Enclosure 4

MFN 07-384

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

NEDO 33217, Revision 3

Non-Proprietary Version

GE Energy
Nuclear
3901 Castle Hayne Rd
Wilmington, NC 28401

NEDO-33217
Revision 3
Class I
July 2007

LICENSING TOPICAL REPORT

ESBWR MAN-MACHINE INTERFACE SYSTEM AND HUMAN FACTORS ENGINEERING IMPLEMENTATION PLAN

PROPRIETARY INFORMATION NOTICE

This is a non-proprietary version of NEDO-33217, Rev 2, 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 **for the purpose of supporting the NRC review of the certification of the ESBWR**. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and any participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to **any unauthorized use**, General Electric Company makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained inthis document.

[[

]]

1.0 OVERVIEW

1.1 Purpose

The purpose of this plan is to describe:

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

This plan also describes how the MMIS and HFE plans and the supporting implementation plans:

- Integrate the HFE design process into the ESBWR development, design, and evaluation.
- Complies with regulatory requirements and guidelines.
- Complies with the requirements of chapter 18 of the ESBWR Design Control Document (DCD).
- Complies with the requirements of chapter 7, Appendix B of the ESBWR DCD.
- Reflect "state-of-the-art" human factors principles.
- Utilize the design information available from the ABWR reference plant and US standard plant design.

1.2 Scope

The scope of the MMIS design process consists of (1) the HFE process including the design of the hardware interfaces and (2) 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 on the design include the following:
   a. Predecessor ABWR Designs – The use of proven MMIS design from predecessor ABWR plants is addressed in DCD chapter 18.3.2.1, [2.1(2)].
   b. Standard Design Features – The ESBWR control room HSI design contains a group of standard features described in DCD chapter 18.1.4 [2.1(2)].
   c. Safety Requirements – Design inputs from regulations and regulatory guidance are discussed in DCD chapter 18.1 [2.1(2)].
   d. Staffing Plan – The initial staffing plan is addressed in DCD chapter 18.6 [2.1(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 High Level Task Analysis.

3. Applicable HSIs - The applicable HSIs, procedures, and training included in the HFE program include operations, accident management, maintenance, test, inspection and surveillance interfaces (including procedures) for those systems that have safety significance. This includes monitoring the designs being presented by ESBWR suppliers, to ensure that 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(5)], "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. Section 3.3.1 provides further definition to 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, and engineering support personnel to the extent that they perform tasks that are directly related to plant safety.

1.3 Definitions and Acronyms

1.3.1 Definitions

The GE Nuclear Topical Plans listed in Section 2.3.1 establish a list of plan specific definitions. The following terms are defined for use with this plan.

Design Record File - A formal controlled information record under GEEN procedures for in-progress and completed engineering work which is retained and from which work can be retrieved.

Design Reviews - Formal, design adequacy evaluations that are performed by knowledgeable persons to verify that product designs meet functional, contractual, safety, regulatory, industry codes and standards, and company 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 solved through the normal HFE process. Additionally, the database is used to document the problem resolution.

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

Integrated System Validation - Integrated system validation is an HFE evaluation using performance-based tests to determine whether an integrated system design (that is, 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 MCR. This includes multifunction panels, as well as single-function LCSs such as controls (for example, valves, switches, and breakers) and displays (for example, 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 from interviews with plant staff.

Man-machine Interface System (MMIS) – The Man-Machine Interface System is comprised of the systems that perform the monitoring, control, and protection functions of the plant. This includes the HSIs and the software that supports 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 that contains tailored guiding principles describing the implementation of HFE guidance to a specific design, such as for a plant control room. Adherence is expected and deviations justified.

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

Verification - The process by which the design is evaluated 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, and the participants ask questions and make comments about possible errors, violation of development standards and guidelines, and other problems.

1.3.2 Acronyms

The GE Nuclear Topical Plans listed in Section 2.3.1 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 requests
CCDP	Conditional core damage probability
CDF	Core damage frequency
CI	Configuration items
CMS	Configuration management system
COL	Combined operating license
COLOG	Combined operating license owners group
COTS	Commercial off the shelf software
CRDT	Control room design team
CRT	Cathode ray tube
CTS	Commitment tracking system
D/A	Digital/analog
DCD	Design control document
DCIS	Distributed control and information system
D-D&D	Defense-in-depth and diversity
DLD	Ddetailed logic diagrams
DoD	Department of Defense
DRF	Design record file
EAL	Emergency action level
ECN	Engineering change notice

EOP	Emergency operating procedure
EPG	Emergency procedure guideline
EPRI	Electric Power Research Institute
ERO	Emergency response organization
ESBWR	Economic Simplified Boiling Water Reactor
ESE	Electrical system engineer
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
GEEN	General Electric Energy Nuclear
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
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 panels
[[	]]
MMIS	Man-machine interface system
NIMs	Network interface modules
NMS	Neutron monitoring system
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control
O&M	Operation and maintenance
OFE	Operational failure events
PAS	Plant automation system
P&ID	Piping and instrument diagram
PDM	Project design manual
PDMS	Product data management system
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	Reg Guide (Regulatory Guideline)
RMUs	Remote multiplexing units
RO	Reactor operator
RSE	Responsible system engineer
RSS	Remote shutdown system
RTPE	Responsible technical project engineer

RV	Responsible verifier
S&Q	Staffing and qualification
SAE	Simulation assisted engineering
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 function gap analysis
SFRA	System functional requirements analysis
SIP	Software installation plan
SLD	Simplified logic diagrams
SLUs	System logic units
SME	Subject matter expert
SMP	Software management plan
SOMP	Software operation and maintenance plan
SOP	System operating procedures
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
SRO	Senior reactor operator
SRS	Software requirements specification
SSA	Software safety analysis
SST	Software safety team
STrngP	Software training plan
SVT	Software validation test

SVVP	Software V&V plan
SW	Software
SyAT	System acceptance testing
SyRS	System requirement specification
TA	Task analysis
TNA	Training needs assessment
TSL	Training services lead
TSG	Technical support guideline
V&V	Verification and validation
VDU	Visual display unit
WDP	Wide display panel

2.0 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

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.
2. ESBWR Design Control Document Chapter 18 (26A6642BX).
3. ESBWR Composite Design Specification (A11-5299), 26A6007, Rev. 0.
4. ESBWR Design Control Document Chapter 17 (26A6642BP), Rev. 3.
5. ESBWR Design Control Document Chapter 15 (26A6642BX).
6. ESBWR Design Control Document Chapter 7 (26A6642BX).
7. Design Specification Standard Review Plans and Reg. Guides (A11-5299) 26A6007AB, Rev. 3.
8. ESBWR Composite Design Specification Industry Codes and Standards (A11-5299), 26A6007AC, Rev. 2.

2.2 Codes and Standards

The following codes and standards are applicable to the activities specified within this plan.

2.2.1 NUREG

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. NUREG-0800, Standard Review Plan, Section 13.2.1, Reactor Operator Training, November 2005.
4. NUREG-0800, Standard Review Plan, Section 13.2.2, Training for non-licensed Plant Staff, November 2005.
5. NUREG-0800, Standard Review Plan, Section 13.5.1, Rev. 0, Administrative Procedures, July1981.
6. NUREG-0800, Standard Review Plan, Section 13.5.2.1, Rev. 1, Operating and Emergency Operating Procedures, November 2005.

* Specific exceptions for the software development plans 2.3.1(13) and 2.3.1(14) are provided in Appendix E.

2.2.2 Code of Federal Regulations

1. 10 CFR 50, Appendix – B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants".
2. 10 CFR 50.120, "Training and Qualification of Nuclear Power Plant Personnel".
3. 10 CFR 52.78, "Training and Qualification of Nuclear Power Plant Personnel".
4. 10 CFR Part 55, "Operators' Licenses".

