

MFN 08-255

Enclosure 2

NEDO-33217

Revision 4

ESBWR Licensing Topical Report – *ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan*

Non-Proprietary Version

DO NOT ELECTRONICALLY TRANSMIT TO NRC



HITACHI

GE Hitachi Nuclear Energy
3901 Castle Hayne Road
Wilmington, NC 28401

NEDO-33217

Revision 4

Class I

eDRE 0000-0048-2821

May 2008

LICENSING TOPICAL REPORT

ESBWR

**MAN-MACHINE INTERFACE SYSTEM AND HUMAN
FACTORS ENGINEERING
IMPLEMENTAION PLAN**

Copyright, GE-Hitachi Nuclear Energy Americas LLC, 2008 All Rights Reserved

NON-PROPRIETARY INFORMATION NOTICE

This document is the non-proprietary version of NEDE-33217P, Rev. 4, and thus, has the proprietary information removed. Portions of this document that have been removed are indicated by open and closed double brackets, as shown here [[]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The information contained in this document is furnished as reference to the NRC Staff for the purpose of obtaining NRC approval of the ESBWR Certification and implementation. The only undertakings of GEH with respect to information in this document are contained in contracts between GEH 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, GEH 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

1.1 Purpose	6
1.2 Scope	6
1.3 Definitions and Acronyms.....	7
1.3.1 Definitions.....	7
1.3.2 Acronyms	9
2.1 Supporting Documents and Supplemental GEH Documents.....	15
2.1.1 Supporting documents.....	15
2.1.2 Supplemental Documents.....	15
2.2 Codes and Standards.....	16
2.3 Regulatory Guidelines.....	16
2.4 DOD and DOE documents.....	16
2.5 Industry and other documents	16
3.1 MMIS and HFE Management Plan	18
3.1.1 Background for MMIS and HFE Management Plan.....	18
3.1.2 Goals for MMIS and HFE Implementation Plan.....	19
3.1.3 Requirements for MMIS and HFE Management Plan	19
3.1.3.1 Process Procedures.....	19
3.1.3.2 Independent Review and Verification.....	19
3.1.3.3 Defense-In-Depth and Diversity Assurance.....	20
3.1.3.4 Safety Margins	21
3.1.3.5 Cyber Security.....	21
3.1.4 General Approach for MMIS and HFE Management Plan	21
3.1.4.1 Project Organization.....	21
3.1.4.2 Management Process and Procedures	27
3.1.4.3 Human Factors Engineering Issue Tracking System.....	34
3.2 HFE Process	35
3.2.1 Background for HFE Process.....	35
3.2.2 Goal for HFE Process.....	35
3.2.3 Requirements for HFE Process	35
3.2.4 General Approach for HFE Process	38
3.2.4.1 HFE Process Description and Flow.....	38
3.2.4.2 Integration of the HFE Process into the ESBWR Design	41
3.2.4.3 COL Applicant Involvement in the HFE Process	42
3.2.4.4 Accident Management.....	42
3.2.5 Application.....	45
3.2.6 Summary of HFE Process	46
3.3 MMIS Software Development	47
3.3.1 Background for MMIS Software Development	47
3.3.2 Goal for MMIS Software Development.....	48
3.3.3 Requirements for MMIS Software Development.....	48
3.3.3.1 Software Classification.....	48
3.3.3.2 Configuration Management and Change Control.....	49
3.3.3.3 Requirements Traceability Matrix.....	49
3.3.3.4 Independent Verification.....	49
3.3.3.5 Testing.....	50
3.3.3.6 Software Safety Analysis	50
3.3.3.7 Baseline Review.....	50
3.3.3.8 Software Developed by Vendors.....	50
3.3.4 General Approach for MMIS Software Development	51

3.3.5 Summary of Software Development Process	52
APPENDIX A: HUMAN FACTORS ENGINEERING ISSUE TRACKING SYSTEM.....	54
APPENDIX B: GUIDELINES FOR CONTROL SYSTEM DATA GATHERING, TRANSMISSION, AND PROCESSING	57
APPENDIX C: GUIDELINES FOR DESIGN OF HSI.....	60
APPENDIX D: GUIDELINES FOR THE CONDUCT OF WALK-THROUGHS.....	65

LIST OF FIGURES

Figure 3.1.4-1. Engineering, Quality and Project Management Organization	23
Figure 3.1.4-2. Process Feedback and Issues Disposition	30
[[.....]]	33
Figure 3.2.4-1. HFE Process Flow Diagram.....	39
Figure A-1. HFE Issue Evaluation Process.....	56

1. OVERVIEW

1.1 PURPOSE

The purpose of this plan is to describe:

- The Human Factors Engineering (HFE) design process.
- The Man-Machine Interface System (MMIS) software development process.
- The management plan contained within to implement the HFE design and MMIS software development processes.
- The supporting implementation plans for the HFE design and MMIS software development processes.

This plan also describes how the management plan and the supporting implementation plans:

- Integrate the HFE design process into the ESBWR development, design, and evaluation.
- Comply with regulatory requirements and guidelines.
- Comply with the requirements of Chapter 18 of the ESBWR Design Control Document (DCD), Rev. 5.
- Comply with the requirements of Chapter 7 of the ESBWR DCD.
- Reflect state-of-the-art human factors principles.
- Utilize the design information available from the ABWR predecessor plants and US standard plant design.

1.2 SCOPE

The scope of the MMIS design process consists of:

- The HFE process including the design of the hardware interfaces and
- The design and development of the software that manipulates data for use by plant personnel, automatic protection, and control equipment.

The following additional scope definition is provided:

- (1) Assumptions and Constraints - The assumptions and constraints of the design include:
 - a. Predecessor ABWR Designs – The use of proven MMIS design from predecessor ABWR plants is addressed in DCD Chapter 18.3, [2.1.1(2)].
 - b. Standard Design Features – The ESBWR Control Room HSI design contains a group of standard features described in DCD Chapter 18.1 [2.1.1(2)].
 - c. Safety Requirements – Design inputs from regulations and regulatory guidance are discussed in DCD Chapter 18.1 [2.1.1(2)].
 - d. Staffing Plan – The initial staffing plan is addressed in DCD Chapter 18.6 [2.1.1(2)].
- (2) Applicable Facilities - The HFE program addresses the Main Control Room (MCR), Remote Shutdown System (RSS), Technical Support Center (TSC), Emergency Operations

Facility (EOF) displays, and Local Control Stations (LCSs) with a safety-related function or as defined by Task Analysis.

- (3) Applicable Human-System Interfaces - The applicable Human-System Interfaces (HSIs), procedures, and training included in the HFE program include operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures) for those systems with safety significance. This includes monitoring the designs being presented by ESBWR suppliers, to ensure supplier designs are consistent with the HFE requirements of the ESBWR HFE Program.
- (4) Applicable Software Products – Applicable software products are those used to implement system controls and associated interfaces described in DCD Chapter 7 [2.1.1(4)], “Instrumentation and Control Systems”. These functions are primarily represented within the Q-DCIS and N-DCIS of the plant I&C System, and may include various other programmable logic controllers hardware outside of these systems. Subsection 3.3.1 provides further definition of the functions within the scope of the MMIS software development process.
- (5) Applicable Plant Personnel - Plant personnel 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:
 - non-licensed operators
 - shift supervisor
 - shift technical advisor
 - instrument and control technician
 - electrical maintenance personnel
 - mechanical maintenance personnel
 - radiological protection technician
 - chemistry technician
 - engineering support personnelto the extent that they perform tasks that are directly related to plant safety.

1.3 DEFINITIONS AND ACRONYMS

1.3.1 DEFINITIONS

The GEH Nuclear Topical Plans listed in Subsection 2.1.2 establish a list of plan-specific definitions. The following terms are defined for use within this plan.

Design Record File (DRF) - A formal and controlled information record within GEH procedures. The DRF is used for in-progress and completed engineering.

Design Reviews - Formal, design adequacy evaluations that are performed by knowledgeable persons to verify product designs meet functional, contractual, safety, regulatory, industry codes and standards, and GEH requirements.

Function Allocation – The process of assigning responsibility for task completion to human or machine resources, or to a combination of human and machine resources.

HFE Issue Tracking System (HFEITS) - An electronic database used to document human factors engineering issues that are not resolved through the normal HFE process and Human Engineering Discrepancies (HEDs) from the design verification and validation activities. Additionally, the database is used to document the problem resolutions.

Human-System Interfaces (HSIs) – The human-system interfaces are the means through which personnel interact with the plant. This includes the alarms, displays, controls, and job performance aids. Generically this includes operations, maintenance, test, and inspection interfaces.

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

Local Control Station (LCS) - An operator interface related to process control that is not located in the Main Control Room (MCR). This includes multifunction panels, as well as single-function LCS controls (Ex: valves, switches, and breakers) and displays (Ex: meters) that are operated or consulted during normal, abnormal, or emergency operations.

Mockup - A static representation of a human-system interface

Operating Experience Review (OER) - A review of relevant history from the plant's on-going collection, analysis, and documentation of operating experiences and also from interviews with plant staff.

Man-Machine Interface System (MMIS) – The Man-Machine Interface System is comprised of the systems performing the monitoring, control, and protection functions of the plant. This includes the HSIs and the software supporting the operator with information displays and control functions as well as alarms.

Risk-Important Human Actions - Actions that are performed by plant personnel to provide reasonable assurance of plant safety. Actions may be made up of one or more tasks. There are both absolute and relative criteria for defining risk-important actions. From an absolute standpoint, a risk-important action is any action whose successful performance is needed to provide reasonable assurance that predefined risk criteria are met.

From a relative standpoint, the risk-important actions may be defined as those with the greatest risk in comparison to all human actions. The identification can be done quantitatively from risk analysis and qualitatively from various criteria such as task performance concerns based on the consideration of performance shaping factors.

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

Style Guide - A document containing tailored guiding principles describing the implementation of HFE guidance to a specific design (Ex: plant control room). Adherence is expected and deviations justified.

Validation (Software) – The testing process to ensure the product meets its intended use and is compliant with system functional, performance and interface requirements.

Verification - Evaluation of a design to determine whether it acceptably satisfies specified requirements and guidelines.

Walk-Through – A static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a segment of a process, procedure, document or code. The participants ask questions and make comments about possible errors, violation of development standards and guidelines, and other problems.

