variation), measurement errors;
3. The effect of design basis event transients in determining the margin between the trip setpoint and the safety limit;
4. The methods used for combining uncertainties;
5. Use of written procedures for preoperational testing and tests performed to satisfy the Technical Specifications;
6. Documented evaluation of replacement instrumentation that is not identical to the original equipment.

### 5.2.3 Equipment Qualification Program

Qualification of safety related I&C equipment is implemented by a program that assures this equipment is able to complete its safety related function under the environmental conditions that exist up to and including the time the equipment has finished performing its function. Qualification specifications will consider conditions that exist during normal, abnormal, and design basis accident events in terms of their cumulative effect on equipment performance for the time period up to the end of equipment life.

An I&C equipment qualification program will be put in place under GEEN QA programs. Documentation for the program will be recorded in a product qualification file that includes a list of safety related I&C equipment accompanied by the following I&C equipment information:

1. Performance specifications under conditions existing during and after design basis accidents. These include voltage, frequency, load, and other electrical characteristics that assure specified equipment performance;

2. Environmental conditions at the location where the equipment is installed. These conditions include:

    a. Number and/or duration of equipment functional and test cycles/events

    b. Process fluid conditions (where applicable to the I&C equipment)

    c. Voltage, frequency, load, and other electrical characteristics of the equipment

    d. Dynamic loads associated with seismic events

    e. Dynamic loads associated with hydrodynamic conditions

    f. System transients and other vibration inducing events

    g. Pressure, temperature, humidity

    h. Chemical and radiation environments

    i. Electromagnetic compatibility

    j. Aging

    k. Submergence (if any)

    l. Consideration of synergistic effects that have significant effect on equipment performance

    m. Consideration of margins for unquantified uncertainty

3. One (or a combination) of the following testing methods used to qualify the equipment;

   a. Type testing of an identical item of equipment under identical or similar conditions with a supporting analysis to show that the equipment to be qualified is acceptable

   b. Type testing of a similar item of equipment with a supporting analysis to show that the equipment to be qualified is acceptable

   c. Experience with identical or similar equipment under similar conditions with a supporting analysis to show that the equipment to be qualified is acceptable

   d. Analysis in combination with partial type test data that supports the analytical assumptions and conclusions

4. Documented results of the qualification that show the equipment performs its safety function when subjected to the conditions predicted to be present when it will perform its safety function up to the end of its qualified life.

### 5.2.4 As-Built Verification Program

A program will be put in place whose objective is to verify that the installed configuration of safety related I&C equipment is bounded by the test configuration and test conditions or that an analysis exists which concludes that any differences will not affect the safety function of the I&C equipment.

## 5.3 General Design Requirements

Requirements pertaining to specific documents or steps in the Hardware and Software Design Implementation Activity are listed in the following sections.

### 5.3.1 Equipment Hardware and Software Performance Specification

The M-MIS Equipment Hardware and Software performance requirements will be covered in the Hardware Design Specifications and Software Design Specifications. The M-MIS equipment will be designed with a sufficient performance margin to perform as designed under conditions of maximum stress, including data scanning, data communications, data processing, algorithmic processing, analytical computation, control request servicing, display processing, operator request processing, and data storage and retrieval.

This specification will include the definition of algorithms and equations, detailed control logic, and data operations to be performed within the software.

### 5.3.2 Equipment User's Manual

User documentation will be developed which specifies and describes the required data, input sequences, operations, program limitations, and other activities/items necessary for the execution of the software. Error messages will be identified in text meaningful to the user, and possible corrective actions will be described.

### 5.3.3 Software Design

Software design will incorporate defensive techniques. The software will include limit checks, assign default values to prevent software instability, and perform out-of-range checks on data entries. The software design will explicitly identify assumptions whose violation would be critical. These assumptions will include both hardware and software violations.

Operating system software will remain "as delivered" from the computer vendor or commercial software house.

Software will be designed to be portable and upward compatible. A minimum number of different compilers, operating systems, programming languages, and other software support packages will be used. New or untried operating systems or compilers will not be used.

Programming will be done in a commonly accepted high-level language appropriate for the algorithms to be programmed. The definition of high-level languages may include use of graphical programming aids, expert system knowledge bases, etc. Assembly language will be used only where sufficient performance cannot be achieved through use of a high level language and will be restricted to low level routines. Machine specific programming dependencies will be restricted to low level modular routines.

Comprehensive diagnostic routines will be performed during initialization.

Programs will be developed as a set of program modules and linked together into an absolute code module to be installed into the processor memory. All software required to perform protective or control functions for safety related systems will reside in non-volatile memory.

Software security measures will be provided to limit access to information, use of critical functions, and changes to critical functions. Access will be controlled both by user identification (password) and terminal location. Authorized plant personnel will have the capability to define access to each of the major functions.

Constants, which are used to tune the system or parameters, which can be changed for a specific set of plant conditions, will not be hardcoded. The operator will be alerted when making constant changes beyond allowable ranges.

## 5.4 Software Implementation

### 5.4.1 Software Source Code

Software coding will be produced to a design standard defined in SMP and SIP which describes coding conventions, color conventions, code formats, code documentation formats, and other standards which ensure uniformity in the software design. Design standards will be produced which cover the relevant conventions and practices for the tools being used (i.e., different conventions exist for software development accomplished with expert system knowledge bases, graphical programming environments, etc.). The software will be designed with descriptive statements or comments incorporated into the source program. Code analysis will be performed to verify that the computer program, as coded, correctly implements the specified design. Software will be designed to facilitate the removal of obsolete code and databases during upgrades.

The software source code will have the following characteristics:

1. Software will be of modular design, and be capable of being verified and validated;
2. The final source program(s) will be readable from start to end;
3. The software design will include self-supervision of control flow and data;
4. A single high level language will be used throughout the entire system to the extent feasible;
5. Assembly languages will not be used for safety systems and control systems except in those cases where required to meet timing or hardware interface constraints;
6. A standard software structure will be used in all processors which provide safety systems functions;
7. A continuous loop, non interruptible software structure will be preferred for deterministic control systems and safety systems; and
8. The use of public or global variables will be located in a common region and defined.

9. Where applicable, test cases will be prepared to ensure that the criteria and test results are adequately documented

### 5.4.2 Software Module Testing

The software module testing will follow the program outlined in IEEE Std. 1008, Standard for Software Unit Testing.

## 5.5 M-MIS Integrated Factory Acceptance Test

Integrated factory testing will be performed to verify that the entire integrated M-MIS correctly implements the design and satisfies all requirements. The factory testing will utilize the M-MIS simulator demonstration facility augmented with DCIS representation in a configuration typical of what would be found in the ESBWR. Integrated factory testing will be conducted and results documented per the GEEN QA.

Excess capacity of M-MIS equipment will be measured as part of the factory acceptance test program.