2.2.3 U.S Nuclear Regulatory Commission (NRC) Regulatory Guides (RG)

1. RG 1.149, Rev 3, Nuclear Power Plant Simulation Facilities for Use in Operator Training and License Examinations, Oct. 2001.
2. RG 1.152, Rev 2, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Jan. 2006. *
3. RG 1.168, Rev. 1, Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Feb. 2004. *
4. RG 1.169, Rev. 0, Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Sept. 1997. *
5. RG 1.170, Rev. 0, Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Sept. 1997. *
6. RG 1.171, Rev. 0, Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Sept. 1997. *
7. RG 1.172, Rev. 0, Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants, Sept. 1997. *
8. RG 1.173, Rev. 0, Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants, Sept. 1997. *
9. RG 1.174, Rev. 1, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Nov. 2002.
10. RG 1.206, Section C.I.18 Human Factors Engineering, June 2006. (Issued for Preliminary Use)

2.2.4 Institute of Electrical and Electronic Engineers (IEEE) Standards

1. IEEE Standard 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. *
2. IEEE Standard 828-1990, IEEE Standard for Software Configuration Management Plans. *
3. IEEE Standard 829-1983, IEEE Standard for Software Test Documentation. *
4. IEEE Standard 830-1993, IEEE Recommended Practice for Software Requirements Specifications. *

* Specific exceptions for the software development plans 2.3.1(13) and 2.3.1(14) are provided in Appendix E.

5. IEEE Standard 1008-1987, IEEE Standard for Software Unit Testing. *
6. IEEE Standard 1012-1998, IEEE Standard for Software Verification and Validation Plans. *
7. IEEE Standard 1028-1997, IEEE Standard for Software Reviews and Audits. *
8. IEEE Standard 1042-1987, IEEE Guide to Software Configuration Management. *
9. IEEE Standard 1074-1995, IEEE Standard for Developing Software Life cycle Processes. *

2.3 Supplemental Documents

The following supplemental documents are used in conjunction with this plan. These are the enabling documents that enable the performance of the activities stated in this plan.

2.3.1 GE Nuclear Topical Reports – Implementation Plans

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

2.3.2 Other GE Topical Reports

1. NEDO-33251, ESBWR Defense-in-Depth and Diversity Plan
2. NEDO-33295, ESBWR – Cyber Security Program Plan (Draft)
3. GE Advanced Boiling Water Reactor (ABWR) First-of-a-Kind Engineering Program, Operational Experience/Lessons Learned Evaluation; 24156-1A1Q-6110-0001, Rev 1, September 1996.

* Specific exceptions for the software development plans 2.3.1(13) and 2.3.1(14) are provided in Appendix E.

2.4 Industry and Other Guidance Documents

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

1. ANSI/ANS 3.5-2005: Nuclear Power Plant Simulators for Use in Operator Training, American Nuclear Society.
2. ANSI/ISA-S 18.1: Publication Annunciator Sequences and Specifications, 1985.
3. ASME-RA-S-2002, Standard for Probabilistic Risk Assessment For Nuclear Power Plant Applications, 2002.
4. ABWR Owners Group Accident Management Guidelines Overview Document, Rev. 1, Nov 1997.
5. EPRI NP-4350, Human Engineering Design Guidelines for Maintainability, 1985.
6. EPRI TR-106439, Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Application, 1998.
7. IAEA, INSAG-7 The Chernobyl Accident: Updating of INSAG-1, 1992
8. IEEE Standard 603-1998 – IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. *
9. IEEE Standard 730-2002, IEEE Standard for Software Quality Assurance Plans. *
10. IEEE Standard 1016-1998, IEEE Recommended Practice for Software Design Descriptions *
11. IEEE Standard 1058.1-1987, IEEE Standard for Software Project Management Plan. *
12. IEEE Standard 1219-1998, IEEE Standard for Software Maintenance. *
13. IEEE Standard 1228-1994 – IEEE Standard for Software Safety Plans. *
14. IEEE Standard 12207-1996 – IEEE/EIA Standard for Software Life Cycle Processes. *
15. ISO 9001:2000, Quality Management Systems – Requirements.
16. NEI 91-04, Rev 1, Severe Accident Issue Closure Guidelines, Nuclear Energy Institute, Report NEI 91-04, 1994.
17. BWROG Emergency Procedure and Severe Accident Guidelines, Rev 2, March 2001

2.5 Regulatory Guidelines

1. NUREG-0711, Rev. 2, Human Factors Engineering Program Review Model, February 2004.
2. NUREG-0700, Rev. 2, Human-System Interface Design Review Guidelines, May 2002.
3. NUREG-0737, Clarification of TMI Action Plan, November 1980.
4. NUREG-0899, Guidelines for the Preparation of Emergency Operating Procedures, 1982.
5. NUREG/CR-3331, A Methodology for Allocating Nuclear Power Plant Control Functions to Human and Automated Control, 1983.

* Specific exceptions for the software development plans 2.3.1(13) and 2.3.1(14) are provided in Appendix E.

6. NUREG/CR-6421, A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications, 1996.

7. NUREG/CR-6634, Computer-Based Procedure Systems: Technical Basis and Human Factors, 2000.

8. NUREG-0800, Standard Review Plan, Section 13.5.2.2, Rev 0 Draft, Maintenance and Other Operating Procedures, June 1996.

9. NUREG-1764, Guidance for the Review of Changes to Human Actions, 2004.

10. NUREG-0933, A Prioritization of Generic Safety Issues, October 2006.

11. NUREG/CR-6400, HFE Insights for Advanced Reactors Based Upon Operating Experience, 1996.

3.0 METHODS

3.1 MMIS and HFE Management Plan

3.1.1 Background for MMIS and HFE Management Plan

Chapter 7 of the ESBWR DCD defines the systems, which perform the monitoring, control, and protection functions of the plant as the MMIS. 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, which provides alarm and display media for plant personnel to access plant processes and equipment status, and controls to operate plant equipment.
- Output processing equipment which provides the necessary interfaces between plant controls and plant equipment actuators. Output processing equipment includes electrical devices and circuitry. Examples would include signal conversion equipment providing signals to plant equipment, including:
  - Analog/Digital (A/D) and Digital/Analog (D/A) converters.
  - Local converters 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 which 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) as well as off-normal, emergency, and accident conditions. The requirements of this document are directed at the plant designers and are applicable to equipment supplied as part of the MMIS (see Section 1.2 Scope). The MMIS specifically includes:

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

- Monitoring and control stations for the plant systems, including the main control room, RSS, TSC, EOF, and LCS with a safety-related function or as defined by high level task analysis.
- 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 intraplant communication associated with plant operation and maintenance.

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

3.1.2 Goals for MMIS and HFE Management Plan

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

To support that goal, this management 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 ESBWR specific gap analysis to ABWRs, including 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 human factors engineering and I&C practices and processes.
6. Monitor the activities for MMIS design and system hardware/software design to ensure outcomes that meet the commitments of ESBWR DCD chapter 18.

3.1.3 Requirements for MMIS and HFE Management Plan

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 Energy Nuclear (GEEN) QA plans as described in the GEEN QA [2.1(1)].
2. Independent Review and Verification - In accordance with GEEN QA [2.1(1)], the MMIS design process provides for independent verification of all aspects of the MMIS design throughout the process. The independent verification process includes verification that individual stages of the process are correct and that the transfer of information from stage to stage has been properly accomplished. The independent review process also validates that

the overall MMIS accomplishes the intended functions, and verification that the individual steps in the process of design have been properly carried out.

3. Defense-In-Depth and Diversity Assurance – The MMIS and HFE design process described in this plan provides assurance that a modification to the reference ABWR to accommodate ESBWR objectives does not compromise the ESBWR defense-in-depth and diversity (D-D&D) analysis [2.3.2(1)]. The D-D&D analysis is a design input to the System Functional Requirements Analysis and is iterated as any other engineering input to the process (see Section 3.2.4.1(1)). Important aspects of defense-in-depth are identified in RG 1.174 [2.2.3(9)], and are evaluated to include:

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

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 that the various safety limits or criteria are not violated. It is also possible to add a safety margin (if desired) to the HA by demonstrating that the action can be performed within some time interval (or margin) that is less than the time identified by the analysis.