1.3.2 ACRONYMS

The GEH Nuclear Energy Topical Plans, listed in Subsection 2.1.2, establish a list of plan-specific acronyms. The following is a list of acronyms used in this plan:

A/D	Analog/Digital
ABWR	Advanced Boiling Water Reactor
ADS	Automatic Depressurization System
AEO	Auxiliary Equipment Operator
ALARA	As Low as Reasonably Achievable
AOF	Allocation of Function
AOP	Abnormal Operating Procedures
ARP	Alarm Response Procedures
BRR	Baseline Review Record
BRT	Baseline Review Team
BWR	Boiling Water Reactor
BWROG	Boiling Water Reactors Owner Group
CAR	Corrective Action Request
CCDP	Conditional Core Damage Probability
CDF	Core Damage Frequency
CI	Configuration Items
CMM	Configuration Management Manager
CMS	Configuration Management System
COL	Combined Operating License
COTS	Commercial Off-The-Shelf Software
CRDT	Control Room Design Team
CRT	Cathode Ray Tube
CTS	Commitment Tracking System

D3	Defense-in-Depth and Diversity
D/A	Digital/Analog
DCD	Design Control Document
DCIS	Distributed Control and Information System
DLD	Detailed Logic Diagrams
DOD	Department of Defense
DRF	Design Record File
EAL	Emergency Action Level
ECN	Engineering Change Notice
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedure
EPG	Emergency Procedure Guideline
EPRI	Electric Power Research Institute
ERO	Emergency Response Organization
ESE	Electrical System Engineer
ESF	Engineering Safety Features
FAPCS	Fuel and Auxiliary Pools Cooling System
FDDR	Field Deviation Disposition Report
FDI	Field Disposition Instruction
FRA	Functional Requirements Analysis
FSS	Full Scope Simulator
GDC	General Design Criteria
GDCS	Gravity Driven Cooling System
GEH	GE Hitachi Nuclear Energy
GPP	General Plant Procedures
HA	Human Action
HED	Human Engineering Discrepancy
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HI	Human Interaction
HPES	Human Performance Evaluation System
HPM	Human Performance Monitoring

HRA	Human Reliability Analysis
HSI	Human-System Interface
HSS	Hardware/Software Specification
I&C	Instrumentation and Controls
IO	Input/Output
IOP	Integrated Operating Procedure
IPD/S	Integrated Plant Design/Simulation
ISV	Integrated System Validation
IV&V	Independent Verification and Validation
IVVT	Independent Verification and Validation Team
LCS	Local Control Station
LD	Logic Diagram
LERF	Large Early Release Frequency
MCR	Main Control Room
MCRP	Main Control Room Panel
[[]]
MMIS	Man-Machine Interface System
N-DCIS	Nonsafety-related Distributed Control and Information System
NIM	Network Interface Modules
NMS	Neutron Monitoring System
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control
O&M	Operation and Maintenance
OER	Operating Experience Review
OFE	Operational Failure Event
P&ID	Piping and Instrument Diagram
PAS	Plant Automation System
PDM	Project Design Manual
PDMS	Product Data Management System
PFRA	Plant Functional Requirements Analysis
PLL	Product Line Leader
PM	Project Manager

PMM	Program Management Manual
PMT	Project Management Team
POC	Point of Contact
PRA	Probabilistic Risk Assessment
PSAR	Preliminary Safety Analysis Report
QA	Quality Assurance
Q-DCIS	Safety-Related Distributed Control and Information System
RAW	Risk Achievement Worth
RE	Responsible Engineer
RG	Regulatory Guideline (Reg Guide)
RMU	Remote Multiplexing Unit
RO	Reactor Operator
RSE	Responsible System Engineer
RSS	Remote Shutdown System
RTPE	Responsible Technical Project Engineer
RPV	Reactor Pressure Vessel
RV	Responsible Verifier
S&Q	Staffing and Qualification
SAE	Simulation Assisted Engineering
SAG	Severe Accident Guideline
SAM	Severe Accident Management
SAMG	Severe Accident Management Guideline
SBD	Software Build Description
SBWR	Simplified Boiling Water Reactor
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SDP	Software Development Plan
SDS	System Design Specification
[[]]
SFGA	System Functional Gap Analysis
SFRA	System Functional Requirements Analysis
SIP	Software Installation Plan

SIntP	Software Integration Plan
SLD	Simplified Logic Diagrams
SLU	System Logic Unit
SME	Subject Matter Expert
SMP	Software Management Plan
SMPM	Software Management Program Manual
SOMP	Software Operation and Maintenance Plan
SOP	System Operating Procedure
SPDS	Safety Parameter Display System
SPE	Software Project Engineering
SPTMS	Suppression Pool Temperature Monitoring Subsystem Function
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Plan
SQAPM	Software Quality Assurance Program Manual
SRO	Senior Reactor Operator
SRS	Software Requirements Specification
SSA	Software Safety Analysis
SSP	Software Safety Plan
SST	Software Safety Analysis Team
STP	Software Test Plan
STrngP	Software Training Plan
SVT	Software Validation Test
SVVP	Software Validation & Verification Plan
SW	Software
SYAT	System Acceptance Testing
SyRS	System Requirement Specification
TA	Task Analysis
TM	Team Member
TNA	Training Needs Assessment
TSC	Technical Support Center
TSL	Training Services Lead
TSG	Technical Support Guideline

V&V	Verification and Validation
VDU	Visual Display Unit
WDP	Wide Display Panel
WL	Walk-Through Leader

2. APPLICABLE DOCUMENTS

Applicable documents include supporting documents, supplemental documents, codes and standards and are given in this section. Supporting documents provide the input requirements to this plan. Supplemental documents are used in conjunction with this plan.

2.1 SUPPORTING DOCUMENTS AND SUPPLEMENTAL GEH DOCUMENTS

2.1.1 SUPPORTING DOCUMENTS

The following supporting documents were used as the controlling documents in the production of this plan. These documents form the design basis for activities stated in this plan.

- (1) NP-2010 COL Demonstration Project Quality Assurance Plan, NEDO-33181, Rev 5.
- (2) ESBWR DCD, Chapter 18, Rev 5 (26A6642BX).
- (3) ESBWR Design Control Document, Chapter 15, Rev 5 (26A6642BP).
- (4) ESBWR Design Control Document, Chapter 7, Rev 5 (26A6642AW).
- (5) NP-2010 COL Demonstration Project, Project Management Manual; NEDC-33216, Rev 5.

2.1.2 SUPPLEMENTAL DOCUMENTS

The following supplemental documents are used in conjunction with this document plan.

- (1) NEDO-33262, Rev 2, ESBWR HFE Operating Experience Review Implementation Plan.
- (2) NEDO-33219, Rev 2, ESBWR HFE Functional Requirements Analysis Implementation Plan.
- (3) NEDO-33220, Rev 2, ESBWR HFE Allocation of Functions Implementation Plan.
- (4) NEDO-33221, Rev 2, ESBWR HFE Task Analysis Implementation Plan.
- (5) NEDO-33266, Rev 2, ESBWR HFE Staffing and Qualifications Implementation Plan.
- (6) NEDO-33267, Rev 3, ESBWR HFE Human Reliability Analysis Implementation Plan.
- (7) NEDO-33268, Rev 3, ESBWR HFE Human-System Interface Design Implementation Plan.
- (8) NEDO-33276, Rev 2, ESBWR HFE Verification and Validation Implementation Plan.
- (9) NEDO-33274, Rev 3, ESBWR HFE Procedure Development Implementation Plan.
- (10) NEDO-33275, Rev 2, ESBWR HFE Training Development Implementation Plan.
- (11) NEDO-33278, Rev 3, ESBWR HFE Design Implementation Plan.
- (12) NEDO-33277, Rev 3, ESBWR HFE Human Performance Monitoring Implementation Plan.
- (13) NEDE-33226P and NEDO-33226, Rev 3, ESBWR I&C Software Management Program Manual.
- (14) NEDE-33245 and NEDO-33245, Rev 3, ESBWR I&C Software Quality Assurance Program Manual.

- (15) NEDO-33251, Rev 1, ESBWR I&C Defense-in-Depth and Diversity Report.
- (16) NEDE-33295P, Rev 0, ESBWR Cyber Security Program Plan.

2.2 CODES AND STANDARDS

The following codes and standards are applicable to the HFE program to the extent specified herein.

- (1) IEEE Standard 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 2003.
- (2) IEEE Standard 828, Standard for Software Configuration Management Plans, 1990.
- (3) IEEE Standard 1012, Standard for Software Verification and Validation Plans, 1998.
- (4) IEEE Standard 1042, Guide to Software Configuration Management, 1987.
- (5) IEEE Standard 1074, Standard for Developing Software Life cycle Processes, 1995.

2.3 REGULATORY GUIDELINES

- (1) NUREG-0800, Rev. 1, Standard Review Plan, Chapter 18, Human Factors Engineering, February, 2004.
- (2) NUREG-0800, Rev. 4, Standard Review Plan, Chapter 7; Branch Technical Position (BTP) HICB-14 R4, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, June, 1997.
- (3) RG 1.152, Rev 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, January, 2006.
- (4) RG 1.173, Rev. 0, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants, September, 1997.
- (5) RG 1.174, Rev. 1, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, November, 2002.
- (6) NUREG-0700, Rev. 2, Human-System Interface Design Review Guidelines, May, 2002.
- (7) 10CFR 50, Appendix - A, General Design Criteria for Nuclear Power Plants.
- (8) 10CFR 52, Licenses, Certifications, and Approvals for Nuclear Power Plants.
- (9) NUREG-0737, Clarification of TMI Action Plan, November, 1980.
- (10) NUREG-0711, Rev. 2, Human Factors Engineering Program Review Model, February, 2004.

2.4 DOD AND DOE DOCUMENTS

None.

2.5 INDUSTRY AND OTHER DOCUMENTS

These standards and guidance documents provide guidance for the implementation activities.

NEDO-33217, Rev. 4

- (1) ABWR Owners Group Accident Management Guidelines Overview Document, Rev. 1, November, 1997.
- (2) EPRI NP-4350, Human Engineering Design Guidelines for Maintainability, 1985.
- (3) NEI 91-04, Rev 1, Severe Accident Issue Closure Guidelines, Nuclear Energy Institute, | Report NEI 91-04, 1994.
- (4) BWROG Emergency Procedure and Severe Accident Guidelines, Rev 2, March, 2001.

3. METHODS

3.1 MMIS AND HFE MANAGEMENT PLAN

3.1.1 BACKGROUND FOR MMIS AND HFE MANAGEMENT PLAN

Chapter 7, "Instrumentation and Control Systems" of the ESBWR DCD [2.1.1(4)] defines MMIS as the systems that perform the monitoring, control, and protection functions of the plant. The MMIS is comprised of the following functions:

- Data gathering equipment, which monitors equipment and process variables.
- Data communication equipment, which transmits equipment and process variables between data processing equipment and plant equipment.
- Data processing equipment, which manipulates data for use by plant personnel and/or automatic protection and control equipment.
- Plant information display and control equipment that provides alarm and display media for plant personnel. This equipment provides access to plant processes, equipment status, and controls for operating plant equipment.
- Output processing equipment comprised of electrical devices and circuitry that provide the necessary interfaces between plant controls and plant equipment actuators. Examples would include signal conversion equipment providing signals to plant equipment, including:
 - Analog/Digital (A/D) and Digital/Analog (D/A) converters.
 - Local converters that are not part of the actuators.
 - Remote Multiplexing Units (RMUs).
 - System Logic Units (SLUs).
 - Network Interface Modules (NIMs).

The MMIS encompasses instrumentation and control systems provided as part of the ESBWR that perform the monitoring, control, alarming, and protection functions associated with all modes of plant normal operation (that is, startup, shutdown, standby, power operation, and refueling). Also included are off-normal, emergency, and accident conditions. The requirements of this document are directed to the plant designers and are applicable to equipment supplied as part of the MMIS (See Subsection 1.2 Scope). The MMIS specifically includes:

- Instrumentation, including sensors and local instruments, for applicable safety and nonsafety systems throughout the plant.
- Automatic and manual controls for applicable safety and nonsafety systems.
- Protection functions that include applicable safety and nonsafety systems.
- Diagnostic systems that include rotating machinery diagnostics, neutron noise monitoring, and so forth.