# 6 Implementation Milestones and Responsibilities

## 6.1 Provisions for COL Applicant Involvement and Responsibilities

Development and execution of the Human Performance Monitoring Plan including document capture of pertinent HFE documents to establish the basis for long-term maintenance and management of the HFE life-cycle process. The M-MIS development plan contains provisions for COL Applicant participation and input at all points throughout the M-MIS implementation process. COL Applicant/Owner participation will be expected at the following stages in the M-MIS design and implementation process:

1. Establishment of the Control Room Design Team (CRDT);
2. Participation in the Control Room prototype (part-task simulator) mockup evaluations;
3. Verification of the HSI design as integrated into the simulator demonstration facility;
4. Verification of the incorporation of the results of the Human Factors Verification and Validation evaluation into the simulator demonstration facility;
5. Verification of the integrated factory testing of the M-MIS hardware and software;

6. Evaluation of the completed M-MIS full scope simulator.

7. The COL Applicant/Holder is responsible for executing continuation of the HFE activities beyond the certification phase:

   - Resolution of outstanding HEDs;
   - Completion of V&V activities, including the final development of the full scope ANS 3.5 compliant simulator for both HFE and Training requirements;
   - Establishment of the Human Performance Monitoring strategy and execution.

## 6.2 Provisions for NRC Conformance Reviews

The M-MIS development plan will contain provisions for NRC conformance reviews of Design Acceptance Criteria (DACs) throughout the M-MIS implementation process. Conformance checkpoints are anticipated at the following stages of the M-MIS design and implementation process:

1. Verification that, following the guidance of ESBWR Standard Review Plan (SRP), Section 7, Branch Technical Position HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems and other applicable NUREG reports, the M-MIS design team includes personnel with the knowledge and experience necessary to assure that human factors related issues are correctly identified and addressed in the M-MIS implementation, and that the organizational structure of the M-MIS Design Team and CRDT, and the resources and authority delegated to the M-MIS Design Team and CRDT are sufficient to assure that human factors are correctly and appropriately addressed throughout the M-MIS design implementation;

2. Verification that the task analyses are conducted in accordance with the governing Human Factors Implementation Plans, and that results of the analyses and assigned function allocations conform to accepted human factors principles;

3. Verification that the M-MIS hardware designated as safety related is in compliance with IEEE Std. 603, and Regulatory Guide 1.153;

4. Verification that the software development plans are in conformance with the M-MIS Design and Implementation Plan, ANSI/IEEE Std. 828, and ANSI/IEEE Std. 1012;

5. Verification that all significant deviations from accepted human factors principles identified in the M-MIS Control Room Prototype Evaluations are corrected or dispositioned in the final control room M-MIS design;

6. Verification that the software development and verification and validation activities satisfy the requirements in the software development plans;

7. Verification that the preoperational test results meet the acceptance criteria defined in Chapter 3 of the ESBWR DCD.

## 6.3 Human Performance Monitoring

This outlines a strategy for going forward with human performance monitoring (HPM) that links human factor engineering methods used during the design with methods for monitoring human performance during operation by the COL applicant.

### 6.3.1 Purpose

The aim of a HPM strategy is to ensure that the high safety standards established during the HSI design are maintained even when changes are made in the plant and to provide adequate assurance that the safety bases remain valid during the operational phase of the plant. There is no intent for M-MIS designer or the COL Applicant to periodically repeat a full-integrated system validation, instead the strategy is to provide a monitoring plan building upon the HFE activities during the design that can be carried forward into the operational phase, using industry accepted methods. The COL applicant may incorporate this monitoring strategy into their problem identification and corrective action program. Current industry programs include the human performance evaluation (HPES) programs that identify and classify human errors, provide for evaluation of the root cause, and support documentation of the corrective action.

### 6.3.2 HPM Strategy Development

A basic HPM strategy will be initially developed by the HSI design team, and then modified and updated by the COL Applicant to be applied during the operational life of the plant.

During the design phase the scope of the performance monitoring strategy will be developed to provide reasonable assurance that:

• The HSI design can be effectively used by personnel within the control room and between the control room and local control stations and support centers to address expected transients, design basis events, significant industry events and key scenarios identified by the PRA/HRA.

• Human actions, using HSI information, cues and controls can be accomplished with margin on time and performance criteria used to determine the probability of success assessments used in the PRA/HRA.

During the operational phase of the plant the performance monitoring strategy will provide reasonable assurance that:

• The acceptable level of performance established during the integrated HSI validation is maintained. The methods for evaluation and trending established for the plant operators through INPO's HPES provides an industry-accepted approach.

• Changes made to the initial HSIs, procedures, and training does not have adverse effects on personnel performance, e.g., a change interferes with previously trained skills. The screening and processing discussed in Regulatory Guide 1.174 will form the basis of the documentation strategy and any links to the content in Chapter 18 for the FSAR.

### 6.3.3 Elements of HPM process

The key elements for developing a HPM strategy will include considerations of data collection, screening for importance, analyzing events to determine the cause and for trending, and will support the development of corrective actions. Where possible the elements of the HPM will draw upon existing information sources and programs to provide the assurances described above.

The COL applicant HPM strategy will be capable of collecting data for trending human performance. Such data will be used to demonstrate that changes implemented result in performance that is consistent with assumptions in the analyses conducted to justify the initial design or changes to the HSI. Existing programs such as licensed operator training or corrective action are expected to include appropriate data for trending human performance. In any case the strategy will be to use existing utility or industry programs for data collection rather than developing new monitoring programs for risk-informed purposes.

The COL applicant HPM strategy will be structured to ensure that (a) human actions are monitored commensurate with their safety importance, (b) feedback of information and corrective actions are accomplished in a timely manner, and (c) degradation in performance can be detected and corrected before plant safety is compromised. This strategy will be implemented through the use of a plant specific simulator during periodic training exercises. An assumption for use during the HSI design process is that a simulator control room will be maintained and upgraded to match the actual control room with good interface and dynamic response fidelity.

When actual conditions cannot be simulated, monitored, or measured, the available information that most closely approximates performance data in actual conditions will be used to assess the impact on risk via the PRA/HRA models and data.

The COL applicant HPM strategy will be capable of maintaining a database of causes determined during the event evaluation and corrective actions taken. Such data will support trending of performance degradation and failures.

The COL applicant HPM strategy will identify and establish corrective actions that will reduce the potential for recurrence of unacceptable failures or degraded performance. A strategy will be developed to systematically identify the cause of the failure or degraded performance to the extent that a corrective action can be defined that would preclude the problem or provide adequate assurance that it will be detected before it becomes a safety concern. The corrective action will derived by (a) addressing the significance of the failure through application of PRA/HRA importance measures, (b) classifying the causes and circumstances surrounding the failure or degraded human performance, (c) illuminating the characteristics of the failure (e.g., being task specific or due to overall plant culture), and (d) determining whether the failure is isolated or has generic or common cause implications.