3.1.4 General Approach for MMIS and HFE Management Plan

The Software Project Engineering (SPE) group was established within the New Units Engineering organization of GE Energy Nuclear Engineering to design and manage the interfaces between the control room operational staff and the plant instrumentation and control equipment. The SPE group 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 management 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 ABWR plants. The reference ABWR plant for the ESBWR is the Lungmen project (Taiwan Power). Other ABWR plants in Japan include, 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 GE standard procedures and processes as well as project specific work plans.

A COL Owners Group (COLOG) is planned to provide a means for consistently maintaining safety performance levels established through staffing, training, procedures, and design as described in the ESBWR Design Control Document [2.1(2)]. Individual ESBWR licensees' programs may vary in content and level of detail; however, the standards established by the COLOG are followed.

3.1.4.5 Project Organization

The project organization is established to design, control, and manage the equipment/computer/ software/hardware interfaces and to ensure that independence is maintained between the design organization and the quality assurance, software safety and verification and validation (V&V) organizations. The organization is shown on Figure 3.1.4-1.

The 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 GE I&C/Electrical Design organization and the (GE and non-GE) hardware/software supplier organization. The GE I&C/Electrical Design organization comprises the I&C/Electrical Engineering Manager, the system Technical Project Engineers (TPEs), 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 and are responsible for interfacing with the system engineers, and hardware/software supplier organizations and providing status reports to management.

The RSEs are responsible for the ISC system design, including 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 that 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 GE or non-GE. A single Point of Contact (POC) is assigned by the hardware/software supplier organization to interface with the TPE.

2. Software Project Engineering

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 Analysis 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, BRT, SAE) are defined in the SQAP [2.3.1(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.
- Control & instrumentation 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.

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 Local Control Stations. This CRDT is made up of members from the HFE design team and include involvement by 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 assure that 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 that all its areas of responsibility are accomplished and to identify problems in the implementation of the HSI design. The HFE design team has the authority to determine where its inputs are required and to access work areas and design documentation. The HFE design team also has the authority to control further processing, delivery, installation, or use of HSI products until the disposition of a non-conformance, deficiency, or unsatisfactory condition has been achieved and hand-over to the licensee is accomplished.

The HFE design team is responsible for:

- The development of all HFE plans and procedures.
- The oversight and review of HFE design, development, test, and evaluation activities.
- The initiation, recommendation, and provision of solutions through designated channels for problems identified in the implementation of HFE activities.
- Verification that solutions to problems have been implemented.
- Assurance that HFE activities comply with the HFE plans and procedures.
- Ensure that the activities of the Quality Plan [2.1(1)] are followed.
- The methods for reviewing MMIS operating experience.

- Scheduling of HFE activities and milestones.

3. Training

Training is part of the Nuclear Services organization. The Training Services Lead is responsible for ensuring that 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), herein referred to as 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 is addressed in the SQAP [2.3.1(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 following activities are included:

- 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 of 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.

3.1.4.5 Management Process and Procedures

1. General Process Procedures - The process through which the team executes its responsibilities is established in ESBWR Project Policies and Procedures (P&Ps), Engineering Operating Procedures (EOPs), and Engineering Service Instructions (ESIs) that implement the GE Energy Nuclear (GEEN) QA plans described in NP-2010 COL Demonstration Project Quality Assurance Plan [(2.1(1)]. These GE 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.
2. This plan and its subordinate implementation plans are controlled documents under configuration control in accordance with GEEN QA [2.1(1)]. When improvements or deficiencies are identified, a Corrective Action Request (CAR) is issued to document the condition. The CAR tracks activities and ensures that corrective and preventive actions are implemented. It ensures that the actions are effective in either eliminating the deficiency or improving the affected plans.
3. A change or revision to this document and its subordinate plans prior to certification approval is established in accordance with the GEEN QA [2.1(1)] and applicable ESBWR project procedures. A change or revision to this document and the subordinate plans listed in Section 2.3.1 after certification approval is accomplished in accordance with Processes for Changes and Departures to Tier 2 information within the applicable appendix for the ESBWR to 10 CFR 52.
4. A project work plan is developed to further define project scope, activities and deliverables for each implementation plan described in Section 4. The project work plan is updated as changes occur in the work scope, design inputs, and outputs.
5. Specific project controls for the management of the software process are described in the Software Management Plan [2.3.1(13)] and requirements and procedures for the quality assurance of the software development process are described in the Software Quality Assurance Plan [2.3.1(14)].
6. Process Management Tools - Tools and techniques (for example, review forms) to be utilized by the team to verify application of SPE/HFE efforts are identified in the HFE and Software implementation plans described in Section 4, or in their respective work plans.
7. Integration of HFE and Other Plant Design Activities - The integration of design activities is established in the ESBWR Program Management Manual, GEEN QA [2.1(1)] and herein. Specific design inputs are described in the individual activity plans in Section 4. [[

]]

3.2 HFE Process

3.2.1 Background for HFE Process

A functional requirements analysis defines functions at plant and system levels for the safe operation of the plant. An allocation of functions determines if human, machine, or a combination of both completes actions to be accomplished in the performance of functions. 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 the following:

- 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 is, to minimize periods of operator underload and overload.
- Operator interfaces minimize operator error and provide for error detection.
- HSI design supports the capability of the operating crew to recovery 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 reference ABWR plants serve as a design basis for the ESBWR MMIS implemented under this plan. The reference ABWR plant is the Lungmen project (Taiwan Power). Other ABWR plants include, Kashiwazaki-Kariwa 6 & 7 (TEPCO), Hamaoka 5 (Chubu Electric), and Shika 2 (Hokuriku Electric Power). Lungmen has been selected as the baseline reference plant because other ABWRs (Kashiwazaki-Kariwa Nuclear Power Station, K6 & K7 in Japan) used older analog technology to support

the human system interface (HSI). Lungmen has digital control for many systems, good human factors documentation, and a design for flat screen interfaces.

2. It is recognized that different operational needs, human factors considerations, and industry standards, codes, and regulations exist between the reference plants and the ESBWR MMIS implemented under this plan. An analysis of the design differences between the ABWR and ESBWR design establishes a Baseline Review Record (BRR). Potential differences may lead to changes in 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 [2.1(2) Section 18.6] establishes a preliminary staffing assumption meeting regulatory requirements and staffing considerations addressed in the ESBWR HFE Staffing and Qualifications Plan [2.3.1(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 highly reliable and provides functional redundancy such that sufficient display and control is available in the main control room and remote locations to conduct an orderly reactor shutdown to cold conditions, even during the postulated ESBWR design basis equipment failures defined in the ESBWR PSAR. Analysis shows that mean time 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 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 reference plants and the US standard plant design. Deviations from the reference MMIS design are made to accommodate:
    a. Regulatory updates, such as NUREG 0700 Rev 2; NUREG 0711 Rev 2; and NUREG 0800 Rev 1, which were issued after ABWR design certification and design of reference 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), which may need to be reflected in design of the ESBWR MMIS.
    c. HFE analysis that is specific for ESBWR, such as allocation of function and task analysis, which may be different from ABWR reference 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 reference plants, and ESBWR DCIS vendor equipment.
9. Standardization of Components minimizes the impact of obsolescence of MMIS equipment throughout 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 such as VDUs, may impact the design of the MCR panels over the life of the plant. ESBWR Program Plans and the Software Management Plan (SMP) 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, including guidance for:
    - The ESBWR plant multiplexing system Distributed Control and Information System (Q-DCIS and N-DCIS).
    - Design Flexibility.
    - Data Transmission.
    - Signal Filtering.
    - Signal Processing.
    - Data Propagation Times.
    - Performance Margins.
    - Reliability Models.
    - Use of Industry Standards.
11. The MMIS utilizes only proven technology. Due to the advantages that currently available modern technology offers over some of the technology found at operating BWRs, the incorporation of modern technology 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 or safety-related systems, proven systems, equipment, subsystems, components, design and services are those which have been evidenced by at least one (1) year of successful operation experience in existing light water reactors. For non-Q class or nonsafety-related systems, they are considered "proven" if they have been evidenced by at least one (1) year of successful operation record in existing light water reactors, fossil plants, or industry process plants, prior to the start up date.
    b. Criteria for Unproven Technology - GE may make use of up-to-date modern technology and design, and understands that some designs, subsystems, systems, equipment or components proposed may not have received the required one (1) year satisfactory service prior to the start up date. For these designs, systems, and subsystems, equipment or components, if proposed, GE may develop a methodology to receive equivalent experience. Such an approach is evaluated and considered acceptable if:
        – 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; and

- Specific proven designs, systems, subsystems, equipment or components, which have been evidenced by at least one (1) year of successful operation experience and which can meet the basic functional requirements are considered; and
- The needed experience data collection can be completed and assessed prior to the issuance of a Operating License and the determination can be made prior to the issuance of the Operating License as to whether the base approach (up-to-date modern technology and design) is acceptable or the back up approach must be utilized, without either of these two approaches impacting the overall project schedule.