- Monitoring and control stations for the plant systems, including the MCR, RSS, TSC, EOF, and LCS with a safety-related function or as defined by TA.
- Instrumentation and control power supplies, grounding, and environmental compatibility.
- Computer systems for control, data acquisition, display, storage and retrieval, monitoring and alarms, technical support, and operations support.
- Plant communications systems including data, visual, and voice intra-plant communication associated with plant operation and maintenance.

Additionally, the use of mockups and a dynamic simulator as tools for the design and verification and validation of the MMIS.

3.1.2 GOALS FOR MMIS AND HFE IMPLEMENTATION PLAN

The goal of the MMIS implementation process is to ensure the vital role personnel play in the plant operation is supported through human-centered design, development, and operational activities. This ensures safe efficient production of electric power at ESBWR plants can be accomplished under normal and emergency conditions.

To support this goal, the MMIS and HFE Implementation Plan serves to:

- (1) Create plans in accordance with NRC guidelines.
- (2) Establish baseline design inputs from previous pertinent ABWR system control room designs.
- (3) Prepare an ESBWR to ABWR gap analysis. This analysis will be conducted in conjunction with an operating experience review.
- (4) Establish methods and tools to monitor the execution of the MMIS and HFE plans from initial design through turnover to the licensee.
- (5) Establish project plan methodology and guidelines that follow standard HFE and I&C practices and processes.
- (6) Monitor the activities for MMIS design and system hardware/software design to ensure that outcomes meet the commitments of ESBWR DCD Chapter 18 [2.1.1(2)].

3.1.3 REQUIREMENTS FOR MMIS AND HFE MANAGEMENT PLAN

3.1.3.1 PROCESS PROCEDURES

Engineering activities in this plan are conducted in accordance with the ESBWR Project Policies and Procedures (P&Ps), Engineering Operating Procedures (EOPs), and Engineering Service Instructions (ESIs) that implement the GE Hitachi Nuclear Energy (GEH) Quality Assurance (QA) plans as described in NEDC-33181 [2.1.1(1)].

3.1.3.2 INDEPENDENT REVIEW AND VERIFICATION

In accordance with GEH Project QA Plan [2.1.1(1)], the MMIS design process provides for independent verification of all aspects of the MMIS design throughout the process.

The independent verification process ensures individual stages of the process are correct and the transfer of information from stage to stage has been properly accomplished.

The independent review process validates the overall MMIS accomplishes the intended functions and verifies that the individual steps in the process have been properly executed.

3.1.3.3 DEFENSE-IN-DEPTH AND DIVERSITY ASSURANCE

The MMIS and HFE design process described in this plan provides assurance that enhancements to predecessor designs to accommodate ESBWR objectives do not compromise the ESBWR Defense-in-Depth and Diversity (D3) analysis [2.1.2(15)]. The D3 analysis is a design input to the System Functional Requirements Analysis and is iterated as any other engineering input to the process (See Subsection 3.2.4.1). Important aspects of defense-in-depth are identified in RG 1.174 [2.3(5)], and are evaluated to include:

- (1) A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- (2) No over-reliance on programmatic activities to compensate for weaknesses in plant design. This may be pertinent to changes in credited Human Actions (HAs).
- (3) System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.
- (4) Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed. Caution is exercised in crediting new HAs to verify the possibility of significant common cause errors is not created.
- (5) Independence of barriers is not degraded.
- (6) Defenses against human errors are preserved. For example, procedures are established for a second check or independent verification that risk-important HAs have been performed correctly.
- (7) The intent of the General Design Criteria (GDC) (Appendix A of 10CFR Part 50 [2.3(7)]) is maintained. Relevant GDC include:
 - a. 3 - Fire Protection.
 - b. 13 - Instrumentation and Control.
 - c. 17 - Electric Power Systems.
 - d. 19 - Control Room.
 - e. 24 - Separation of Protection and Control Systems.
 - f. 35 - Emergency Core Cooling System.
 - g. 38 - Containment Heat Removal.
 - h. 44 - Cooling Water.

3.1.3.4 SAFETY MARGINS

Safety margins are often used in deterministic analyses to account for uncertainty and quantify relative distance from safety limits or criteria. Maintaining adequate safety margins reduces the chance of various safety limits or criteria being violated.

If desired, it is also possible to add a safety margin 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.

3.1.3.5 CYBER SECURITY

The ESBWR Cyber Security Program Plan [2.1.2(16)] defines the requirements for the development and management of an effective cyber security program for the ESBWR.

This plan captures the cyber security requirements from applicable regulatory requirements and guidance. The plan provides guidance to the HFE and software implementation plans in the application of a comprehensive cyber security program plan for the ESBWR.

3.1.4 GENERAL APPROACH FOR MMIS AND HFE MANAGEMENT PLAN

The Software Project Engineering (SPE) group was established within the New Units Engineering organization of GEH Energy Nuclear Engineering to design and manage the interfaces between the control room operational staff and the plant instrumentation and control equipment. SPE combines the expertise of human factors, BWR operations, software design, and simulation engineering to establish a cross-functional team with the design disciplines to achieve the safety and efficiency goals for the ESBWR program.

The ESBWR MMIS and HFE Implementation Plan establishes plans for the implementation of the MMIS design activities and provides guidance and support for the performance of plan activities.

A Baseline Review Record (BRR) establishes the design inputs from predecessor plants. The most recent predecessors are the ABWR plants including the Lungmen project (Taiwan Power), Kashiwazaki-Kariwa 6 & 7 (TEPCO), Hamaoka 5 (Chubu Electric), and Shika 2 (Hokuriku Electric Power).

The project organization and teams are formed combining the proper experience and disciplines to successfully perform project tasks. Procedures and standards are established to guide the teams' performance. The progress and outcomes of project activities are managed using GEH standard procedures and processes as well as project specific implementation plans.

As described in the ESBWR Design Control Document [2.1.1(2)], a fleet-wide owners' group is planned to provide a means for consistently maintaining safety performance levels established through staffing, training, procedures, and design. While individual ESBWR licensees' programs may vary in content and level of detail, the standards established by the fleet-wide owners' group are followed.

3.1.4.1 PROJECT ORGANIZATION

The project organization is established to design, control, and manage the equipment/computer/software/hardware interfaces. The project organization will ensure independence is maintained

between the design organization and quality assurance and between the software safety and verification and validation (V&V) organizations. The project organization is shown on Figure 3.1.4-1, Engineering Quality and Project Management Organization.

The project organization performs the following functions:

- I&C and Electrical Systems Engineering.
- Software Project Engineering (SPE).
- Human Factors Engineering (HFE).
- Configuration Management.
- Project Controls.
- Training.

[[

]]

Figure 3.1.4-1. Engineering, Quality and Project Management Organization

(1) I&C and Electrical Systems Engineering

The I&C organization comprises the GEH I&C/Electrical Design organization and the (GEH and non-GEH) hardware/software supplier organization. The GEH I&C/Electrical Design organization comprises the I&C/Electrical Engineering Manager, the system Technical Project Engineers (TPEs), and the Responsible System Engineers (RSE).

The I&C/Electrical Engineering Manager is responsible for overall performance and schedule of the I&C effort, including the management and direction of the system TPEs, system engineers, and hardware/software supplier organizations.

The platform TPEs are responsible for day-to-day management, coordination, and scheduling of the system design and software development effort. They are also responsible for interfacing with the system engineers and the hardware/software supplier organizations and providing status reports to management.

The RSEs are responsible for the ISC system design that includes production of the applicable sections of the Design Control Document (DCD), System Design Specifications (SDS), Logic Diagrams (LD), and various databases to support the design. For nonsafety-related systems, the RSEs are responsible for verifying the software produced by the hardware/software supplier organizations meets requirements.

The hardware/software supplier organizations produce the software and firmware in accordance to requirements established in the HFE and software development activities. The hardware/software supplier organizations may be GEH or non-GEH. A single Point of Contact (POC) is assigned by the hardware/software supplier organization to interface with the TPE.

(2) Software Project Engineering (SPE)

The SPE is independent of the design team to ensure organizational freedom to perform the quality tasks without undue pressure or conflict of interest related to budget and schedule.

The following SPE teams are established to support project tasks:

- Independent Verification and Validation Team (IVVT).
- Software Safety Team (SST).
- Baseline Review Team (BRT).
- Simulation Assisted Engineering Team (SAE).
- Human Factors Engineering Team (HFE).

The roles and responsibilities of the software teams (IVVT, SST, and BRT) are defined in the SQAPM [2.1.2(14)].

The HFE team, with the support of other engineering staff, prepares the various implementation plans required to support the HSI design activity, and manages the activity through final validation of the implemented design. 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 HFE design team throughout the process.

The HFE design team is comprised of at least the following areas of expertise:

- Technical project management.
- Systems engineering.
- Nuclear engineering.
- Instrumentation & Control engineering.
- Architect engineering.
- Human factors.
- Plant operations.
- Computer systems engineering.
- Plant procedure development.
- Personnel training.
- System safety engineering.
- Reliability, availability, maintainability, and inspection expertise.
- Quality assurance.
- HRA/PRA.
- Cyber security.

As a part of the HFE design team, a special Control Room Design Team (CRDT) is established to coordinate the design of the MCR, Remote Shutdown panels, and LCSs. The CRDT is comprised of members from the HFE design team and include involvement by Combined Operating License (COL) applicant staff familiar with plant engineering, operations, and maintenance.

The duties of the HFE design team are to establish and perform the activities as defined in this plan. The HFE design team's specific duties are to guide and oversee the design implementation activity and to ensure the execution and documentation of each step in the activity is carried out in accordance with the established program and procedures.

The HFE design team has the authority to

- Ensure all its areas of responsibility are accomplished and to identify problems in the implementation of the HSI design.
- Determine where its inputs are required and to access work areas and design documentation.
- 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 licensee is accomplished.

The HFE design team is responsible for:

- Developing all HFE plans and procedures.
- Overseeing and reviewing HFE design, development, test, and evaluation activities.

- Initiating, recommending, and providing solutions through designated channels for problems identified in the implementation of HFE activities.
- Verifying the solutions to problems have been implemented.
- Assuring that HFE activities comply with the HFE plans and procedures.
- Ensuring the activities of the Project Quality Plan [2.1.1(1)] are followed.
- Reviewing the methods for MMIS operating experience.
- Scheduling HFE activities and milestones.

(3) Training

Training is part of the Nuclear Services organization. The Training Services Lead (TSL) is responsible for ensuring the training requirements are accomplished.

(4) Configuration Management Manager

The Configuration Management Manager (CMM) has the overall responsibility and authority for the Configuration Management System (CMS) which is referred to as the Product Data Management System (PDMS).

Configuration management is responsible for defining the configuration management process and tools, as well as execution of PDMS to maintain and control traceable records of:

- Design requirements and inputs.
- Design activities.
- Design outputs.
- Authorizations to execute change requests to the controlled records.
- Approvals of the execution of change requests.