## Implementation Plan Process Flow Chart

**PROCESS FOR PERFORMANCE AND PREPARATION OF HFE**

Figure 1-2

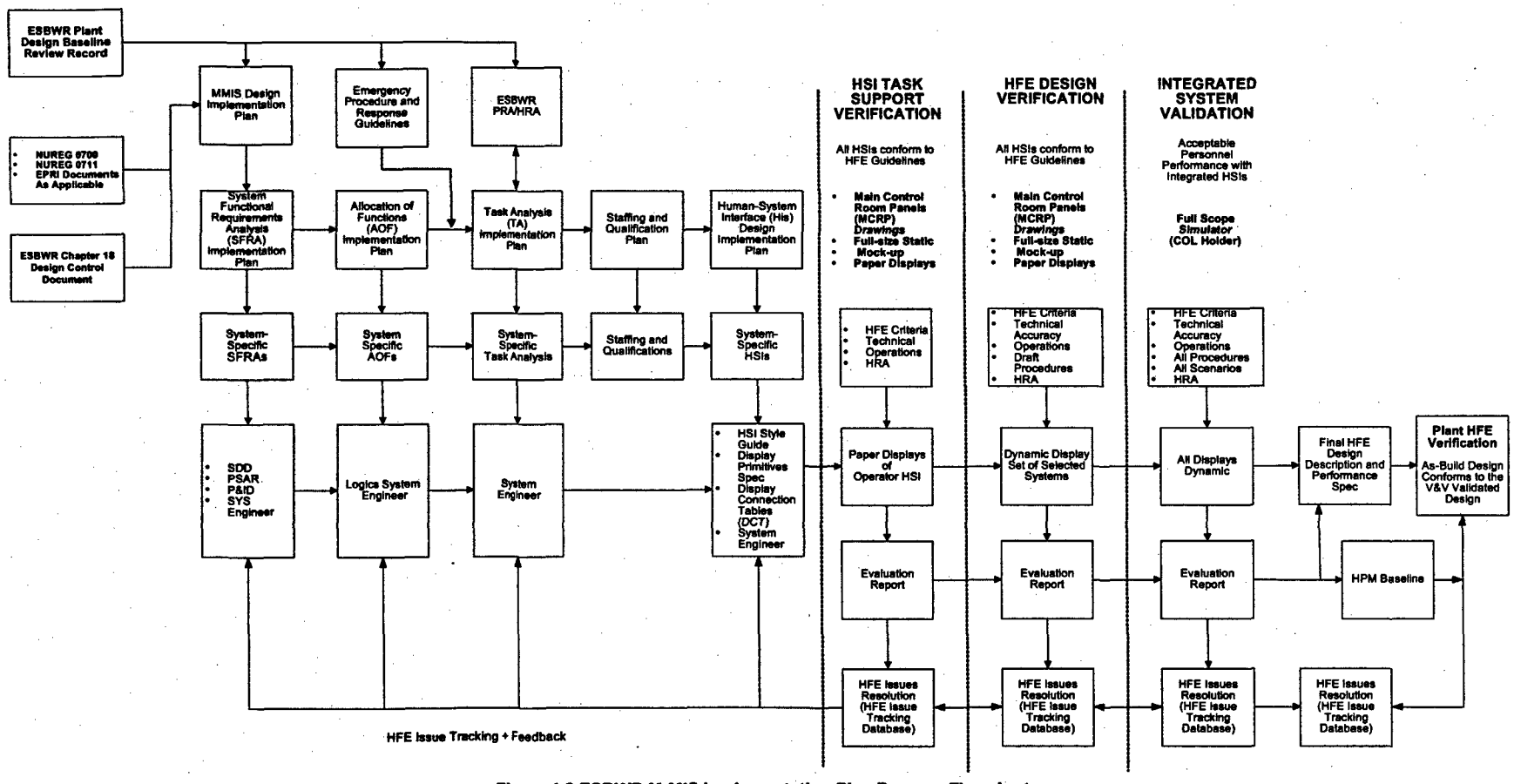


**Figure 1.2 ESBWR M-MIS Implementation Plan Process Flowchart**

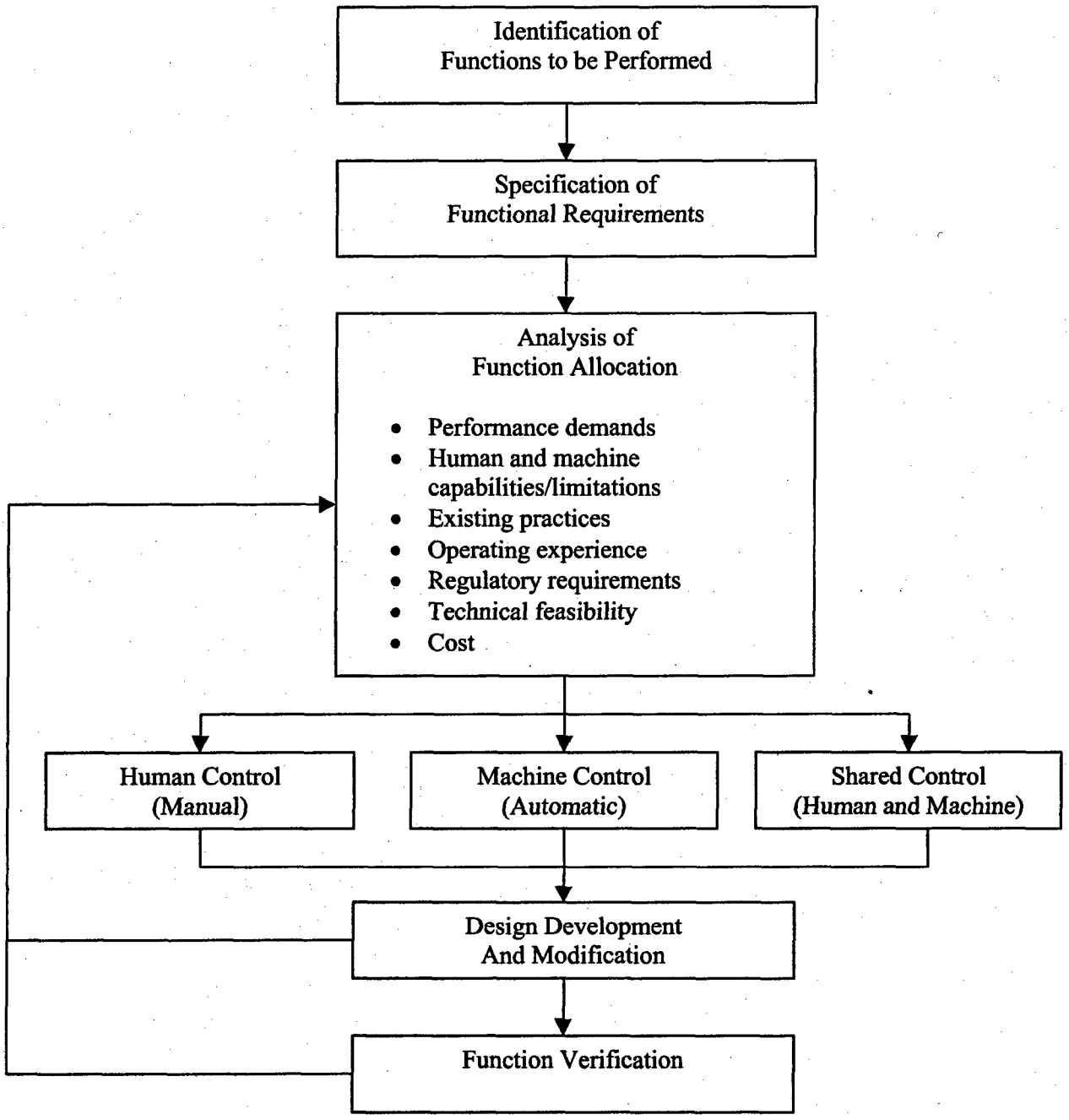


**Figure 4.4 Allocations of Functions to Human and Machine Resources**

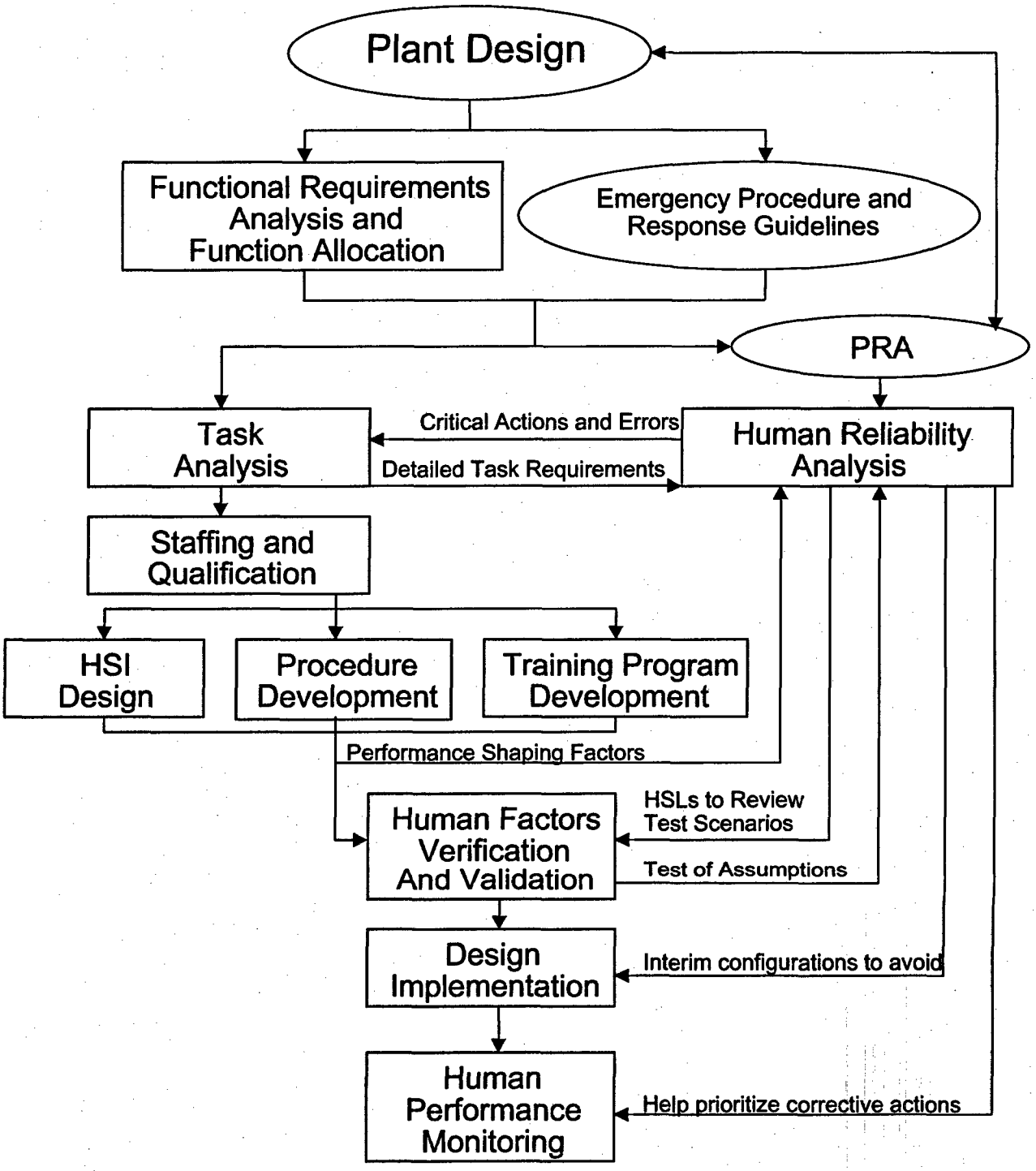


**Figure 4.7-1 The Role of Human Reliability Analysis in the HFE Program**

# Appendix A: Human Factors Engineering Issue Tracking System

## HFE Issue Tracking System

The HFE Issue Tracking System (HFEITS) addresses human factors issues (HEDs) identified throughout the HSI Design and Implementation activity. HFE Issues may be identified in the performance of the following activities:

- Operating Experience Evaluation performed under U.S. ESBWR
- Human Factors Validation & Verification

Each identified HFE issue will be considered for correction using the process flowchart shown in Figure A-1 below.

All identified HFE issues will be maintained with sufficient information to track the status of the issue. The system should identify the issue, summarize the issue evaluation, corrective action, and verification.

The following information is required in the tracking system:

1. HFE Issue Identification

   a. The design process by which the HFE issue was identified:

      i) Operating Experience Evaluations

      ii) Human Factors Validation

      iii) Human Factors Verification

   b. b. HFE issue number

   c. Area of the control room affected

   d. The HFE principle or guideline pertinent to the issue (e.g., Workspace, legibility, screen content, etc.)

   e. The plant system affected

   f. The control board panel affected