12. General guidelines for the design of HSI are provided in Appendix C and include guidance for:
    - Electronic Displays
    - Testability
    - Maintainability
    - Constructability
    - Alarms

[[

]]

[[

]]

3.2.4.5 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 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 descriptions of the respective activities in Section 4.1 and are summarized in the results summary reports.

3.2.4.5 Emergency Management Program

Following TMI, Emergency Management was identified as an unresolved issue. An industry initiative committed utilities to access current capabilities to respond to emergency conditions and implement appropriate improvements. Two industry primary documents address the preparation for managing nuclear plant resources to respond to emergencies and to prevent or mitigate severe accident. BWROG Emergency Procedure and Severe Accident Guidelines (EPG/SAG, Rev 2) provide a generic framework around which site specific Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMGs) are written. NEI 91-04 Rev. 1 [2.4(16)] describes the closure process to develop plant specific SAM guidelines (SAMGs), to interface SAM guidelines with the emergency plan, to incorporate SAM into training, and to evaluate new SAM information.

The typical elements of an emergency management strategy are:

- Emergency Operating Procedures (EOPs) that respond to emergencies and events that may degrade into emergencies up until primary containment flooding is required.
- Severe Accident Guidelines (SAGs) that define strategies applicable after primary containment flooding is required based on the BWROG EPG/SAG Rev. 2.

This section describes GE and COL applicant roles and responsibilities for development of the emergency management program.

1. GE performs the following in support of the emergency management program development:

- Provides to the COL applicant, the technical basis for an emergency management program, including emergency procedure guidelines (EPGs), to ensure core damage prevention and mitigation, including meeting off-site dose limits.
- Translates the plant design bases into operation limitations and responses, which can be developed into procedural guidelines and training by the COL applicant.
- Confirms that the plant design is compatible with the EPGs and emergency management program using the ESBWR PRA and other relevant information.
- Identifies systems and equipment, which may be useful as part of the emergency management program. These include safety and non-safety, onsite as well as offsite equipment.

2. The COL applicant is responsible for the following to establish the emergency management program:

- Develop procedures that will identify those actions to be taken to prevent and mitigate the effects of accidents, including:
  - 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, including:
  - Section 5.2, which contain 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
  - Section 5.3.3, Computational Aids for Technical Support.
  - Section 5.3.4, Information Needed to Respond to a Spectrum of Severe Accidents.
  - Section 5.3.5, Delineation of Decision-Making Responsibilities.
  - Section 5.3.6, Utility Self Evaluation

- Incorporate the BWROG Accident Management Guidelines Overview Document, Rev. 1, Section 6. This includes four interrelated assessments:
  - The Control Parameter Assessment, which obtains and processes plant data.
  - The Plant Status Assessment, which evaluates current plant conditions.
  - The System Status Assessment, which evaluates the availability of systems needed to implement EOPs and SAGs.
  - The EPG/SAG Action Assessment, which prioritizes system restoration actions and determines the appropriate timing of procedural actions.
- Prepare the 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 code. This information relates to severe accident phenomena in the 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). This 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 use of alternate injection sources such as AC-Independent Fire Water Addition System to provide long term cooling.
- Prepare Functional Requirements 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 Emergency Operating Procedures (EOPs) and Severe Accident Guidelines (SAGs).
- Develop ESBWR Accident Training that addresses a broad range of accidents up to and including severe accidents. Training is provided for the Emergency Response Organization (ERO) personnel with their responsibilities defined in the emergency plan. Training to specific personnel that have severe accident assessment and mitigation responsibilities is also provided:
  - Evaluators – Responsible for accessing plant symptoms in order to determine the plant damage condition(s) of interest and potential strategies that may be utilized to mitigate an event.
  - Decision Makers – in the emergency Response Organization (ERO) designated to access and select the strategies to be implemented.

- Implementers - responsible for performing those steps necessary to accomplish the objectives of the strategies (e.g., hands-on control of valves, breakers, controllers, and special equipment).

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 provides reliability and protection against the propagation of failures. Application of signal validation to selected parameters is used to assure 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.

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; and
- 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, including the development of the graphical user interfaces to be used by the operator. The part-task simulator is used in 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 general development of key implementation plans, analyses, and evaluation of the following are identified and described in Section 4.1:

- Operating experience review
- Functional requirements analysis
- Allocation of function
- Task analysis
- Staffing and qualifications
- Human reliability analysis
- HSI design
- Procedure design
- Training design
- Human factors verification and validation
- Design implementation
- Human performance monitoring.

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 described in chapter 7 "Instrumentation and Control Systems" of the ESBWR DCD [2.1(6)]. These functions are primarily represented within 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 bounded by the systems and functions described in chapter 7 of the ESBWR DCD [2.1(5)].

The software development process is governed by two planning documents:

- Software Management Plan (SMP) [2.3.1(13)]
- Software Quality Assurance Plan (SQAP) [2.3.1(14)]

Software Management Plan (SMP) 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 SMP are:

- Software Development Plan (SDP).
- Software Integration Plan (SintP).
- Software Installation Plan (SIP).
- Software Operation and Maintenance Plan (SOMP).
- Software Training Plan (STrngP).

The Software Quality Assurance Plan (SQAP) includes the software plans used by the Quality Assurance (QA) and the Software Project Engineering organizations. The SQAP includes the following planning documents:

- Software Verification & Validation Plan (SVVP).
- Software Safety Plan (SSP).
- Software Configuration Management Plan (SCMP).
- The SQAP also includes the following testing:
  - Software Testing.
  - System Acceptance Testing.
  - Factory Acceptance Testing.
  - Site Acceptance Testing.

Together, the SMP and the SQAP include all the software plans that conform to the guidance provided by NUREG 0800, Standard Review Plan [2.2.1(1)]. These plans are discussed from the perspective of software life cycle phases in Section 3.3.4 and summarized as individual plans in Section 4.2.

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 Section 3.3.4.

3.3.3 Requirements for MMIS Software Development

1. Software Classification

   The Software Class is determined as shown below and is performed during the SSA Preparation phase as described in Section 3.3.4.1. This scheme is based on IEEE Std. 1012 "IEEE Standard for Verification and Validation Plans" [2.2.4(6)].

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: a. Software whose inadvertent response to stimuli, failure to respond when required, response out-of-sequence could directly result in an accident or transient as defined in the DCD, chapter 15 [2.1(5)]. b. Software that is intended to mitigate the result of an accident. c. Software that is intended to support recovery from the result of an accident
Software Class N2	• Software failure cannot adversely affect a safety-related function· • Software failure results in inconvenience to the user

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

2. Configuration Management and Change Control

   Unless otherwise specified, the design outputs (including verification package, test and analysis reports) are configuration items (CI) and as such, are controlled as specified in the SQAP [2.3.1(14) Section 10.0]. A discrepancy or deficient condition detected in a configuration item is resolved in accordance with the Change Control process described in the SCMP [2.3.1(14) Section 10].

3. Requirements Traceability Matrix

   A requirements traceability matrix is prepared for software class Q and software class N design outputs. The traceability matrix clearly shows 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.

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 [2.3.1(14) Section 7.0].