(5) Software Quality Assurance Manager

The SQA Manager interfaces with the SPE Manager, and has the overall responsibility and authority for the SQA program. The SQA Manager and responsibilities are addressed in the SQAPM [2.1.2(14)].

(6) Project Management Team

The Project Management Team (PMT) is responsible for the commercial aspects of the project. A commercial Project Manager (PM) is assigned to oversee each of the projects, and is responsible for delivering the commitments of a Purchase Order and/or Sales Contract for product delivery.

The PMT activities include:

- Project work planning.
- Development and maintenance of the integrated project schedule or plant specific project schedule. The TPE supporting the I&C Manager and the SPE task leads provide input and support for this activity.

- Update the integrated schedule to show that project tasks are completely and accurately reflected.
- Assignment of project resources and skill sets to support the project needs.
- Preparation of project progress reports.
- Project risk management assessment.
- Project budgeting.
- Engineering procurement and/or fabrication.
- Communication with COL applicant and vendors.

(7) Team Composition for Project Activities

Table 3.1.4-1 provides the team composition for the project activities described in implementation plans in Subsection 2.1.2. The table provides the needed areas of team expertise for the performance of the activity.

3.1.4.2 MANAGEMENT PROCESS AND PROCEDURES

General Process Procedures - The project team executes its responsibilities through the processes established in ESBWR Project Policies and Procedures (P&Ps), Engineering Operating Procedures (EOPs), and the Engineering Service Instructions (ESIs) that implement the GEH Nuclear Energy Nuclear QA plans described in NP-2010 COL Demonstration Project Quality Assurance Plan [(2.1.1(1))].

The GEH internal procedures address:

- Assigning activities to individual team members.
- Governing the internal management of the team.
- Making management decisions.
- Making design decisions.
- Governing equipment design changes.
- Design team review of products.

The MMIS and HFE Implementation plan and its subordinate implementation plans are controlled documents under configuration control in accordance with the GEH Project QA Plan [2.1.1(1)]. When improvements or deficiencies are identified, a Corrective Action Request (CAR) is issued to document the condition. The CAR tracks activity and ensures corrective and preventive actions are implemented. The CAR also ensures the actions are effective in either eliminating the deficiency or improving the affected plans.

A change or revision to this document and its subordinate plans prior to certification approval is established in accordance with the GEH Project QA Plan [2.1.1(1)] and applicable ESBWR Project and Procedures. To make a change or revision to this document and the subordinate plans listed in Subsection 2.1.2 after certification approval, the changes must in accordance with Processes for Changes and Departures to Tier 2 Information within the applicable appendix for the ESBWR to 10CFR 52 [2.3(8)].

A project work instruction is developed to further define project scope, activities and deliverables for each implementation plan listed in Subsection 2.1.2. The project work instruction is updated as changes occur in the work scope, design inputs, and outputs.

Specific project controls for the management of the software process are described in the Software Management Program Manual [2.1.2(13)] and requirements and procedures for the quality assurance of the software development process are described in the Software Quality Assurance Program Manual [2.1.2(14)].

Process Management Tools - Tools and techniques (Ex: review forms) to be utilized by the team to verify application of SPE/HFE efforts are identified in the HFE and software implementation plans listed in Subsection 2.1.2, or in their respective work instructions.

Integration of HFE and Other Plant Design Activities - The integration of design activities is established in the ESBWR Project Management Manual [2.1.1(5)], GEH Project QA Plan [2.1.1(1)] and herein.

Specific design inputs are described in the individual activity plans listed in Subsection 2.1.2. Figure 3.1.4-2, Process Feedback and Issues Disposition, depicts a process for identifying, documenting, and communicating general (out of process) issues encountered in design activities.

A summary of the HFE integration into the ESBWR design process is provided in Subsection 3.2.4.2.

Feedback and Issues Disposition

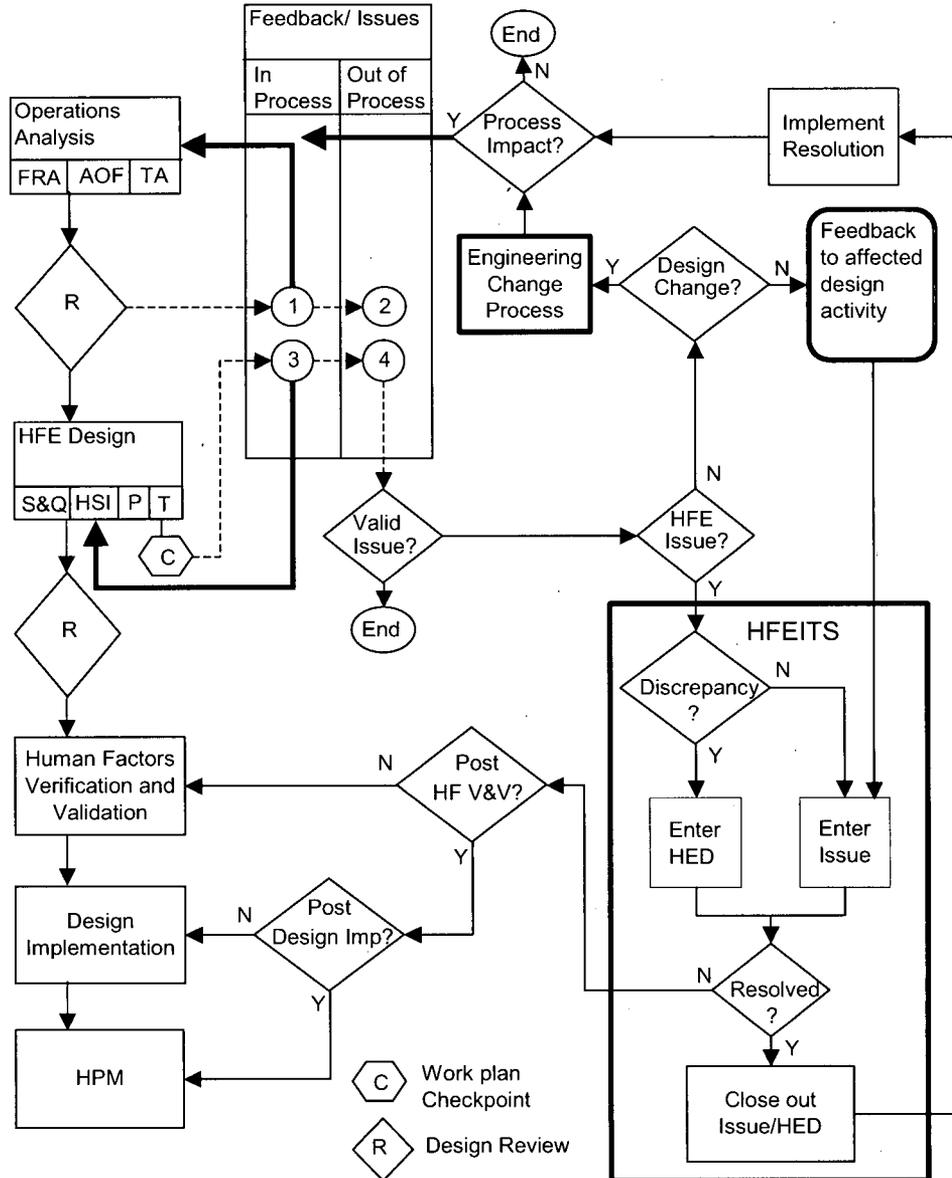


Figure 3.1.4-2. Process Feedback and Issues Disposition

Process Feedback and Issues Disposition - Figure 3.1.4-2 demonstrates two feedback processes within the HFE program; design reviews (R) and work instruction checkpoints (C), which identify both in-process and out-of-process issues.

Design reviews are formal processes as described in Subsection 3.1.4.2, while requirements and conduct of work instructions checkpoints are established in the work instructions of the individual activities.

In-process issues and feedback are directed to the affected activities through normal project communications. Out-of-process issues are documented and resolved in either the Engineering Change Process, described in GEH Project QA Plan [2.1.1(1)], or the Human Factors Engineering Issue Tracking System (HFEITS), described in Subsection 3.1.4.3, and communicated to the appropriate design activities.

HFE Interfaces to Software Development - The HFE interfaces to the software development process are depicted in Figure 3.1.4-3, HFE Interface to Software Development. This is expanded in the HFE and software implementation plans listed in Subsection 2.1.2, which provide additional detail for system designer integration.

HFE Program Milestones - HFE milestones are identified so evaluations of the effectiveness of the HFE effort can be established 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 is available for review.

Design reviews - Design reviews identified in the program schedule are conducted in accordance with GEH operating procedures as established in the GEH Project QA Plan [2.1.1(1)].

Walk-Through reviews - Walk-through reviews are conducted in accordance with the guidelines in Appendix D, Guidelines for the Conduct of Walk-Throughs.

HFE and Software Documentation - HFE and software documentation items are identified here and in the specific implementation plans listed in Subsection 2.1.2(13) and (14). Management of the documents is controlled by the GEH Project QA Plan [2.1.1(1)] and includes retention and limited access requirements.

The HFE and software implementation plans describe summary reports that contain the primary information the NRC staff will need for its review. A Human Factors Engineering Issue Tracking System described in Subsection 3.1.4.3 compiles and maintains issues and discrepancies for team resolution as controlled documents within the GEH Project QA Plan documentation system [2.1.1(1)].

Subcontractor HFE Efforts - HFE requirements are included in each subcontract and the subcontractor's compliance with HFE requirements are periodically verified in accordance with the GEH Project QA Plan [2.1.1(1)].

Design Bases and Life Cycle Management - GEH maintains the standard ESBWR licensing bases of the standard ESBWR software configuration and software quality assurance throughout the development, validation and the operating phases. Each licensee is responsible to maintain as-built design bases and SQA records during the operating life of the related ESBWR license. A fleet-wide owners' group provides a means of coordination between GEH and the ESBWR licensees to facilitate and maintain uniformity of:

[[

]]

[[

[[

]]

]]

3.1.4.3 HUMAN FACTORS ENGINEERING ISSUE TRACKING SYSTEM

Software problems and issues, HFE issues, and Human Engineering Discrepancies (HEDs) are tracked within the HFEITS. Figure 3.1.4-2, Feedback and Issues Disposition, depicts processes for identifying out-of-process issues, and discrepancies for tracking by HFEITS. HFEITS facilitates resolution of problems, issues and HEDs by providing the means to record and track issues throughout the process (life cycle) of design, development, and evaluation. Tracking by the SPE/HFE team ends when design implementation activity is completed and tracking is transferred to the licensee.

(1) Issue and HED Identification and Tracking

The HFEITS ensures problems, issues, and HEDs identified throughout the development and evaluations of the MMIS implementation are addressed. Project work instructions for HFEITS describe:

- How to identify problems, issues, and discrepancies and enter them with a unique tracking number into the log.
- An administrative position responsible for maintaining the tracking system and tracking logs.
- The methodology for the evaluation and documentation of proposed resolutions and the residual effects, criticalities, and likelihoods of the implemented resolutions for the issue. This methodology follows the one described in NUREG-0800 [2.3(1)] and applies the content and process contained in the HFE Verification and Validation Implementation Plan.
- Responsibilities for SPE/HFE team members and CRDT members for issue identification, resolution, and closeout.
- The format of the reports from the HFEITS for use by the design team.