   g. Component or topic item affected (e.g., switch, mimic, VDU, lighting, etc.)

   h. Operator task or function affected

i. Human performance characteristic affected (e.g., vision, hearing, decision making, motor skills, etc.)

j. Identification date

k. Reviewer

l. A brief description of the HFE issue

2. HFE Issue Evaluation

a. Yes/No if the HFE issue requires correction

b. Justification statement if no correction needed

c. Date evaluation performed

d. Name of authorized evaluator

3. Proposed Corrective Actions

e. Description of the proposed corrective action

f. Date

g. Name of engineering discipline assigned for corrective action

h. Corrective action tracking number

4. Evaluation of Corrective Actions

i. Commit date

j. Responsible organization/manager

k. Completion date

5. Verification of Corrective Actions Implementation

l. Verification statement/summary of findings

m. Name of authorized verifier

n. Date of verification

6. HFE Issue Closeout

a. Responsible HFE Design Team Member

b. Date

**Table A-1 Example HFE Tracking Issue Data Sheet**

**HFE Issue Tracking Information**

No. _____

**A. HFE Issue Identification**

Design Process:

Area: Guideline/HFE Principle:

Plant System: Plant Subsystem:

Control Board Panel: Control Board Section:

Component/Topic Item: Human Performance:

Task/Function:

Reviewer: Date:

HFE Issue Description:

**B. HFE Issue Evaluation**

To be corrected? Yes ☐ No ☐

Justification, (if necessary):

Evaluator: Date:

**C. Proposed Corrective Actions:**

Name: Date:

**D. Evaluation of Corrective Actions:**

Name: Date:

**E. Corrective Actions Implementation**

Commit Date: Responsible Organization/Manager:

Completion Date:

**F. Verification Statement:**

Name: Date:

**G. Item Closed - Name:** Date:

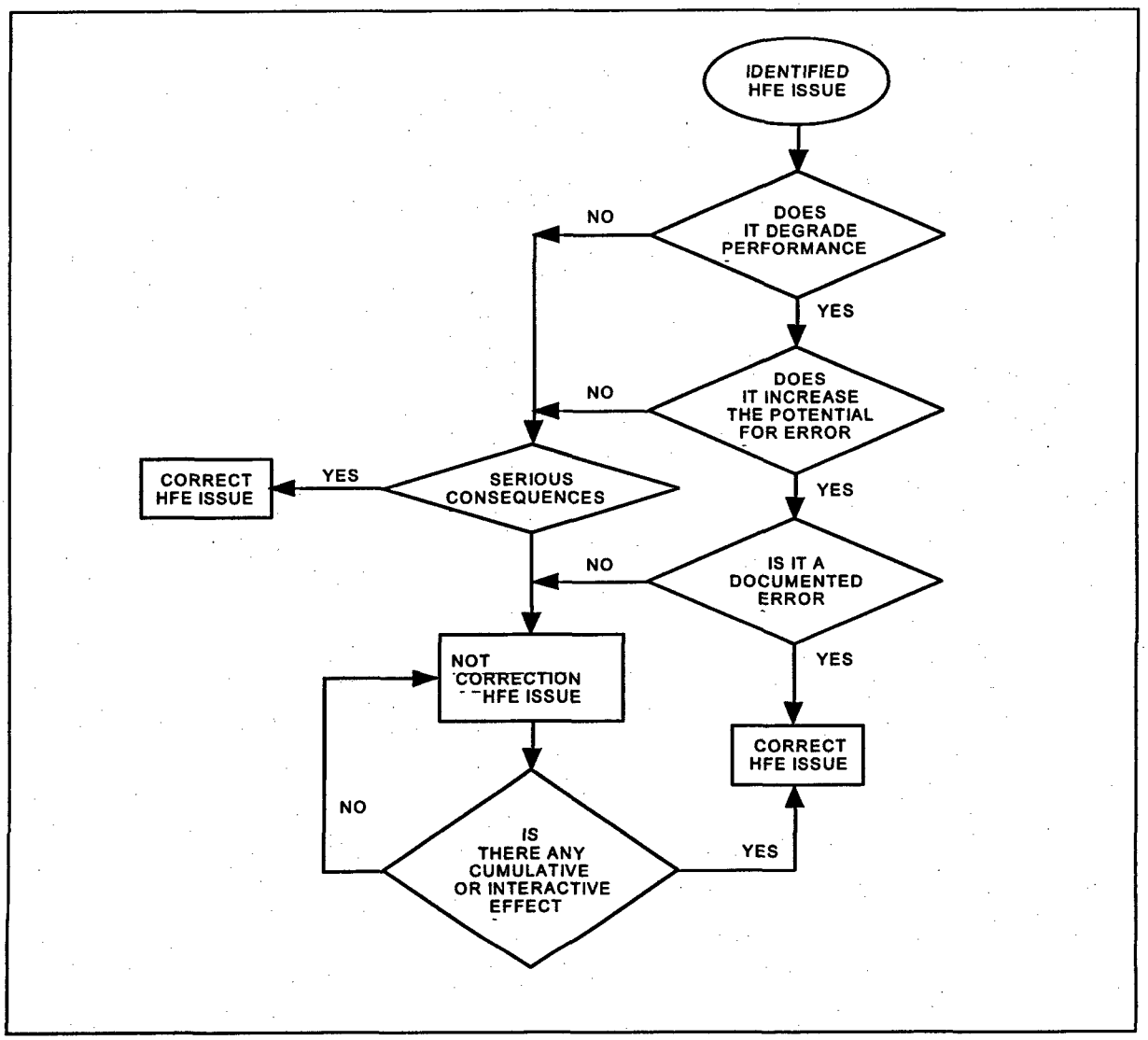


**Figure A-1 HFE Issue (HED) Evaluation Process**

# Appendix B: ESBWR Subordinate Plan Outlines

ESBWR Subordinate Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

## Attachment A: System Functional Requirements Analysis Implementation Plan (Draft) Table of Contents


**1 Introduction**

- 1.1 Purpose
- 1.2 Scope

**2 Reference Documents**

- 2.1 Supporting Documents
- 2.2 Codes and Standards
- 2.3 Regulatory Requirements and Guidelines
- 2.4 Electric Power Research Institute (EPRI)
- 2.5 Department of Defense and Energy
- 2.6 Industry and Other Documents

**3 Methods and Criteria for Identification of Plant Performance Requirements**

- 3.1 Method for Plant Primary Subgoals Identification (PFL-2)
  - 3.1.1 Safety Related Subgoals Identification [S.G. at PFL-2]
  - 3.1.2 Availability Subgoals Identification [A.G. at PFL-2]
- 3.2 Method for Critical Functions Identification (PFL-3)
- 3.3 Method for Performance Requirements Identification (PFL-4)

**4 Methods and Criteria to Perform System Level Functional Analysis Based on Plant Performance Requirements**

- 4.1 Interface Between Plant Performance Requirements and System Functions
- 4.2 System Functional Analysis Methodology
  - 4.2.1 System Functions Identification (SFL-1)
  - 4.2.2 System Process Identification (SFL-2)
  - 4.2.3 System Processing Elements Identification (SFL-3)
  - 4.2.4 System Performance Requirements Identification (SFL-4)
  - 4.2.5 System Support Requirements Identification (SFL-5)

**5 Identification of Functions Critical to Safety**

- 5.1 General
- 5.2 Accident Analysis

5.3 Interface Between ESBWR PSAR Chapter 15 and System Functional Requirements Analysis

**6 Method for Developing Graphic Function Description**

6.1 Method Description

**7 Method for Developing Detailed Functions Narrative Description**

7.1 Plant Performance Requirements Narrative Description

7.2 System Level Function Narrative Description

**8 Analysis Methods Which Define the Integration of Closely Related Subfunctions or the Division of Identified Subfunctions**

8.1 Integration/Division of Plant Performance Requirements

8.2 Integration/Division of System Functions/Subfunctions

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

### Attachment B: Allocation of Functions Implementation Plan (Draft) Table of Contents


**1 Introduction**

- 1.1 Purpose
- 1.2 Scope
- 1.3 Definition of Terms
- 1.4 Activities Not Within the Scope of AOF

**2 Reference Documents**

- 2.1 Supporting Documents
- 2.2 Codes and Standards
- 2.3 Regulatory Requirements and Guidelines
- 2.4 Department of Defense and Energy
- 2.5 Industry and Other Documents

**3 Basis and Criteria for Allocation**

- 3.1 Allocation of Functions Philosophy
- 3.2 Allocation of Function in the ESBWR Plant Design Process
  - 3.2.1 Precursors to Function Allocation
  - 3.2.2 Phases of Function Allocation
  - 3.2.3 Feedback from Other Phases of the Design Process
- 3.3 A Framework for Function Allocation
  - 3.3.1 Psychomotor and Cognitive Behaviors
  - 3.3.2 Recommended Model
  - 3.3.3 Core Performance Areas
- 3.4 The Allocation Decision Space
- 3.5 Precursors to Function Allocation
  - 3.5.1 Defining the Role of the Human
  - 3.5.2 Functional Requirements Analysis
  - 3.5.3 Organization and Composition of Design Team
  - 3.5.4 Organization of Documentation

**4 Phases of Function Allocation**

- 4.1 Defining and Evaluating the Functions

4.1.1 Defining the Functions
4.1.2 Evaluating the Allocated Functions
4.2 Function Allocation
4.2.1 Functional Allocation to Human or Machine for Mandatory Reasons
4.2.2 Functional Allocation to Human or Machine for Technical Reasons
4.2.3 Function Allocation to Human or Machine by Other Criteria
4.2.4 Global Test
4.2.5 Record Function Allocation
4.2.6 Record Automation Requirements
4.3 Evaluation of Function Allocation
4.3.1 General Method
4.3.2 Phases to Evaluate Function Allocation
4.3.3 Tradeoff Studies

**5 Allocation of Functions Report**

**Human Capabilities and Limitations**

A1 Criteria that Limit or Preclude Human Participation in a System Function
A2 Criteria that Define Unique Human Capabilities

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR MAN-MACHINE INTERFACE SYSTEM AND HUMAN FACTORS ENGINEERING IMPLEMENTATION PLAN NEDO-33217.