   Independent Verification records consist of at least:

   - Scope of the review, including acceptance criteria
   - Identification of the document reviewed
   - Statement of results and conclusion of the review
   - Date of review and identification of reviewer
   - (For anomalies) Identification of the specific criteria violated
   - (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 SMP [2.3.1(13) Section 5.4]. The responsible verifiers are individual(s) or groups(s) who are competent to perform the verification based on knowledge and experience. The individual(s) are not to 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 SVVP [2.3.1 (14) Section 7.0]. 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 GEEN DRF system.

5. Testing

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

6. Software Safety Analysis

   Software Safety Analysis (SSA) is performed to ensure the safety of the Class Q software for software product. Safety is the most important consideration for the safety-related I&C, taking precedence over budget and schedule. SPE SST team, an independent organization, conducts the SSA in accordance with the SSP [2.3.1(14) Section 9.0].

7. Baseline Review

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

   - The design information developed during the software life cycle phase adheres to the requirements.
   - The V&V and SSA adhere to the procedures outlined in the SVVP [2.3.1(14) Section 7] and SSP [2.3.1(14) Section 9].

8. Software Developed by Vendors

   Software products developed by the vendors shall comply with the quality requirements of the SQAP [2.3.1(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 assure compliance with the requirements specified in the SQAP [2.3.1(14) Section 14].

3.3.4 General Approach for MMIS Software Development

The SMP and SQAP and their associated plans represent a well-defined 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 based on RG 1.152 [2.2.3(2)], RG 1.173 [2.2.3(8)] and IEEE 1074 [2.2.4(9)] are defined below:

1. Planning Phase – This is the definition of the project scope, methodologies, and resources needed 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 – 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) integrated systems test which is 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 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, 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, effect on existing software products that are to remain operational in the operating environment, disposition of the retired software product including security disposition. This 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.

3.3.4.5 Planning Phase

The purpose of the Planning Phase is to:

- Develop, review, and approve SMP, SQAP, and Cyber Security Plans.
- Review and ensure that the team is trained and familiar with the software plans (SMP, SQAP).
- Define the scope of the software product, and identify and evaluate the overall objectives, design requirements and required functionality.
- Identify the safety and license requirements of the software product based on the safety significance of the function and the results of the Software Safety Analysis.
- Develop a strategy to identify and evaluate the key resources (standards, methodology(s), documents, and tools) and project risks to accomplish the software product objectives.
- Define the integrated project schedule (identifying the tasks to be performed for all software product, on an individual system basis) and establish short, timely milestones for each system.

Input documents for this initial phase are:

- Customer Contract.
- MMIS and HFE Implementation Plan.
- Design Control Documents, chapters 7B and18.
- Functional Requirements Analysis (HFE Activity).
- Allocation of Functions (HFE Activity).
- Task Analysis (HFE Activity).

[[

]]

[[

		]]	

3.3.4.5 Design Phase

The purpose of the Design Phase is to:

- Configure the software requirements into well-structured components.
- Identify the software modules that must be developed (through either the writing of new software modules, or the modifications of the previously developed software modules).
- Define the software coding conventions and guidelines.
- Develop test procedure and test cases required to test all software functions.

The input documents to this phase are the outputs from the Requirements Phase (Table 3.3.4-2). The key activities performed in this phase are:

- Prepare software design description.
- Prepare internal data communication protocol specifications.
- Prepare validation test plan, procedures, and test case specifications.

- Prepare the Software Conventions and Guidelines Document.
- Conduct software safety analysis and prepare SSA report for the Design Phase.
- Perform Design Phase baseline review record.

[[

3.3.4.5 Implementation Phase

The purpose of the implementation phase is to:

- Transform the software design into software source code using the defined Software Conventions and Guidelines document.
- Perform a review of the completed software modules for coding style conformance.
- Perform software functional testing of the module/unit to identify and resolve errors.
- Confirm that the module/unit correctly implements the software design specification and that the performance is stable, correct and repeatable.

The input documents to this phase are the outputs from the Design Phase (Table 3.3.4-3). The key activities performed in this phase are:

- Review software coding readiness.

- Identify software coding.
- Conduct safety analysis of software coding.
- Review code for each software module.
- Perform software functional testing.
- Prepare software functional test report.
- Prepare the software build description.
- Prepare the implementation baseline review record.

[[

		]]	

3.3.4.5 Test Phase

The purpose of the test phase is to demonstrate that the software is operational and conforms to the functional and performance requirements specified in the HSS and SRS and do not perform unintended functions.

The input documents to this phase are the outputs from the Implementation Phase (Table 3.3.4-4). The key activities performed in this phase are:

- Conduct software validation testing.
- Review and update the build description.
- Release firmware/software for production.
- Prepare the Test Phase Baseline Review Record

[[

		]]	

3.3.4.5 Installation Phase

The purpose of the Installation Phase is to:

- Install the production software on the production (target) hardware [[ ]]
- [[ ]]
- Install the Multi-System Factory Acceptance Tested software products at the target environment and perform installation checkout.
- Perform Site Acceptance Test (SAT).

The input documents to this phase are presented in Table 3.3.4-6. The key activities performed in this phase are:

- [[ ]]
- Conduct multi-system factory acceptance testing.
- Conduct site acceptance testing.
- Prepare installation baseline review record.
- Prepare software operations and maintenance manuals.
- Prepare software training manuals.

[[

]]

[[			
		]]	

[[			
		]]	

[[			
		]]	

3.3.4.5 Operations and Maintenance Phase

The objective of the Operations and Maintenance Phase is to provide a controlled process for implementing software modifications during the software life cycle process after control of the software and hardware has transferred to the licensee.

Input documents for this phase are:

- HFEITS Report.
- Corrective Action Reports (CAR) – Internal or External.

The key activities performed in this phase are:

- Review and update the validation test baseline.
- Implement the software engineering change control process.

[[

		]]	

3.3.4.5 Retirement Phase

The purpose of the Retirement Phase is to use the software engineering change control process to control, authorize and implement changes resulting in removal of software product and the engineering controlled documents.

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" [2.2.3(2)]. Conformance with RG 1.152 comprises the functional and design requirements of computers used in safety systems of nuclear power plants, and the security of various hardware, controls and data networks with safety-related systems, as described in [2.1(6) DCD Tier 2 Chapter 7]. The Cyber security program is described in NEDO-33295, "ESBWR – Cyber Security Program Plan" Licensing Topical Report [2.3.2(2)]. The software process plans will refer to the cyber security program plan for development, operation and maintenance of safety-related software that, as stated above, conforms to RG 1.152 and endorses IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" [2.2.4(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.

Branch Technical Position HICB-14 (BTP 7-14) [2.2.1(2), Appendix "B"] outlines the many activities to be considered 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 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 two previously described software (SW) plans and are described individually in Section 4.2. According to BTP 7-14, a separate document need not 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. In certain cases, deviation has been taken from the detailed requirements described in the guidance documents, in which case the process outlined in the plans is followed.

4.0 IMPLEMENTATION

The MMIS and HFE program described within the this plan and the subordinate implementation plans represents 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 supports the maintenance of human performance objectives in the operational phase of the plant facilities.

4.1 HFE Process

4.1.1 Operating Experience Review

4.1.1.5 Overview

As part of the HFE process described in Figure 3.2.4-1, operating experience reviews (OERs) are conducted to identify HFE-related safety and availability issues. The OER obtains and analyzes information on the past performance of predecessor designs. In the case of a new plant such as the ESBWR, the evolution of the design comes from years of BWR experience and improvements. The ESBWR builds upon the operational experience of the ABWR and the testing and design experience of the SBWR. The issues and lessons learned from previous operating experience provide a basis for improving the plant design and the Human System Interface (HSI) at the beginning of the design process.

History has demonstrated that valuable lessons can be learned from incidents and accidents. This was demonstrated after the accident at Three Mile Island nuclear power plant in the United States of America in 1979, when far-reaching follow-up actions were taken to minimize the risk of a recurrence and to improve the HSI and procedures for accident management. The accident at Chernobyl demonstrated that the lessons from the Three Mile Island accident had not been acted upon in the USSR: in particular, the importance of systematic evaluation of operating experience, the need to strengthen the on-site technical and management capability, including improved operator training, and the importance of the man-machine interface (IAEA, INSAG-7, [2.4.7]).