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

(2) Issue and HED Resolution Verification

Resolution verification is the process element that verifies HFEITS issues are evaluated and documented. Identified HEDs are justified, analyzed, prioritized, and documented, so design solutions can be developed and evaluated. In this way, the modification can be adequately addressed in the design.

Issues that cannot be resolved until the plant full scope simulator is available are identified and incorporated into the design verifications of the software and HFE V&V activities. Those issues that cannot be resolved until the plant facility is available are addressed in the Design Implementation activity [2.1.2(11)].

The final resolution of remaining HEDs and open issues, and transfer of HFEITS is accomplished in the Design Implementation activity [2.1.2(11)].

3.2 HFE PROCESS

3.2.1 BACKGROUND FOR HFE PROCESS

For the safe operation of the plant, a functional requirements analysis defines functions at plant and system levels. An allocation of functions determines if human, machine, or a combination of both perform actions to accomplish functions. The information and control needs established from the analysis of tasks provide the input for the design of Human System Interfaces (HSIs) and standard plant procedures and training.

The list of plant functions and parameters, function allocations, control and display needs, and the HSI design requirements establish inputs for the software development activities.

A full-scale ESBWR control room mockup and part-task simulator serves 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 are 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 is the principal means to facilitate plant evaluations throughout the entire MMIS implementation process. As development on the mockup/part-task simulator proceeds, the intention is to complete the MMIS design process with final validation taking place using the ESBWR full-scope simulator.

3.2.2 GOAL FOR HFE PROCESS

The general objectives of the program can be stated in human-centered terms, which as the HFE program develops, are refined and used as a basis for HFE planning, test, and evaluation activities. Generic human-centered HFE design goals include:

- Personnel tasks can be accomplished within time and performance criteria.
- HSIs, procedures, staffing/qualifications, training and management, and organizational elements support a high degree of operating crew situation awareness.
- Plant design and allocation of functions maintain operator vigilance and provide acceptable workload levels that minimize periods of operator under load and overload.
- Operator interfaces minimize operator error and provide for error detection.

HSI design supports the capability of the operating crew to recover from previous decisions and actions that did not achieve intended results.

3.2.3 REQUIREMENTS FOR HFE PROCESS

- (1) The proven MMIS design of the BWR and ABWR predecessor plants serve as a design basis for the ESBWR MMIS implemented under this plan. The most recent predecessors are the ABWR plants Lungmen (Taiwan Power), Kashiwazaki-Kariwa 6 & 7 (TEPCO), Hamaoka 5 (Chubu Electric), and Shika 2 (Hokuriku Electric Power).
- (2) It is recognized that different operational needs, human factors considerations, and industry standards, codes, and regulations exist between the predecessor plants and the ESBWR MMIS implemented under this plan. An analysis of the design differences between the ABWR and ESBWR establishes a Baseline Review Record (BRR). Potential differences

may lead to changes in the MMIS design, and these changes are analyzed against the current ESBWR plans. Therefore, MMIS design changes are the result of ABWR-ESBWR plant differences and new requirements identified in the ESBWR specific plans.

- (3) The ESBWR DCD Subsection 18.6 [2.1.1(2)] establishes a preliminary staffing assumption meeting regulatory requirements and staffing considerations addressed in the ESBWR HFE Staffing and Qualifications Implementation Plan [2.1.2(5)].
- (4) Safety-related systems monitoring displays and control capability are provided in full compliance with regulations regarding electrical separation and independence.
- (5) The MMIS design is reliable and provides functional redundancy such that sufficient display and control is available in the MCR and remote locations to conduct an orderly reactor shutdown to cold conditions. Analysis shows that meantime between forced outages caused by failures of MMIS equipment is greater than fifty reactor-operating years. In addition, the mean time between MMIS equipment failures that result in a reduction in plant availability is greater than five years over the entire design life of MMIS equipment.
- (6) The principal functions of the Safety Parameter Display System (SPDS) as required by Supplement 1 of NUREG-0737 [2.3(9)] are integrated into the MMIS and HSI design.
- (7) Accepted HFE principles as applied to the needs of the ESBWR plant operators are utilized for the MMIS and HSI design.
- (8) The ESBWR design utilizes the design of the ABWR predecessor plants and the US certified ABWR plant design. Deviations from these MMIS designs are made to accommodate:
 - a. Regulatory updates, such as NUREG 0700 (Rev 2) [2.3(6)]; NUREG 0711 (Rev 2) [2.3(10)]; and NUREG 0800 (Rev 1) [2.3(1)], which were issued after ABWR design certification and design of predecessor ABWRs.
 - b. Differences in operational needs, human factors considerations, and industry standards, codes, and regulations that exist between reference ABWRs and the identified ESBWR Baseline Review Record (BRR). The differences may need to be reflected in design of the ESBWR MMIS.
 - c. HFE analysis specific for ESBWR, such as allocation of function and task analysis, which may be different from ABWR predecessor plants, and which would need to be reflected in design of the ESBWR MMIS.
 - d. Differences in DCIS vendor equipment designs and capabilities between vendors for ABWR predecessor plants, and ESBWR DCIS vendor equipment.
- (9) Standardization of Components minimizes the impact of obsolescence of MMIS equipment throughout the plant life. The MMIS design is modular in construction (both hardware and software) and standardizes MMIS equipment. The ESBWR design process establishes plans early in the project to identify what potential hardware (Ex: VDUs) may impact the design of the MCR panels over the life of the plant. ESBWR Program Plans and the Software Management Program Manual (SMPM) address standardization goals and requirements. Extensive use of HFE-established style guides and display primitives are incorporated.

- (10) Guidelines for Control System Data Gathering, Transmission, and Processing are provided in Appendix B. This includes guidance for:
- a. The ESBWR plant multiplexing system Distributed Control and Information System (Q-DCIS and N-DCIS).
 - b. Design Flexibility.
 - c. Data Transmission.
 - d. Signal Filtering.
 - e. Signal Processing.
 - f. Data Propagation Times.
 - g. Performance Margins.
 - h. Reliability Models.
 - i. Use of Industry Standards.
- (11) The MMIS only utilizes proven technology. Due to the advantages offered by modern technology over some of the technology at current operating BWRs, the incorporation of more modern technology is used wherever possible to improve existing designs.
- a. Criteria for Proven Technology - The proposed instrumentation, control and MMIS 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 (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 experience in existing light water reactors. For non-Q class (nonsafety-related systems), technology is considered "proven" if it has been evidenced by at least one (1) year of successful operation in existing light water reactors, fossil plants, or industry process plants, prior to the start-up date.
 - b. Criteria for Unproven Technology - GEH may employ up-to-date modern technology and design and understands that some designs, subsystems, systems, equipment or components 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, GEH may develop a methodology to receive equivalent experience. Such an approach is evaluated and considered acceptable if the following criterion are met:
 - i. A defined program of prototype testing which has been designed to verify their performance in the project MMIS application, has been completed and a detailed plan has been developed for the collection of one (1) year operation experience
 - ii. The proven designs, systems, subsystems, equipment or components have been evidenced by at least one (1) year of successful operation experience and can meet the basic functional requirements
 - iii. The needed experience data collection can be completed and assessed prior to the issuance of an Operating License. Determine if the base approach (up-to-date modern technology and design) is acceptable or if the back up approach must be

utilized. Neither of these two approaches may impact the overall project schedule.

(12) Appendix C, Guidelines for Design of HSI, includes guidance for:

- a. Electronic Displays
- b. Testability
- c. Maintainability
- d. Constructability
- e. Alarms

(13) Guidance for the design and review of the elements of the HFE process, as it relates to cyber security, is established in the ESBWR Cyber Security Program Plan [2.1.2(16)].

3.2.4 GENERAL APPROACH FOR HFE PROCESS

3.2.4.1 HFE PROCESS DESCRIPTION AND FLOW

Figure 3.2.4-1, HFE Process Flow Diagram, provides the overall flow of the HFE process. The process is comprised of Inputs, Operational Analysis, HFE Design activities, Verification and Validation, and Design Implementation and Human Performance Monitoring.

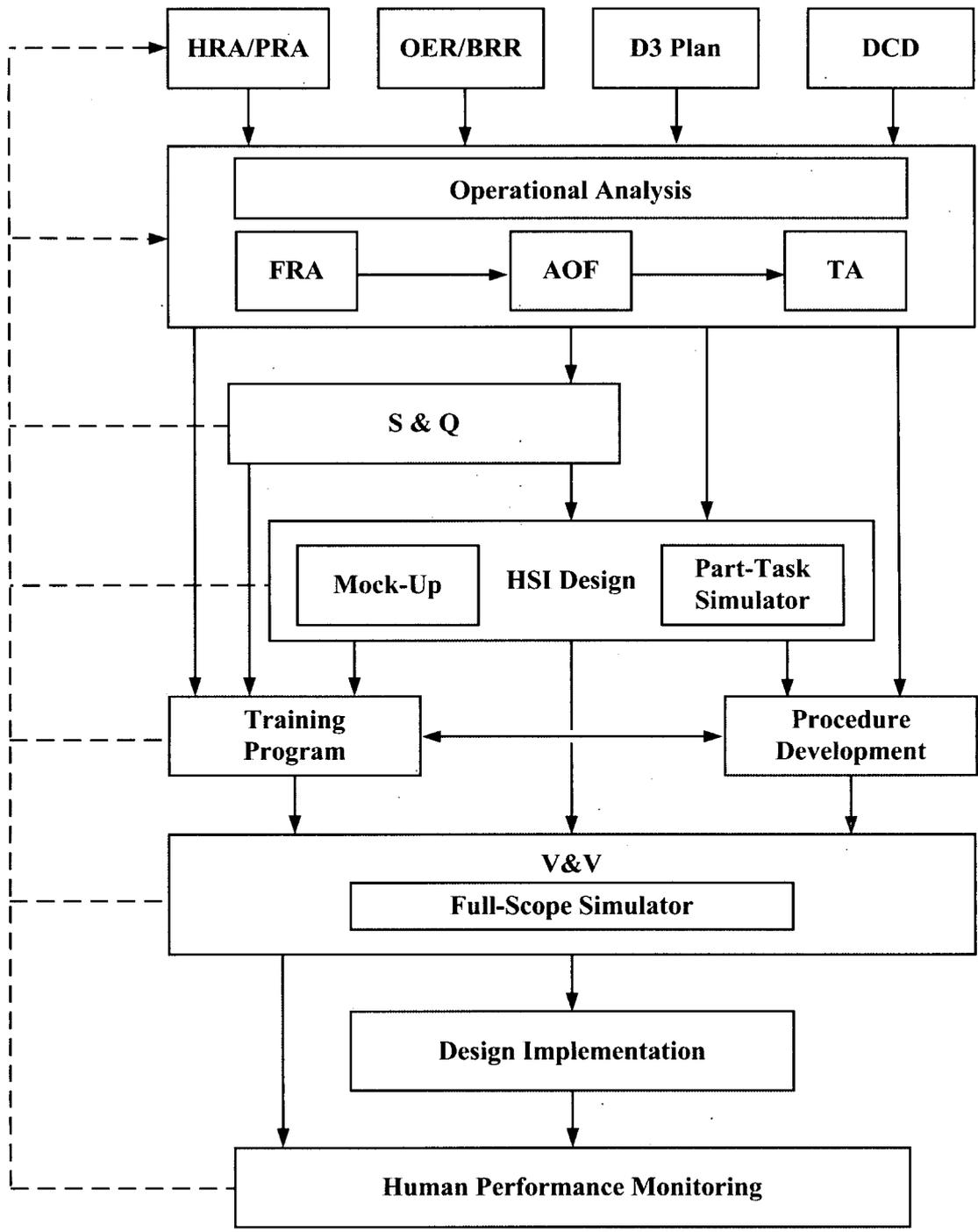


Figure 3.2.4-1. HFE Process Flow Diagram

[[

3.2.4.2 INTEGRATION OF THE HFE PROCESS INTO THE ESBWR DESIGN

[[

]]

3.2.4.3 COL APPLICANT INVOLVEMENT IN THE HFE PROCESS

On-site COL applicant representatives are integrated into the HFE design team. The HFE process involves the participation of licensed Senior Reactor Operators (SROs) from COL organizations to support standard plant design activities, including:

- Review planning and work documents from the COL applicant perspective
- Provide input to operating experience review activities
- Participate in operations analysis activities in which plant operations expertise is needed
- Participate on the Control Room Design Team (CRDT) providing input to HSI design from an operational perspective
- Provide guidance during procedures and training development
- Provide continuity for the HFE process when activities shift to on-site facilities.