### Attachment C: Task Analysis (Draft) Table of Contents


**1 Introduction**

- 1.1 Purpose
- 1.2 Scope

**2 References**

- 2.1 Supporting Documents
- 2.2 Codes and Standards
- 2.3 Regulatory Requirements and Guidelines
- 2.4 Electric Power Research Institute (EPRI)
- 2.5 Department of Defense and Energy
- 2.6 Industry and Other Documents

**3 Task Analysis**

- 3.1 Why Use Task Analysis?
- 3.2 How Must Task Analysis Be Accomplished?
- 3.3 Methods and Data Sources to Be Used in Conducting the Task Analysis
- 3.4 Performers of Task Analyses
  - 3.4.1 Use of Operational Sequence Diagrams
  - 3.4.2 Use of Narrative Descriptions of Personnel Activities Required for the Completion of the Task
  - 3.4.3 Definition of the Input, Process, and Output Required by and of Personnel
- 3.5 Methods for Conducting the Initial (High Level) Task Analysis
  - 3.5.1 Converting Functions to Tasks
  - 3.5.2 Example of Converting Functions Into Tasks
  - 3.5.3 Developing Narrative Task Descriptions
  - 3.5.4 Example of Developing Narrative Task Description
  - 3.5.5 Developing the Basic Statement of the Task Functions
  - 3.5.6 Decomposition of Task to Individual Activities
  - 3.5.7 Example of Breakdown of Task to Individual Activities
  - 3.5.8 Development of Operational Sequence Diagrams (OSD)
- 3.6 Methods for Developing Detailed Task Descriptions
  - 3.6.1 Operator Decision-Making Model
  - 3.6.2 Table Data Form: General Requirements

3.6.3 Task Analysis Data Form: Data Identification
3.6.4 Task Analysis Data Form: Information and Decision-Making Requirements
3.6.5 Task Analysis Data Form: Response Requirements
3.6.6 Task Analysis Data Form: Feedback and Task Support Requirements
3.6.7 Task Analysis Data Form: Staffing, Communications, and Workplace Requirements
3.6.8 Task Analysis Data Form: Hazards Involved
3.6.9 Database Recommendations
3.6.10 Workload Assessment
3.7 Methods for Identification of Critical Task
3.8 Identification of Requirements for Alarms, Displays, Controls, and Data Processing
3.9 Task Analysis Report

**4 Methods for the Evaluation of the Task Analysis Results**
4.1 Objectives
4.2 Techniques
4.2.1 Paper and Pencil Evaluations
4.2.2 System Operating Procedures (SOPs)
4.2.3 Interface Surveys
4.3 Advantages
4.3.1 Ergonomics Checklists
4.3.2 Interface Surveys
4.4 Disadvantages
4.4.1 Ergonomics Checklists
4.4.2 Interface Surveys
4.5 ESBWR Evaluation Techniques

**5 Training**
5.1 Methods to Document and Assemble the Task Analysis Results to Provide Input for Development of Personnel Training Programs

**6 Maintainability**

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

### Attachment D: Human System Interface Design Implementation Plan (Draft) Table of Contents


**1 Purpose**

1.1 Definition of Terms

**2 Scope**

2.1 Review and Evaluations

2.1.1 Mockups

2.1.2 Dynamic Simulation

2.2 HSI and Equipment Detail Design Documents and Drawings

2.3 Work Environment, Crew Stations, Facilities and HSI Design

2.4 Human Engineering Performance and Design Specifications

**3 Applicable Documents**

3.1 Supporting and Supplemental Documents

3.1.1 Supporting Documents

3.1.2 Supplemental Documents

3.2 Codes and Standards

3.2.1 Institute of Electrical and Electronic Engineers (IEEE) Standard

3.3 Regulation and Regulatory Requirements

3.3.1 U.S. Nuclear Regulatory Commission Regulations

3.3.2 U.S. Nuclear Regulatory Commission Standard Review Plan (SRP)

3.4 Electric Power Research Institute (EPRI) Guidelines

3.5 Department of Defense and Energy

3.6 Industry and Other Documents

**4 Human Factors Analysis**

4.1 Background for HSI Design

4.1.1 Introduction

4.1.2 General Human Factors Requirements

4.1.2.1 Provision of Applicable Human Capabilities and Characteristics

4.1.2.2 Location and Protection

4.1.2.3 Space, Configuration and Environment

4.1.2.4 Panel Layout

4.1.2.5 Location Aids
4.1.2.6 Information System
4.1.2.7 Controls
4.1.2.8 Control-Display Integration
4.1.2.9 Communication System
4.1.2.10 Other Requirements
4.1.2.11 Conclusion
4.1.3 Operating Experience Review of Previous NPP HSI Designs
4.1.3.1 Existing Operating Plants
4.1.3.2 Other Industries
4.1.4 Standard Design Features
4.1.4.1 Listing of Features
4.1.4.2 Main Control Console
4.1.4.3 VDUs Driven by the PCS
4.1.4.4 VDUs Driven by the SSLC System
4.1.4.5 Fixed-Position, Dedicated Function Switches
4.1.4.6 Automation Design
4.1.4.7 Wide Display Panel (WDP)
4.1.4.8 Fixed-Position Alarms
4.1.4.9 Alarm Processing Logic
4.1.4.10 Equipment Alarms
4.1.4.11 Supervisor's Console
4.1.5 HSI Technology
4.1.5.1 Introduction
4.1.5.2 HSI Technology
4.1.6 Minimum Displays, Controls and Alarms
4.1.7 Requirements Developed from Operations Analyses
4.1.7.1 Operating Crew
4.1.7.2 Design Information from Other Sources
4.2 HSI Design
4.2.1 Workspace and Environmental Conditions Design
4.2.2 Panel Layout Design
4.2.3 Alarm and Annunciator System Design
4.2.4 Displays and Controls Design
4.2.4.1 Features for CRT Display and FD Design Specifications
4.2.4.2 Features for Computer Processing Control Design Specifications
4.2.4.3 Display System Implementation
4.2.5 Communications System Design
4.3 HSI Design Analyses
4.3.1 Criteria to be Used in Selecting HFE/HSI Design and Evaluation Tools
4.3.2 Definition of the Design/Evaluation Tools Used in the Conduct of the HSI Design Analyses
4.3.2.1 Design Criteria Checklist
4.3.2.2 Drawings

4.3.2.3 Mockups
4.3.2.4 Specifications
4.3.2.5 Questionnaires and Interviews
4.3.2.6 Test and Evaluation Methods for Evaluating and Resolving HFE/HSI Design Issues
4.4 Human-System Interface (HSI) Specification
4.5 Human-System Interface
4.5.1 Display Conventions and Guidelines
4.5.1.1 Hardware Requirements
4.5.1.2 Software Requirements
4.5.1.3 Human-Machine Interface Detail Guidelines
4.5.2 Displays and Controls