The analysis of operating experience events to understand the role of human actions supports the HSI design decisions that enhance safety. The OER documentation provides a basis for design decisions, a starting point for developing performance indicators, and an experience review system for the operating plant.

4.1.1.5 Purpose

The purpose of this implementation plan is to establish methods, criteria and guidance for identifying, analyzing and documenting lessons learned from published reviews of past events, PRA's and other available information sources. The lessons learned and insights gained are used to recommend potential tools and technological solutions to reduce human errors and their impact on risk and reliability of plant operation. In this way, negative features associated with predecessor designs may be avoided in the current design while retaining positive features. The plan describes a methodology for the design team and the Control Room Design Team (CRDT) to utilize experience information to support design efforts.

4.1.1.5 Scope

The OER plan establishes a process for the review of experience and identification of problems in prior HSI implementations, including human factors problems. The results of the review are addressed throughout the design process. The interaction of the OER subtasks with other HFE tasks is shown in Figures 4.1.1-1 and 4.1.1-2.

The scope of this plan includes the following:

- Process for incorporating OER information. A framework and classification system for analyzing the human factor aspects of operating experience is established. This includes identifying information for design consideration as well as developing guidance and format for the design response. Both the information for design consideration and the response are documented in the operating experience and lessons learned tracking.
- Literature review for new HSI technologies. Published research documents that address experience with the HSI in different modes of operation and transitions between modes are reviewed for applicable design considerations (for example, if touch-screen interfaces are planned, the HFE issues associated with using them are reviewed).
- Review of events summary documents. Experience summary documents are reviewed in detail and the insights that support enhancement of human actions affecting the risk and reliability of normal, abnormal, emergency, and outage operations are integrated into the OER (for example, generic safety issues defined by the NRC).
- BRR/OER reference design database. Events reported by BWR and ABWR predecessor systems and other plants with similar design features are classified and provided to the ESBWR system designers and HFE design team for review and consideration.
- Operator Interviews. Feedback from utility operators on needs of operators, maintainers, testers, and outage planners is obtained and incorporated into OER process.
- Documentation of results. Applicable review results are documented within the operating experience and lessons learned tracking.

[[

]]

[[ ]]

[[ ]]

4.1.1.5 Methods

An OER for the ABWR was performed entitled First-of-a-Kind-Engineering (FOAKE) Operational Experience / Lessons Learned Evaluation (24516-1A10-6110-0001) [2.3.2(3) . The FOAKE OER results are incorporated into the plant-level and system-level designs of one ABWR currently under construction. The ESBWR design incorporates many BWR and ABWR design features and therefore already reflects predecessor BWR and ABWR experience. The FOAKE OER is reviewed to identify predecessor BWR and ABWR operating experience incorporated in the ESBWR design, and operating experience requiring additional review.

A review of the industry experience with similar designs is conducted for selected HSI equipment technologies. The review of HSI technologies includes literature pertaining to the human factors issues for similar system applications and interviews with personnel experienced with their operation. Relevant HFE issues/concerns associated with the selected HSI equipment technologies are documented in the HFE Issue Tracking System (HFEITS).

For example, new elements of the HSI design, in which further development of the industry is expected include:

- Use of flat panel display panels and CRT/VDU displays.
- Use of CRTs in selected applications.
- Use of touch screen technology vs. other types of pointing/input devices.
- Use of electronic on-screen controls.
- Use of wide display panels.
- Use of prioritized alarm systems.
- Automation of process systems.
- Operator workstation design integration.
- Any other areas where clear industry developments have been made which may address HSI and HFE areas.

Also, recognized industry HFE issues such as those documented in NRC documents NUREG-0933 and NUREG/CR-6400 and others are addressed. The sources for these operating experience reviews include:

- Recognized industry HFE Issues.
- Reports provided by industry organizations such as EPRI.
- Review of applicable research in these design areas.
- Proceedings published by HFE professional societies.
- Review of applicable research and experience reports published by HSI equipment vendors.
- Review with actual users or industries (for example, non nuclear power generation, process industries, aerospace, DOD, so forth) of the new elements of HSI design.

Lessons learned from reviews of previous nuclear plant HSI designs are screened, analyzed for risk importance, and entered into the operating experience and lessons learned tracking to assure that problems observed in previous designs are adequately addressed in the ESBWR design implementation.

A BRR database, in conjunction with an OER database, is established for use by the ESBWR system designers to review and incorporate OER results. The BRR/OER database comprised of predecessor design and operating experience documentation is evaluated by the ESBWR design team for application to the ESBWR design. The BRR database establishes guidance for identifying significant differences between the ESBWR design and predecessor designs, as well as establishing a process for evaluating and resolving identified differences.

Personnel interviews are conducted to determine the operating experience related to predecessor plants or systems. The topics included in the interviews as a minimum include plant operations and HFE design topics. Plant operations address normal plant evolutions, instrument failures, HSI equipment and process failures, transient, accidents and reactor shutdown periods, and

cooldown using a remote shutdown system. HFE design topics include decisions about selection of alarm and annunciation elements, displays, control and automation elements, information processing and job aids, real-time communications with plant personnel and other organizations, procedures, training, staffing/qualifications, and job design.

The ESBWR HFE team uses OER information, particularly safety lessons learned, for the process of allocating functions to manual, shared, or automated resources. Figure 4.1.1-2, derived from Table 3.1 of NUREG 0711 Rev 2 [2.5(2)], shows the OER support contribution to the key HFE task elements.

4.1.1.5 Implementation

The ESBWR Operating Experience Review Implementation Plan defines the inputs, process, and outputs for the activities described in Section 4.1.1.4.

4.1.1.5 Results

OER results are documented in a results summary report. The report addresses:

- The OER team members and backgrounds.
- The scope of the OER.
- The sources of operating experience reviewed and documented results.

The report is broken down into the three areas of review:

- Review of HSI equipment/technologies.
- Review of nuclear and other industry summary documents.
- Personnel interviews.

For each issue, the report summarizes:

- A statement of the issue.
- Issue source.
- Potential human performance impact.
- Classification.
- Priority.
- Human performance improvements.

Other OER outputs are:

- Operating experience and lessons learned tracking. Resolutions to OER issues are entered into a tracking system to assure applicable lessons learned are incorporated.
- BRR/OER database. A database for easy user access to OER results is provided to system designers.

4.1.2 Function Requirements Analysis

4.1.2.5 Overview

The HFE Process depicted in Figure 3.2.4-1 establishes three specific activities that support operational analysis:

- Functional Requirements Analysis (FRA).
- Allocation of Functions (AOF).
- Task Analysis (TA).

These steps determine:

Functions required to achieve plant goals and system functions.

- Distribution of functions among human, machine, and shared control.
- The integrated actions required at the task level.

[[

]]

4.1.2.5 Purpose

The purpose of the FRA implementation plan is to prescribe and guide FRA conduct for the ESBWR plant design [Figure 4.1.2-2]. It establishes methods to:

- Conduct the FRA consistent with accepted HFE methods.
- Denote the ESBWR mission, goals, and operating states.
- Identify critical safety functions.

- Validate system functions identified in the ESBWR System Design Specifications (SDS) from an HFE perspective.
- Define the relationships between high-level functions and plant systems.
- Reconcile any differences between Plant-level analyses and the SDS.
- Provide analysis method to assess the impact of design, staffing, training procedure, and HSI changes on the ability of operators to monitor and coordinate activities.

4.1.2.5 Scope

The scope of the FRA Plan establishes the following elements for the analysis:

- Objectives, performance requirements, and constraints.
- Methods and criteria for conducting the Plant-level Functional Requirements Analysis (PFRA) in accordance with accepted human factors principles and practices.
- Methods and criteria for conducting the System Functional Requirements Analysis (SFRA) in accordance with accepted human factors principles and practices.
- System requirements that define the system functions.
- Resultant systems HSI requirements.
- Critical safety functions resulting from PRA, HRA, and deterministic evaluations.
- Descriptions for each identified function.
- Overall system configuration design.