The details for the involvement of the COL applicant team representatives are provided in the implementation plans [2.1.2] and are summarized in the results summary reports.

3.2.4.4 ACCIDENT MANAGEMENT

Accident Management consists of actions taken during the course of an accident by the Emergency Response Organization (ERO); specifically plant operations, technical support, and plant management staff. These actions are to:

- Prevent the accident from progressing to core damage.

- Terminate core damage once it begins.
- Maintain the capability of the containment as long as possible.
- Minimize on-site and off-site releases and their effects.

The BWR Owners' Group Emergency Procedure and Severe Accident Guidelines (SAGs) are the primary vehicles for implementing accident management strategies for the entire spectrum of severe accident response. This includes operator actions required to prevent or mitigate what are termed severe accidents for the current plant designs.

The EPGs and SAGs function together as an integrated set of instructions. Each EPG protects one of the principal barriers for radioactivity release through control of key plant parameters. The EPG contingencies form extensions to the top-level guidelines by providing more detailed instructions for controlling individual parameters under more degraded conditions. The SAGs extend the EPGs even further and address severe accident conditions.

Two documents take a generic approach to the development, maintenance, and implementation of the activities for accident conditions. The documents are the BWR Owners Group Accident Management Guidelines Overview Document and NEI 91-04 [2.5(1)], Rev. 1: Nuclear Energy Institute Severe Accident Issue Closure Guidelines [2.5(3)].

The current BWROG EOP/SAG guidelines [2.5(4)] were developed in an iterative process. The owners group used collegial input of both the technical analysis of plant capabilities for mitigation of proposed accident sequences, and the operating experience and input from the operating plants and their simulators.

Similarly for the ESBWR, the integration of the multiple resources providing a multi-faceted approach to the development of accident management guidelines is employed and is as follows:

- Compliance with current BWR Owners' Group Emergency Procedure and Severe Accident Guidelines and development of the related design-specific Appendix C data provide a technical review of plant capabilities within the realm of the design for both accident severity and system capability for mitigation.
- The ESBWR HFE Functional Requirements Analysis Implementation Plan [2.1.2(2)] provides the integrated functional review of the plant systems and their capabilities. This includes a review of boundaries for radioactive release and the plant functions used to protect each boundary in the event of analyzed transients.
- The ESBWR HFE Allocation of Functions Implementation Plan [2.1.2(3)] determines the required functions that achieve plant goals and system functions, distribution of functions among manual, remote manual, automatic, plant automation, and shared control, and the integrated human actions (HAs) required at the task level.

This section describes GEH and COL applicant roles and responsibilities for development of the accident management guidelines.

In support of the EOP/SAG development, GEH performs the following:

- Provide to the COL applicant, the technical basis for accident management, including Emergency Procedure Guidelines (EPGs), to ensure core damage prevention and mitigation. This includes meeting off-site dose limits.

- Translate the plant design bases into operation limitations and responses which will be developed into procedural guidelines and training.
- Confirm the plant design is compatible with the EPGs, the accident management program using the ESBWR PRA, and other relevant information. This includes cyber security risk analysis.
- Identify systems and equipment, which may be useful for accident management. These include safety and nonsafety onsite equipment.
- Develop procedures that will identify those actions needed to prevent and mitigate the effects of accidents. These include:
 - Preventing core damage.
 - Recovering from core damage without vessel failure.
 - Maintaining containment integrity.
 - Minimizing offsite radiation releases.
- Address applicable sections of NEI 91-04 Rev. 1 [2.5(3)]. These include:
 - Section 5.2 contains implementation guidance relative to the formal industry position on severe accident management.
 - Section 5.3.1, Severe Accident Management Guidance/Strategies for Implementation.
 - Section 5.3.2, Training in Severe Accidents, learning objectives and related training materials.
 - Section 5.3.3, Computational Aids for Technical Support.
 - Section 5.3.4, Information Needed to Respond to a Spectrum of Severe Accidents.
- Incorporate the BWROG Accident Management Guidelines Overview Document, Rev. 1, Section 6. This includes four interrelated assessments:
 - The Control Parameter Assessment obtains and processes plant data.
 - The Plant Status Assessment evaluates current plant conditions.
 - The System Status Assessment evaluates the availability of systems needed to implement EOPs and SAGs.
 - The EPG/SAG Action Assessment prioritizes system restoration actions and determines the appropriate timing of procedural actions.
- Prepare the accident management support documentation. This document provides a technical basis supporting severe accident management for the ESBWR. The information is based on the severe accident analysis performed with the MAAP 4.0.6 code. This information relates to severe accident phenomena in the Reactor Pressure Vessel (RPV) (metal-water reaction, onset of melting, core relocation and RPV breach) and associated conditions in the containment (radionuclide and hydrogen distribution and changes in pressure, temperature and suppression pool water level).

The severe accident management support document includes:

- Insights regarding the timing of key events for postulated severe accidents.
- Characteristic pressure and temperature profiles for a spectrum of postulated severe accidents.
- Characteristics of suppression pool level response for a spectrum of postulated severe accidents.
- Characteristics of core hydrogen generation and distribution in containment for a spectrum of postulated severe accidents.
- Insights regarding the use of alternate injection sources, such as AC-Independent Fire Water Addition System, to provide long term cooling.

To establish the accident management programs, the COL applicant is responsible for the following:

- Address applicable sections of NEI 91-04 Rev. 1, which include:
 - Section 5.3.2, Training in Severe Accidents, which performs training for implementers, evaluators, and decision makers.
 - Section 5.3.5, Delineation of Decision-Making Responsibilities.
 - Section 5.3.6, Utility Self Evaluation
- Identify systems and equipment which may be useful for accident management. These include safety and nonsafety plant-specific onsite, as well as offsite, equipment.
- Prepare Technical Support Guidelines. The Technical Support Guidelines (TSGs) provide guidance to Emergency Response Organization (ERO) personnel on supporting and optimizing accident management strategies implemented through plant EOPs and SAGs.
- Verify, validate, and maintain the EOPs and SAGs, and related basis documents.

3.2.5 APPLICATION

The MMIS design employs 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 provide reliability and protection against the propagation of failures. Application of signal validation to selected parameters is used to ensure plant operators have data of high quality. Multiplexed data communication is 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 reduces the overall maintenance calibration burden. Fiber optic cables for data transmission are used to provide high data transmission rates with electrical isolation and protection from electromagnetic interference at reduced costs.

The application of cyber security methods includes secure design/coding practices and training of operators to recognize cyber threats and results in a safe and secure plant.

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

It is expected that the MMIS 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 HSI design implementation activity includes the development of dynamic models for evaluating the overall plant response as well as individual control systems, including operator actions. These dynamic models are:

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

A dynamic part-task simulator is built to support the requirement for development of dynamic models. Using the part-task experience from the ABWR, an initial set of systems is identified for modeling. This includes the development of the graphical user interfaces used by the operator.

The part-task simulator is used in the preliminary ESBWR design and is expanded to include ESBWR-unique design features. As the ESBWR design progresses, the part-task simulator evolves through a series of iterative evaluations and results in the development of a complete control room full scope simulator. In addition, the simulator facility is intended to be the focal point for licensee operator evaluations and feedback checkpoints throughout the entire MMIS design process.

3.2.6 SUMMARY OF HFE PROCESS

The MMIS and HFE program described in this plan and the subordinate implementation plans represent a living program that extends throughout the life cycle of the facilities constructed from the standard plant design. The plans provide guidance for initial analyses, design, validation, implementation, and support the maintenance of human performance objectives in the operational phase of the plant facilities.

The HFE implementation plans are listed in Subsection 2.1.2, References (1) through (12) and include details for the following HFE activities:

- Operating experience review
- Functional requirements analysis
- Allocation of functions
- Task analysis
- Staffing and qualifications

- Human reliability analysis
- HSI design
- Procedure design
- Training design
- Human factors verification and validation
- Design implementation
- Human performance monitoring.

Results summary reports are prepared for each of the activities as described in the implementation plans.

3.3 MMIS SOFTWARE DEVELOPMENT

3.3.1 BACKGROUND FOR MMIS SOFTWARE DEVELOPMENT

The software development process is applied to the software products used to implement system controls and associated interfaces as described in Chapter 7, Instrumentation and Control Systems of the ESBWR DCD [2.1.1(4)].

The functions for the software products are primarily represented in the Q-DCIS and N-DCIS plant I&C systems and include various programmable logic controllers (hardware) outside of these systems. The scope of the MMIS software development is bound by the systems and functions described in Chapter 15 of the ESBWR DCD [2.1.1(3)].

The software development process is governed by two planning documents:

- Software Management Program Manual (SMPM) [2.1.2(13)]
- Software Quality Assurance Program Manual (SQAPM) [2.1.2(14)]

The SMPM includes the key planning documents for the Instrument and Controls (I&C) design team and governs the design and development activities for the Digital Computer-Based Instrumentation and Control software for the ESBWR.

The planning documents included in the SMPM are:

- Software Management Plan (SMP)
- Software Development Plan (SDP)
- Software Integration Plan (SIntP)
- Software Installation Plan (SIP)
- Software Operation and Maintenance Plan (SOMP)
- Software Training Plan (STrngP)

The SQAPM includes the software plans used by the Quality Assurance (QA) and the Software Project Engineering organizations.

The planning documents included in the SQAPM are:

- Software Quality Assurance Plan (SQAP)
- Software Verification & Validation Plan (SVVP).
- Software Safety Plan (SSP).
- Software Configuration Management Plan (SCMP).
- Software Test Plan (STP)

The SQAPM also includes the following testing:

- Software Testing.
- System Acceptance Testing.
- Factory Acceptance Testing.
- Site Acceptance Testing.