**5 HSI Documentation**
5.1 Configuration Management

**Results of Operating Experience Review of Previous NPP Previous NPP HSI Designs**
A.1 Control Room Design
A.2 Control Board Design
A.3 Computer
A.4 CRT Displays
A.5 Anthropometric
A.6 Controls
A.7 Indicator Lights
A.8 Display and Information Processing
A.9 Meters
A.10 Chart Recorders
A.11 Annunciator Warning Systems
A.12 Coding of Displays and Controls
A.13 Labeling
A.14 Communications
A.15 Task Analysis
A.16 Procedures
A.17 Operator Errors
A.18 Maintenance and Testing

**Inventory of Controls, Displays, and Alarms Based Upon the ESBWR EPGs and PRA**
B.1 Inventory of Controls Based Upon the ESBWR EPGs and PRA

B.2 Inventory of Displays Based Upon the ESBWR EPGs and PRA
B.3 Inventory of Alarms Based Upon the ESBWR EPGs and PRA
**HSI Design Implementation Process**
**Criteria for Control Device Selection**
**ESBWR Display Hierarchy for CRTs**

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR MAN-MACHINE INTERFACE SYSTEM AND HUMAN FACTORS ENGINEERING IMPLEMENTATION PLAN NEDO-33217.

### Attachment E: Human Factors Verification and Validation (Draft) Table of Contents


**1 Introduction**

1.1 Purpose

1.2 Scope

**2 Applicable Documents**

2.1 Supporting and Supplemental Documents

2.1.1 Supporting Documents

2.1.2 Supplemental Documents

2.2 Codes and Standards

2.3 Guidelines

2.3.1 Regulatory Guidelines

2.3.2 Electric Power Research Institute (EPRI)

2.3.3 Department of Defense (DOD)

2.4 Publications

**3 HF V&V Program Management**

3.1 Program Management Requirements

3.1.1 General Goals and Scope

3.1.2 Process and Procedures for Quality Assurance

3.2 Program Management Implementation

**4 HF V&V Requirements, Activities, and Implementation**

4.1 HF V&V Requirements

4.2 HF V&V Activities

4.2.1 Human-System Interface Task Support Verification

4.2.2 Human Factors Engineering Design Verification

4.2.3 Integrated System Validation

4.2.4 Human Factors Issue Resolution Verification

4.2.5 Final Plant HFE/HSI Design Verification

4.2.6 Relation to Hardware/Software V&V Process

4.2.7 HF V&V Team

4.2.8 End-Users as Participants and Test Subjects

4.2.9 Documentation, Reporting, and Integration of Results

4.3 HF V&V Implementation
4.3.1 Implementation of HSI Task Support Verification
4.3.2 Implementation of HFE Design Verification
4.3.3 Implementation of Integrated System Validation
4.3.4 Implementation of Human Factors Issue Resolution Verification
4.3.5 Implementation of Final Plant HFE/HSI Design Verification
4.3.6 Implementation of HFEITS

**5 Activities Schedule**

**HF V&V Requirements Traceability**

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

### Attachment F: Procedures Development Implementation Plan (Draft) Table of Contents

**1 Introduction**

1.1 Purpose

1.2 Scope

**2 Reference Documents**

2.1 Supporting Documents

2.2 Codes and Standard

2.3 Regulation and Regulatory Requirements

**3 Implementation Plan**

3.1 Plant Operating Procedures Development

3.2 Emergency Operating Procedures Development

3.3 Implementation of the Plan 8

**4 Procedures Included in Scope of Plan**

4.1 Integrated Operating Procedures

4.2 System Operating Procedures

4.3 Alarm Response Procedures

4.4 Abnormal Operating Procedures

4.5 Surveillance Test Procedures

4.6 Emergency Operating Procedures

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217P

### Attachment G: Software Management Plan (Draft) Table of Contents


**1 Introduction**

1.1 Purpose and Scope

1.2 Software Developed by Vendors

**2 Organization and Responsibilities**

2.1 Organizational Units

2.2 Organizational Responsibilities

**3 Definitions, Acronyms and Abbreviations**

**4 Applicable Documents**

4.1 Supporting and Supplemental Documents

4.1.1 Supporting Documents

4.1.2 Supplemental Documents

4.2 Codes and Standards

4.2.1 American Society of Mechanical Engineers (ASME) Codes

4.2.2 Institute of Electrical and Electronic Engineers (IEEE) Standards

4.2.3 International Standards

4.2.4 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides (Reg Guide)

**5 Software Engineering Process**

5.1 Planning

5.1.1 Equipment Design Requirements - SDDs, LDs and P&IDs and I/O Lists

5.1.2 Management Plans

5.1.2.1 Software Management Plan

5.1.2.2 Software Configuration Management Plan

5.1.2.3 Software Verification and Validation Plan

5.1.2.4 Software Safety Plan

5.1.3 Deleted

5.1.4 Planning Baseline Review Record

5.2 Design Definition

5.2.1 Hardware/Software Specification

5.2.2 Software Requirements Specification (SRS)

5.2.3 System Block Diagram
5.2.4 Instrument Performance Specification (with Software Requirements)
5.2.5 Sub-System Schematic
5.2.6 Data Communications Protocol
5.2.6.1 External Data Communications Protocol Specification(s)
5.2.7 Software Test Plan
5.2.8 User's Manual
5.2.9 Support Software and Tools
5.2.10 Third Party Software
5.2.11 Adaptation of Previously Developed Software
5.2.12 Safety Analysis of Design Definition
5.2.13 Design Definition Baseline Review Record
5.2.14 Safety Analysis of Concept Definition
5.3 Software Design
5.3.1 Software Design Specification
5.3.2 Internal Data Communication Protocol Specification
5.3.3 Validation Test Procedures and Test Cases Specification
5.3.4 Software Conventions and Guidelines Document
5.3.5 Safety Analysis of Software Design
5.3.6 Software Design Baseline Review Record
5.4 Software Coding
5.4.1 Coding
5.4.1.1 Software Source Code
5.4.1.2 Code Reviews
5.4.2 Software Module Testing
5.4.2.1 Module Test Reports
5.4.3 Safety Analysis of Software Coding
5.4.4 Software Coding Baseline Review Record
5.5 Integration Test
5.5.1 Integration Testing
5.5.2 Integration and Installation Test Report
5.5.3 Safety Analysis of Integration Test
5.5.4 Integration Test Baseline Review Record
5.6 Validation Test
5.6.1 Validation Testing
5.6.2 Validation Test Report
5.6.3 Safety Analysis of Validation Test
5.6.4 Validation Test Baseline Review Record
5.7 Change Control
5.7.1 Change Control Objective and Scope

**6 Document Formats**

A.1 Hardware/Software Specification (HSS)

A.2 Software Requirements Specification (SRS)

A.3 Instrument Performance Specification (IPS)

## 7 Requirement Standards

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

### Attachment H: Software Configuration Management Plan (Draft) Table of Contents


**1 Introduction**

1.1 Purpose and Scope

1.2 Definitions, Acronyms and Abbreviations

1.3 Applicable Documents

1.3.1 Supporting and Supplemental Documents

1.3.1.1 Supporting Documents

1.3.1.2 Supplemental Documents

1.3.2 Codes and Standards

1.3.2.1 American Society of Mechanical Engineers (ASME) Codes

1.3.2.2 Electrical Power Research Institute (EPRI)

1.3.2.3 Institute of Electrical and Electronic Engineers (IEEE) Standards

1.3.2.4 International Standards

1.3.2.5 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides (Reg Guide)