To accomplish these objectives, plant-level and system-level goals and functions are systematically analyzed concurrently. The functional relationships between plant functions and system functions are reconciled through a system function gap analysis. The output of the gap analysis is used as a design input to ensure that plant-level and system level goals are met.

FRA results are entered into a data structure during initial design. This data structure is shared with the Probable Risk Assessment (PRA) and plant simulation efforts during the pre-operational and operational phases to evaluate the impact of design changes on the HFE aspects of ESBWR.

[[

]]

4.1.3 Allocation of Function

4.1.3.5 Overview

Three activities comprise the operational analysis of the ESBWR design process. They are:

- Functional Requirements Analysis (FRA).
- Allocation of Functions (AOF).
- Task Analysis (TA).

These steps determine:

- Functions required to achieve plant goals and system functions.
- Distribution of functions among human, machine, and shared control.
- The integrated human actions (HAs) and machine actions required at the task level.

The overall operations analysis is an iterative integration of the three activities to establish requirements for the Human-System Interface (HSI) design including plant equipment, software, personnel, training, and procedures. This plan covers the second of these steps, allocation of functions.

[[

]]

4.1.3.5 Purpose

The Allocation of Function (AOF) Implementation Plan addresses methods, processes, and criteria for verifying that the AOF portion of operational analysis is consistent with accepted ESBWR HFE practices and principles. The HFE team uses the allocation of function process to ensure that overall operational analysis successfully generates allocated tasks to accomplish all needed system functions. The output forms the requirements for HSI design, training, procedures, and staffing and qualifications. Through this process, applicable guidelines of NUREG/CR-3331 [2.5(6)], NUREG-0700 [2.5(3)], and NUREG-0711 R2 [2.5(2)] are addressed.

The AOF Plan establishes methods to:

- Conduct the AOF consistent with accepted HFE methods.
- Promote the ESBWR mission, goals, and philosophy.
- Allocate functions between human, machine and shared control.
- Coordinate human and machine tasks for shared functions during normal, abnormal, and emergency operation.

- Coordinate human and machine tasks for shared functions for surveillance functions.
- Coordinate human and machine tasks for shared functions for maintenance functions.
- Provide analysis method to assess the impact of design, staffing, training, procedure, and HSI changes on the ability of operators to monitor and coordinate activities.

4.1.3.5 Scope

Monitoring and control functions from the FRA are analyzed and allocated to human, machine, or shared ownership by the AOF process. AOF places emphasis on Human Actions (HAs) that have been found to affect plant risk by means of Human Reliability Analysis (HRA)/Probabilistic Risk Assessment (PRA). The probability of successful completion of these tasks is increased by the proper allocation of supporting functions such as machine backup, machine limits on human actions, and supporting automations.

The details of AOF scope are as follows:

1. AOF allocates functions from the following areas to the appropriate owners:
   - Normal, abnormal, and emergency operations.
   - Full range of plant operating modes, including startup, low-power, normal operations, shutdown, abnormal, transient, and emergency operating conditions.
2. The AOF plan establishes the following elements for the analysis:
   - Objectives, performance requirements, and constraints.
   - Methods and criteria for conducting the AOF in accordance with accepted human factors principles and practices.
   - System and function requirements that define function allocation restraints.
   - Results from the HRA/PRA, OER/BRR, and deterministic evaluations are included.
   - Each function identified in the FRA is allocated.
   - AOF results in sets logical, coherent, and meaningful tasks.

[[

]]

4.1.4 Task Analysis

4.1.4.5 Overview

Three specific activities support operational analysis:

- Functional Requirements Analysis (FRA).
- Allocation of Functions (AOF).
- Task Analysis (TA).

These steps determine:

- Functions required to achieve plant goals and system functions.
- Distribution of functions among human, machine, and shared control.
- The integrated human actions (HAs) and machine actions required at the task level.

The overall operations analysis is an iterative integration of the three elements of functional requirements, function allocation, and task analysis to establish requirements for the Human-System Interface (HSI) design. Plant equipment, software, personnel, and procedural requirements are systematically defined. As a result, functional objectives are met.

Task analysis scrutinizes tasks that support functional requirements for plant operation to support:

- Start-up, power operation, shutdown, and refueling activities.

- Normal, abnormal, and emergency operation.
- Performance of maintenance, calibration, and surveillances.

Subsequent HFE tasks refine this initial assignment by strategically employing human and machine capabilities. Factors considered during TA include:

- Existing baseline review record (BRR) operating experience review (OER).
- Regulatory guidance (e.g., Reg. Guides/NUREG/DCD).
- ESBWR mission and supporting goals.
- Reliability of the human, machine, and shared control schemes (e.g., Defense-in-Depth and Diversity).
- Operator workload and situational awareness (e.g., HRA/PRA).
- Capital cost, operating costs, and technical feasibility.

4.1.4.5 Purpose

The TA plan establishes methods to:

- Conduct the TA consistent with accepted HFE methods.
- Promote the ESBWR mission, goals, and philosophy.
- Identify prerequisites to performing a task or task sequence.
- Identify the parameters required to coordinate tasks and task sequences.
- Identify the termination criteria to abort a task or task sequence.
- Identify the parameters that confirm successful completion of tasks or task sequences.
- Sequence tasks to support normal operation.
- Sequence tasks to support abnormal operation.
- Sequence tasks to support surveillance functions.
- Sequence tasks to support maintenance functions.
- Provide analysis methods to assess the impact of design, staffing, training, procedure, and HSI changes on the sequence and coordination of tasks.

Task analysis identifies the need for information, controls, and alarms; supports operations during periods of maintenance and tests of plant systems and equipment, including HSI equipment; and evaluates tasks that are risk-important as determined by the HRA/PRA.

4.1.4.5 Scope

The TA plan establishes the following scope elements for the analysis:

- Objectives, performance requirements, and constraints.
- Methods and criteria for conducting the TA in accordance with accepted human factors principles and practices.

- System and function requirements that define task sequencing and coordination restraints.
- Resultant systems HSI requirements.
- TA's responsiveness to HRA/PRA, and deterministic evaluations.
- Task sequencing for each identified function.
- Overall system configuration design.

To accomplish these objectives, component-level, system-level, and plant-level functions are systematically analyzed. The relationships and interaction between human and machine tasks are examined through several iterations of analysis. TA considers all functions identified by the FRA and allocated to the plant operator (human and shared).

Task analysis applies to the full range of plant operating modes including:

- Startup.
- Normal operations.
- Abnormal and emergency operations.
- Transient conditions.
- Low power operation.
- Shutdown conditions.

[[

[								

]]

4.1.5 Staffing and Qualification

4.1.5.5 Overview

Plant staff and their qualifications are important considerations throughout the design process. The planned initial staffing level is established based on experience with ABWR reference plants, staffing goals (such as optimizing the staffing levels and their qualification), initial safety function allocation, task analyses, and regulatory staffing requirements for nuclear reactors.

[[

]]

TA may show that the extended time for safety actions may reduce the number of staff needed for local actions. The HRA may show that some actions that were important in previous BWR designs are eliminated in the passive design. Improved display features may help clarify the plant state during transient events and possibly reduce the size of the control room staff. Moreover, tasks that have no direct interface to the allocated safety functions may be screened from HFE evaluation.

The details and content of the procedures and training for safety-related tasks are matched to the final baseline staff and qualifications developed during this HFE task.

4.1.5.5 Purpose

The purpose of S&Q plan is to:

- Establish an initial baseline shift operations staff appropriate for managing plant safety during normal operation of the ESBWR.
- Provide guidance, for the use of the initial staffing assumptions, in systematic evaluations of staffing needs and qualifications throughout the design effort.
- Recommend a refined description of baseline staffing needs and qualifications for using the ESBWR HSI.
- Address staff HSI needs, a screening process is used to focus the HFE effort on the tasks and staff needed to support reactor safety functions.
- Provide baseline ESBWR S&Q inputs for systematic verifications of the HSI design, and development of procedures and the training program.