Together, the SMPM and the SQAPM include all software plans conforming to the guidance provided by NUREG 0800, Standard Review Plan [2.3(2)]. These plans are discussed from the perspective of software life cycle phases in Subsection 3.3.4.

3.3.2 GOAL FOR MMIS SOFTWARE DEVELOPMENT

The goal of the software development process is to produce high quality ESBWR Instrumentation and Control (I&C) software. I&C software provides for safe plant shutdown, Engineered Safety Features (ESF), control systems, and condition monitoring. A further goal of the I&C software is to support operator actions during plant evolutions and modes during event management. These goals are fulfilled through the implementation of a formally defined software lifecycle with planned design activities and a comprehensive quality management program.

The formally defined software lifecycle with planned design activities and comprehensive quality management program is discussed further in Subsection 3.3.4.

3.3.3 REQUIREMENTS FOR MMIS SOFTWARE DEVELOPMENT

3.3.3.1 SOFTWARE CLASSIFICATION

As shown below, the Software Class is determined and performed during the Software Safety Analysis (SSA) Preparation phase as described in Subsection 3.3.4. This scheme is based on IEEE Std. 1012, IEEE Standard for Verification and Validation Plans [2.2(3)].

Classification	Description
Software Class Q	Software performs functions classified as Safety-Related.
Software Class N3	Nonsafety-related systems software whose failure could challenge safety systems as defined below: Software whose inadvertent response to stimuli, failure to respond when required, response out-of-sequence could directly result in an accident or

	<p>transient as defined in the DCD, Chapter 15 [2.1.1(3)].</p> <p>Software that is intended to mitigate the result of an accident.</p> <p>Software that is intended to support recovery from the result of an accident.</p>
Software Class N2	<p>Software failure cannot adversely affect a safety-related function.</p> <p>Software failure results in inconvenience to the user.</p>

The type of quality tasks (i.e., IV&V and SSA) to be performed is dependent on the Software Class of the software products.

3.3.3.2 *CONFIGURATION MANAGEMENT AND CHANGE CONTROL*

Unless otherwise specified, the design outputs (including verification package, test and analysis reports) are configuration items (CIs) and are controlled as specified in the SCMP of the SQAPM [2.1.2(14)]. A discrepancy or deficient condition detected in a configuration item is resolved in accordance with the Change Control process described in the SCMP of the SQAPM [2.1.2(14)].

3.3.3.3 *REQUIREMENTS TRACEABILITY MATRIX*

A requirements traceability matrix is prepared for software Class Q and Software Class N design outputs. The traceability matrix indicates the linkage between each requirement imposed on the software by the input documents. The matrix allows traceability in both directions. It is organized so that as design, implementation, and validation take place, traceability information can be added for these activities. It is updated at the completion of each life cycle activity group. The final matrix permits tracing from the system requirements and design through the software requirements, design, implementation, integration, validation, and installation. Such tracing or traceability can be done with automated tools or by the use of a simple traceability matrix.

3.3.3.4 *INDEPENDENT VERIFICATION*

With the exception of the Baseline Review Record, Independent Verification and Validation (IV&V) is conducted on the design outputs as specified in the SVVP of the SQAPM [2.1.2(14)].

At the least, Independent Verification records consist of:

- a. Scope of the review, including acceptance criteria.
- b. Identification of the document reviewed.
- c. Statement of results and conclusion of the review.
- d. Date of review and identification of reviewer.
- e. (For anomalies) Identification of the specific criteria violated.

- f. (For anomalies) Identification of Responsible Engineer (RE) for resolution and commit date.

For Software Class N software product, independent verification is performed in accordance with the procedures described in the SMPM [2.1.2(13)]. The responsible verifiers are individual(s) or groups(s) who are competent to perform the verification based on knowledge and experience. The individual(s) cannot be the same engineer(s) who originated the design but may be from the same design team or organization.

For Software Class Q software product, the SPE IVVT team, which is an independent organization, performs independent verification in accordance with the SVVP of the SQAPM [2.1.2(14)]. The Responsible Verifier prepares the IV&V Review Report and the Anomaly Report, if necessary, documenting the Independent Verification and any anomalies observed. The report(s) are maintained within the GEH Design Record File (DRF) system.

3.3.3.5 TESTING

Testing is conducted to ensure the correctness and completeness of the requirements specified in the Requirements and Design Phase documents. The responsible design and verification group is specified for each life cycle phase.

3.3.3.6 SOFTWARE SAFETY ANALYSIS

Software Safety Analysis (SSA) is performed to ensure the safety of the Software Class Q for I&C systems software products. Safety is the most important consideration for the safety-related I&C, and takes precedence over budget and schedule. Software Project Engineering Software Safety Team (SPE SST), an independent organization, conducts the SSA in accordance with the SSP of the SQAPM [2.1.2(14)].

3.3.3.7 BASELINE REVIEW

Baseline review is performed at the completion of each of the software life cycle phases to ensure:

- a. The design information developed during the software life cycle phase adheres to the requirements.
- b. The V&V and SSA adhere to the procedures outlined in the SVVP and the SSP of the SQAMP [2.1.2(14)].

3.3.3.8 SOFTWARE DEVELOPED BY VENDORS

Software products developed by the vendors shall comply with the quality requirements of the SQAPM [2.1.2(14)]. If a vendor elects to follow its established SQA program, then the SQA program as defined in the contract/purchase order shall be reviewed and approved by the SQA Manager to ensure compliance with the requirements specified in the SQAPM [2.1.2(14)].

The implementation of cyber security program requirements for the software development and testing are described in the ESBWR Cyber Security Plan [2.1.2(16)].

3.3.4 GENERAL APPROACH FOR MMIS SOFTWARE DEVELOPMENT

The SMPM and SQAPM and their associated plans represent a software engineering process implemented in a traceable, planned, and orderly manner. They comprise a set of formal elements (methods, tools, documents, practices, standards and procedures) applied during the phases of the software life cycle. The phases, which are based on RG 1.152 [2.3(3)], RG 1.173 [2.3(4)] and IEEE 1074 [2.2(5)], are defined below:

- (1) Planning Phase – This is the definition of the project scope, methodologies, and resources to develop and maintain the deliverable software. The planning activities include, evaluation of system and COL applicant requirements, identification of resources, and development of schedule projections and risk assessments.

The Planning Phase Baseline Review Report documents successful completion of this phase.

- (2) Requirements Phase – This is the definition of the detailed functional and performance requirements, design constraints, and validation criteria.

The Requirements Phase Baseline Review Report documents successful completion of this phase.

- (3) Design Phase – This is the process that transforms requirements into an architectural representation of software, and a detailed representation of software.

The Design Phase Baseline Review Report documents successful completion of this phase.

- (4) Implementation Phase – This phase transforms the software design into software source or application codes. The implementation phase activities also include software code review and software functional test.

The Implementation Phase Baseline Review Report documents successful completion of this phase.

- (5) Test Phase – This phase includes the software validation testing, which tests for potential defects (errors). The results are documented in the software validation test report.

The Test Phase Baseline Review Report documents successful completion of this phase.

- (6) Installation Phase – This phase includes the installation of the validated software product in the target environment through installation in the plant.

[[

]]

The Site Acceptance Test (SAT) is the integrated systems test performed at the licensee site. The results are documented in the Site Acceptance Test Report.

The Installation Phase Baseline Review Report documents successful completion of this phase.

- (7) Operations & Maintenance (O&M) Phase – This phase involves the functional and operational life of the software product(s). It includes the operation, maintenance, calibration, surveillance, and other processes associated with the use of the system. Application is based on data, documentation, and procedures provided with each system in the O&M manual. Maintenance of the software includes procedures to maintain and resolve any operational anomalies. The O&M phase shall repeat previous phases as necessary to resolve issues and incorporate enhancements or modernizations required during plant operation.
- (8) Retirement Phase – In the retirement lifecycle phase, the effect of replacing or removing the existing software product from the operating environment must be addressed. These activities should include: user notification, the effect on existing software products that are to remain operational in the operating environment, and disposition of the retired software product including security disposition. The retired disposition includes deactivation, deletion or the removal of the software product from the operating environment, operational comparison of the new and old software products, and any documentation activities (including archiving of records).

Unless otherwise specified, the design team is responsible for preparation and maintenance of the design documentations described in this section. The design team is the team responsible for the detailed design, implementation and production of the software products.

3.3.5 SUMMARY OF SOFTWARE DEVELOPMENT PROCESS

The ESBWR computer-based, safety-related control system designs conform to RG 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants [2.3(3)]. Conformance with RG 1.152 comprises the functional and design requirements of computers used in safety systems of nuclear power plants. The conformance also comprises security of various hardware, controls and data networks with safety-related systems, as described in DCD Tier 2 Chapter 7 [2.1.1(4)]. The Cyber Security Program is described in NEDO-33295, ESBWR Cyber Security Program [2.1.2(16)]. The software process plans refer to the Cyber Security Program Plan for development and operation and maintenance of safety-related software that conform to RG 1.152 and endorse IEEE Std. 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations [2.2(1)], for the functional and design requirements of computers used in safety systems of nuclear power plants. IEEE Std 7-4.3.2 does not provide guidance regarding security measures for computer-based system equipment and software systems. However, RG 1.152 provides specific guidance concerning computer-based (cyber) safety system security to supplement the lack of guidance in IEEE Std. 7-4.3.2. The functional and design requirements of the safety-related systems conform to IEEE Std. 7-4.3.2 and these requirements comprise the hardware and software designs.

Appendix B of the Branch Technical Position HICB-14 (BTP 7-14) [2.3(2)] outlines the activities to consider when constructing a design development and quality assurance program for the computer-based I&C product, herein referred to as a software product. BTP 7-14 documents these activities as eleven (11) software development groups. The overall guidance from BTP 7-14 is that the software planning documents should encompass all of the topics. The software development groups are documented in the SMPM and SQAPM. According to BTP 7-14, a

separate document does not need to be developed for each of the software development topics, provided that the required information is included in one of the SW plans.

The ESBWR SW plans address the software quality assurance requirements specified in selected RGs and industry standard guidance documents. If there is any deviation in the detailed requirements as described in the guidance documents, the process outlined in the plans is followed.

APPENDIX A: HUMAN FACTORS ENGINEERING ISSUE TRACKING SYSTEM

[[

||

[[

]]

Figure A-1. HFE Issue Evaluation Process

APPENDIX B: GUIDELINES FOR CONTROL SYSTEM DATA GATHERING, TRANSMISSION, AND PROCESSING

1B. DATA GATHERING

1B.1 The ESBWR Plant Multiplexing System Distributed Control and Information System (Q-DCIS and N-DCIS):

- (1) Minimizes the plant wiring.
- (2) Considers the vulnerability of the MMIS to a single component failure, which can affect more than one system or function. Single component failures and common mode failures are analyzed in accordance with the Plans identified in Subsection 2.1.2.
- (3) Supports the plant maintenance and test requirements.
- (4) Minimizes the disruption to the plant database when a component, equipment, subsystem, or system failure occurs. The methodology for handling of the plant databases is established through the SMPM.