1.3.2.6 NUREG

**2 Configuration Management Structure**

2.1 Organization

2.1.1 Design Interfaces

2.1.1.1 Internal Design Interfaces

2.1.1.2 External (Vendor) Design Interface

2.2 SCM Responsibilities

2.2.1 Responsible Engineering Technical Lead

2.2.2 Responsible Technical Project Engineer

2.2.3 Responsible Engineer

2.2.4 Responsible Configuration Control Engineer

2.2.5 Baseline Review Team Chairperson

2.2.6 Baseline Review Team

2.2.7 Responsible Software Safety Engineer

2.3 Applicable Policies, Directives, and Procedures

2.3.1 Naming and Numbering the CIs

2.3.1.1 Issued Documents

2.3.1.2 Design Record File Documents

2.3.1.3 Software Configuration Items Identification
2.3.1.4 Physical Media Identification
2.3.1.5 Vendor Documents Identification
2.3.1.6 Acquired Software Identification
2.3.2 Product Measurement

**3 Configuration Management Activities**

3.1 Software Configuration Management Plan Implementation
3.1.1 Baselines
3.2 Configuration Control Tools and Methodologies
3.2.1 Engineering Document Management
3.2.2 Software Library for Computer-Based Configuration Items
3.2.3 Design Record File
3.2.4 Engineering Information System
3.2.5 Engineering Computer Programs
3.3 Configuration Items Identification
3.3.1 Baseline Items for Planning Phase
3.3.2 Baseline Items for Design Definition Phase
3.3.3 Baseline Items for Software Design Phase
3.3.4 Baseline Items for Software Coding Phase
3.3.5 Baseline Items for Integration Test Phase
3.3.6 Baseline Items for Validation Test Phase
3.3.7 Baseline Items for Change Control Phase
3.4 Configuration Control Process
3.4.1 Baseline Review
3.4.2 Baseline Items Approval Process
3.4.3 Baseline Review Record
3.4.4 Baseline Item Storage
3.5 Configuration Change Control
3.5.1 Change Control Process
3.5.1.1 Responsible Individuals
3.5.1.2 Change Approval
3.5.1.3 Change Notification
3.6 Status Accounting
3.7 Configuration Reviews and Audits
3.7.1 Configuration Reviews
3.7.2 Functional Configuration Audit
3.7.3 Physical Configuration Audit
3.8 Configuration Items Release Procedures
3.9 Product Release

**4 Vendor Control**

4.1 Software Developed by Vendors for the Project

**5 Acquired Software**

5.1 Configuration Change Control of Acquired Software

**6 Record Collection and Retention**

**Sample Forms to be Used**

A.1 Baseline Review Record

A.2 Software Problem Report

A.3 Engineering Tool Problem Report

**Requirement Standards**

**Software Library Structure**

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

### Attachment I: Software Verification and Validation Plan (Draft) Table of Contents


**1 Introduction**

1.1 Purpose and Scope

1.2 Definitions, Acronyms and Abbreviations

1.3 Applicable Documents

1.3.1 Supporting and Supplemental Documents

1.3.1.1 Supporting Documents

1.3.1.2 Supplemental Documents

1.3.2 Codes and Standards

1.3.2.1 American Society of Mechanical Engineers (ASME) Codes

1.3.2.2 Electrical Power Research Institute (EPRI)

1.3.2.3 Institute of Electrical and Electronic Engineers (IEEE) Standards

1.3.2.4 International Standards

1.3.2.5 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides

1.3.2.6 NUREG

**2 Management of Verification and Validation**

2.1 Internal V&V

2.1.1 Qualification of Responsible Individuals

2.1.1.1 Design Reviews

2.1.1.2 Independent Design Verifications

2.1.1.3 Code Reviews

2.1.1.4 Module Testing

2.1.1.5 Integration Testing

2.1.1.6 Validation Testing

2.1.2 Resources, Schedule and Milestones

2.3 M-MIS Integration and Validation Test

2.3.1 M-MIS Integrated Factory Acceptance Test

2.3.2 M-MIS Factory Validation and Verification Test

**3 General V&V Requirements**

3.1 V&V Requirements for Nonconformance Tracking and Closure

3.2 V&V Requirements for Vendor Software

3.3 V&V Requirements for Acquired Software

**4 Verification and Validation Methods and Tools**

4.1 Methods of Verification

4.1.1 Informal Design Reviews

4.1.2 Internal Verification and Validation

4.2 Methods of Validation

4.2.1 Software Testing

4.3 Verification & Validation Tools

4.3.1 Traceability Matrix

4.3.2 Baseline Review Record

4.3.3 Test Tools

**5 Verification and Validation Activities**

5.1 Internal V&V

5.1.1 V&V Implementation for Software Engineering Process

5.1.1.1 V&V for Planning Phase

5.1.1.2 V&V for Design Definition Phase

5.1.1.3 V&V for Software Design Phase

5.1.1.4 V&V for Software Coding Phase

5.1.1.5 V&V for Integration Test Phase

5.1.1.6 V&V for Validation Test Phase

5.1.1.7 V&V for Change Control Phase

5.2 Independent V&V Overview

5.3 Baseline Reviews

5.3.1 Planning Phase

5.3.2 Design Definition Phase

5.3.3 Software Design Phase

5.3.4 Software Coding Phase

5.3.5 Integration Test Phase

5.3.6 Validation Test Phase

**Requirement Standards**

**Design Walkthrough Report**

## APPENDIX B

ESBWR Plan Outlines are provided herein for background information only. Specific ESBWR reports will have unique ESBWR NEDx Number assignments and will be produced in accordance ESBWR Man-Machine Interface System And Human Factors Engineering Implementation Plan NEDO-33217.

### Attachment J: Software Safety Plan Table of Contents


**1 Introduction**

- 1.1 Purpose and Scope
- 1.2 Safety Goals
- 1.3 Probabilistic Goals

**2 Definitions, Acronyms and Abbreviations, and References**

- 2.1 Definitions
- 2.2 Acronyms
- 2.3 References
  - 2.3.1 Supporting Documents
  - 2.3.2 Supplemental Documents
  - 2.3.3 Codes and Standards

**3 Software Safety Management**

- 3.1 Organization and Responsibilities
- 3.2 Resources
- 3.3 Staff Qualification and Training
- 3.4 Software Life Cycle
- 3.5 Documentation Requirements
- 3.6 Software Safety Program Records
- 3.7 Software Configuration Management Activities
- 3.8 Software Quality Assurance Activities
- 3.9 Software Verification and Validation Activities
- 3.10 Tool Support and Approval
- 3.11 Previously Developed or Purchased Software
- 3.12 Subcontract Management
- 3.13 Process Certification

**4 Software Safety Analyses**

- 4.1 Concept Definition Analysis
  - 4.1.1 Task Description
  - 4.1.2 Input Documents

4.1.3 Outputs
4.1.4 Methods
4.1.5 Reporting Requirements
4.2 Design Definition Analysis
4.2.1 Task Description
4.2.2 Input Documents
4.2.3 Outputs
4.2.4 Methods
4.2.5 Reporting Requirements
4.3 Software Design Analysis
4.3.1 Task Description
4.3.2 Input Documents
4.3.3 Outputs
4.3.4 Methods
4.3.5 Reporting Requirements