1B.2 The ESBWR Plant DCIS Attributes are Defined which Allows 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 meets the most restrictive requirement among the systems or functions that use the signal.
- (2) Identify cases where the signal characteristics required for special applications (for example, 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 are provided if the high performance requirements result in the selection of a device with lower reliability, higher drift, higher sensitivity to its environments, so forth.
- (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 is contained in the Software Management Plan.

1B.3 Design Flexibility

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

- (1) A modular design (both functionally and physically) to accommodate replacements, upgrades, and functional expansions easily and in a cost-effective manner.
- (2) Spare capacity in instrument panels, I/O capacity, storage capacity, processing capacity, alarm and display systems, data communication (throughput loading), power supply, HVAC, so forth.

2B. DATA TRANSMISSION

2B.1 General

- (1) All data on the plant-wide data buses 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 is attached to the signal. All data have a signal quality tag associated with it. The quality tag contains sufficient information to support troubleshooting.
- (2) The data transmission process provides sufficient inherent integrity and error checking to assure that random errors in the process do not degrade the availability and reliability of the systems and functions that utilize the data.
- (3) The DCIS documentation describes the use of standard protocols and interfaces, methods of signal tagging, the data transmission process and process for data time tagging.

2B.2 Signal Filtering

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

2B.3 Signal Processing

- (1) All signal processing such as scaling, linearization, rate of change calculation, so forth, assure that.
 - 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.
 - Coefficients or other constants used in signal processing retain their values through power interruptions and processor down time.
 - Signal rate of change is determined in a manner, which is not unduly influenced by random noise.
- (2) The DCIS requirements document describes the methods for signal processing to meet the above requirements.

2B.4 Data Propagation Times

The propagation time for multiplexed data is analyzed to demonstrate the prevention of significant degradation in performance of plant control and monitoring systems. The propagation time includes 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 provides operator acknowledgment of a requested action within 0.25 seconds of the operator request. Propagation times are modeled as a part of the DCIS safety analysis plan.

2B.5 Performance Margins

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

2B.6 Reliability Models

When redundant data paths and signal selection are used, the reliability model of the data path includes 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 are prepared in accordance with the DCIS safety analysis plan.

2B.7 Use of Industry Standards

Plant-wide data highway protocols and interfaces to controllers, sensors, actuators, so forth, are 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 is a standard interface. Nuclear industry standards for network security are incorporated.

APPENDIX C: GUIDELINES FOR DESIGN OF HSI

1C. CONTROL AND DISPLAY INTERFACES

1C.1 General

- (1) 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 are related to differences in use of the information by the operators.
- (2) Position or status indications provided to the operator are the actual component status or position where possible. The information, controls or and alarms displayed to the user are based upon the HFE program studies. The information and controls will use plant and system state to present the correct state of a component. Using color and shape coding the displays provide the operator with the correct valve line-up and component states. A demand indication is used only if it provides the operator with needed information.
- (3) The design of the ESBWR electronic user interface displays is specified and described in the N-DCIS Hardware/Software Specification. The user interface displays is consistent with the requirements of NUREG-0700 [2.3(6)]. The details of the displays are defined in the Style Guide established in the HSI Design activity.

1C.2 Testability

- (1) The MMIS implementation process defines the test requirements in formal test plans. These tests are written for various test stages that exist in the MMIS design and implementation process. These plans, 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 MMIS design, prepare the systems for operation, and surveillance tests required after the systems are in service are included in the plans. Each test plan is developed under the SQAPM and Software V&V Plan. These:
 - a. Identify the items to be tested, including their version or revision where appropriate.
 - b. Identify all features of the system under test that are not to be tested, and the reasons why.
 - c. Describe the overall test approach.
 - d. Specify relevant test case specifications.
 - e. Specify the acceptance criteria for pass/fail decision for each test and requirements for dispositioning and retesting failed steps.
 - f. Specify the test environment and test equipment.
 - g. Identify group responsibilities for performing the test.
 - h. Identify the test staffing needs and associated skill levels.
 - i. Specify a test sequence and provide an estimate of the time to carry out the tests.

MMIS equipment are 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.

1C.3 Maintainability

- (1) Although the MMIS design must facilitate cost-effective testing and maintenance, the M-MIS design also takes 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 utilizes the M-MIS functions as maintenance aids to optimize the operating and maintenance costs of the other power plant systems.
- (2) The MMIS is 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 normally is accomplished by modular replacement in the field and must be considered in the design of the components.
- (3) The MMIS is designed for maintenance in accordance with good human factors engineering principles. EPRI NP-4350, Human Engineering Design Guidelines for Maintainability [2.5(2)], is utilized to assist in placing proper emphasis on human factors. The MMIS maintenance considers 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.
- (4) Labeling and coding of components inside and outside of cabinets is unambiguous, readable and consistent with other plant labeling practices established in the Style Guide developed in the HSI Design activity.
- (5) The HFE Program ensures that the maintainability requirements, including the preparation of instruction and maintenance manuals prepared by GEH and its suppliers are met. The maintainability group with the assistance of the HFE group performs 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 [2.2(2)] and IEEE Std. 1042 [2.2(4)], is established for MMIS software. This software maintenance plan will be a revision of the currently utilized software management plan for GEH plant monitoring and control products, revised to reflect all requirements of the ESBWR DCD and program specific plans.

1C.4 Constructability

The MMIS design incorporates features that reduce the time and effort to fabricate and install the MMIS equipment. The components of the MMIS design are designed to allow installation and functional checkout of each module separately, prior to complete system integration. Cabinets and panels are fabricated, internally wired, and functionally tested before plant installation. The MMIS design contributes significantly to reducing field wiring.

2C. ALARMS

2C.1 General

- (1) The ESBWR alarm system design is documented as a Subsection to the N-DCIS Hardware/Software specification. The ESBWR alarm system is designed to:
 - a. Alert operators to off-normal conditions which require them to take action.
 - b. Guide the operators, to the extent possible; to the appropriate response.

- c. Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions.
 - d. Minimize distraction and unnecessary workload placed on the operators by the alarm systems.
- (2) The alarm system provides 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 are checked through periodic functional testing by the operators.
 - (3) The effectiveness of the alarm system is verified through real-time, dynamic simulation. Simulator evaluations 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.

2C.2 Selection of Alarm Conditions

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

- (1) For each alarm there is a defined action the operator is to take in response.
- (2) The alarm conditions are 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 is chosen such that the operator is 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 provide alerts before a major system or component problem results in a condition that causes a loss of availability.
- (5) Alarms for process deviations are based, where possible, on validated process signals rather than individual sensor indications.
 - a. The alarm system is designed to minimize the potential for nuisance alarms. To support elimination of potential nuisance alarms, the alarm system incorporates: Capability to apply time filtering and/or time delay to the alarm inputs to allow filtering of noise or eliminate unneeded momentary alarms.
 - b. 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.

2C.3 Nuisance Alarming

- (1) Each individual alarm is evaluated to examine its potential for nuisance alarming. The evaluation considers:
 - a. All modes of operation of the plant and the associated system.

- b. Maintenance of the associated system or component (for example, the potential for many alarms to come in due to a component being shutdown for extensive maintenance).
 - c. Possible momentary alarm occurrences due to equipment startup.
 - d. 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.
 - e. Potential sources of noise in the alarm input.
 - f. Unusual, but plausible, lineups for the associated system or component.
 - g. Other conditions that might lead to the unnecessary occurrences of the alarm.
- (2) Alarms that are formed from the combination of more than one input condition through "OR" logic have reflash capability. The need to implement reflash capability for multiple-input alarms is evaluated on a case-by-case basis.
 - (3) The alarm system is 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 are reduced by use of filtering, conditioning logic, and prioritization logic.
 - (4) The alarm system includes features or capabilities that are appropriate for dealing with alarms that are out of service, including spatially dedicated alarms on the wide display panel.
 - (5) Presentation of alarms is based upon the guidelines established in the HSI Design Implementation Plan [2.1.2(7)]. Alarms are presented in a prioritized manner on the main control room VDU's. Priorities are based upon relative importance and time urgency within which the operator responds. Priorities are plant mode dependent; a particular alarm can change priority as the plant mode changes.
 - (6) For each alarm condition, an alarm response procedure is prepared, defining the required operator action and giving other information needed to ensure an adequate response. These alarm response procedures are made available via hard copies and electronically (on the VDUs).
 - (7) The alarm list on the VDU is designed with the intention to display all of the plant highest priority alarms, in all credible scenarios, without display paging.
 - (8) The alarm system is capable of driving multiple audible tones or signals to annunciate alarm conditions. The types and volumes of audible tones are chosen such that:
 - a. The operator is alerted to the presence of the alarm condition.
 - b. The operator can, from the specific tone or direction of sound, determine where the alarm originated (functional area of the plant, or station).
 - c. The amount of distraction due to audible alarm signals is minimized through choice of alarms and provision for silencing audible alarms.

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

APPENDIX D: GUIDELINES FOR THE CONDUCT OF WALK-THROUGHS

II

MFN 08-255

Enclosure 3

Affidavit

GE-Hitachi Nuclear Energy LLC

AFFIDAVIT

I, **David H. Hinds**, state as follows:

- (1) I am the General Manager, New Units Engineering, GE-Hitachi Nuclear Energy, LLC (GEH) have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.
- (2) The information sought to be withheld is contained in Enclosure 1 of GEH letter MFN 08-255, Mr. Richard E. Kingston to U.S. Nuclear Regulatory Commission, entitled *Submittal of ESBWR Licensing Topical Report – ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan*, Revision 4 (NEDE-33217P) – GEH Proprietary Information, dated July 10, 2008 is delineated by a [[dashed underline inside double square brackets.⁽³⁾]]. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation ⁽³⁾ refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.
- (3) In making this application for withholding of proprietary information, of which it is the owner, GEH relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.390(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualifies under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).
- (4) Some examples of categories of information which fit into the definition of proprietary information are:
 - a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by GEH competitors without license from GEH constitutes a competitive economic advantage over other companies;
 - b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;
 - c. Information which reveals aspects of past, present, or future GEH customer-funded development plans and programs, resulting in potential products to GEH;
 - d. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a., and (4)b., above.

- (5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GEH, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GEH, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements, which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.
- (6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge. Access to such documents within GEH is limited on a "need to know" basis.
- (7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GEH are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.
- (8) The information identified in paragraph (2), above, is classified as proprietary because it identifies details of GEH ESBWR methods, techniques, information, procedures, and assumptions related to the application of the software plans to the GEH ESBWR.

The development of the evaluation process along with the interpretation and application of the regulatory guidance is derived from the extensive experience database that constitutes a major GEH asset.

- (9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GEH's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GEH's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GEH.

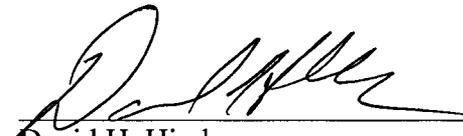
The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GEH's competitive advantage will be lost if its competitors are able to use the results of the GEH experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GEH would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GEH of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 10th day of July 2008.



David H. Hinds
GE Hitachi Nuclear Energy