The detailed evaluation of HSI requirements for maintaining plant safety and availability goals over the complete range of transient event conditions clarifies the basis for the staffing and qualifications of the baseline ESBWR. The evaluation is accomplished through the systematic examination of the design specific ESBWR functions, tasks, known priorities, risk importance of HAs, and baseline procedures. Recommendations for changes in the baseline ESBWR plant S&Q is provided in a results summary report. The recommended staffing level is reflected in ESBWR procedures and training program design.

4.1.5.5 Scope

The scope of this task recommends a baseline staff and their qualifications for safely operating the ESBWR during normal power operation, as well as during transient events included in the plant design basis. The applicable plant personnel, who are addressed by the HFE program prior to plant startup, include licensed control room operators as defined in 10 CFR 50.54m and 50.55.

The categories of personnel defined by 10 CFR 50.120, who perform tasks related to plant safety through the HSI, are screened for tasks involving reactor safety functions allocated to manual operation that are monitored and controlled through the HSI. The personnel include non-licensed operators, shift supervisor, shift technical advisor, instrument and control technicians, electrical and mechanical maintenance personnel, radiological protection technicians, chemistry technicians, and engineering support personnel.

In addition, any other plant personnel who perform tasks that are directly related to plant safety are addressed. The tasks they perform include:

- Qualification.
- Repair.
- Maintenance.
- Record keeping.
- Configuration control.
- Monitoring, automatic actions.
- Surveillance and testing.

These tasks are performed on plant equipment during startup, normal operations, abnormal operations, transient conditions, low power, and during shutdown conditions.

The initial focus of this task during the design stage is on the shift personnel controlling the plant during normal operations through the applicable HSIs needed for operations and response to transient events, for example, operator interface in the Main Control Room (MCR), the Remote Shutdown Systems (RSSs) panels, and Local Control Stations (LCSs) with a safety-related function or as determined by high level task analysis.

The initial proposed baseline staff for plant operation during shifts is expanded to include personnel who perform tasks related to plant safety as the design progresses to the combined operating license (COL) applicant and plant operation. The overall staffing analysis prior to plant start up recommends the number and background of personnel for the full range of plant conditions and operational tasks (normal, abnormal, and emergency), plant maintenance, and plant surveillance and testing.

An organizational staff is recommended by the utility using input from past operational S&Q experience and the design phase HFE program on specific safety-related tasks to address the full range of activities at the plant. For example, staff needed to plan and conduct work for planned outages or during outages for equipment maintenance, handling and storage of new or spent fuel, and radioactive materials is addressed using past operational experience with input from the HFE to refine either staff assignments or qualifications.

Recommendations for personnel involved in administration, security, training, engineering, fire/hazard response, access monitoring, record keeping, or local services (for example, cafeteria and janitorial) reflect operating utility experience and regulatory requirements. During initial design, it is assumed that personnel needed to accomplish these activities are available, but are not included in the baseline operational staff for normal shifts. As the design progresses and if a task using the safety system HSI is identified during the HFE analysis for site support staff, recommendations for refinement to the staff and their qualifications are provided. The operational staffing organization is under the authority of the licensee (for example operating utility).

External personnel brought in for special maintenance and repair are assumed to also use elements of the HSI during outages, refueling, and waste handling. Tasks for external personnel may be identified during the HFE process; however, personnel for these tasks are not included in the baseline staffing for plant operations.

[[

]]

4.1.6 Human Reliability Analysis

4.1.6.5 Overview

For advanced nuclear power plants such as the ESBWR, the NRC expects that vendors address severe accidents during the design stage using Probabilistic Risk Analysis (PRA) tools. This allows the designers to take full advantage of the insights gained from the probabilistic safety assessments, operating experience, severe accident research, and accident analysis by designing features to reduce the likelihood that severe accidents will occur and, in the unlikely occurrence of a severe accident, to mitigate the consequences of such an accident. Incorporating insights and design features during the design phase is more cost effective than modifying existing plants.

Quantification of human interactions is a needed element for making risk-informed performance-based decisions in the context of severe accident sequences. The human reliability analysis (HRA) element of a PRA enhances understanding of the impact that operator actions have on measures such as core damage frequency (CDF), and large early release frequency (LERF). The HRA also supports evaluation of margins to safety goals on these risk measures.

HRA is a required activity of a probabilistic risk assessment (PRA) for both pre- and post-initiator human actions as established in ASME-RA-S-2002 [2.4(3)]. This input to the Human Factor Engineering process provides a means for prioritizing the HSI needs based on specific human actions that contribute to the overall safety of the plant.

Since there is a perceived difficulty in providing quantitative estimates of human reliability due to a lack of data, many risk-based assessments take little credit for planned operator actions that can be taken to avert potential accident conditions or mitigate their consequences. Key factors that influence planned operator actions that are considered as operational defense-in-depth elements are:

1. Ability of the Human System Interface (HSI) to detect and present abnormal conditions to the operators.
2. Selection of personnel with abilities for plant and main control room (MCR) operations.
3. General training of operators.
4. Level of operator training for specific actions and contingency planning.
5. Robustness of the procedures for a wide range of accident conditions.

6. Availability of HSI for monitoring, controlling, and providing feedback on actions taken in response to specific events.

[[

]]

4.1.6.5 Purpose

This implementation plan describes how information generated by HRA tools is used to support the HSI HFE design goals. This occurs when use of the HSI impacts a significant accident sequence defined in the PRA. The initial "design level" ESBWR PRA/HRA is submitted in support of NRC licensing requirements using an HSI reference design with many system features from predecessor ABWRs. The key ESBWR design features of passive safety systems and natural circulation in the core change the way traditional defense in depth barriers are protected. The HSI reflects these design features as well as technology advances in indication displays, control and instrumentation approaches (e.g., analog to digital).

Risk-informed decision-making is used to justify the specific design features for the ESBWR. Changes from the predecessor BWR licensing basis meets a set of key principles. These principles are written in terms typically used in traditional engineering decisions (e.g., defense in depth). While written in these terms, it is understood that risk analysis techniques are encouraged to help ensure and demonstrate that these principles are met. The following bullets from RG 1.174 provide a framework for interpreting and evaluating changes in risk when design choices are made for the HSI during the design process.

- The proposed change meets the current regulations unless it is explicitly related to a requested exemption or rule change, i.e., a "specific exemption" under 10 CFR 50.12 or a "petition for rulemaking" under 10 CFR 2.802.
- The proposed change is consistent with the defense-in-depth philosophy.
- The proposed change maintains sufficient safety margins.
- When proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.
- The impact of the proposed change should be monitored using performance measurement strategies.

HRA update iterations with the PRA addresses the impact of human-error mechanisms on the ESBWR HSI design. Through these updates, the impact of HSI changes on core damage frequency and large early release frequency evaluations can be assessed. The update assessment permits evaluations of margins to safety over established safety goals (e.g., RG 1.174[2.2.3(9)]) based on the inherent design features in the ESBWR and the HSI.

Human errors identified and quantified in the PRA are analyzed to determine if new or modified HSI design features are needed to reduce the likelihood and impact of those errors on accident sequences. The HRA activity both qualitatively and quantitatively links the HFE program into the PRA and risk analysis. In addition, the results become design inputs to the software development activities.

Operator requirements for maintaining plant safety and availability goals over the complete range of transient event conditions are clarified through systematic examination of the functions, tasks, known priorities, risk importance, procedures, and training. Any resulting changes in the recommended baseline ESBWR plant S&Q are provided in revisions to S&Q Results Summary

Report document. The recommended staffing level is reflected in procedures and training program design.

4.1.6.5 Scope

This plan establishes a HRA process in conformance with the NEDO-33217 ESBWR Man-Machine Interface System (MMIS) and Human Factors Engineering Implementation Plan and NUREG-0711r2, Human Factors Engineering Program Review Model. The interaction of the HRA tasks with other HFE tasks is shown in Figure 4.1.6-1.

The scope of this plan includes the following:

- Using a multidisciplinary team as described in Section 3 to analyze human actions within the context of the PRA.
- Developing a process for using PRA/HRA (e.g., level 1, level 2, internal and external events) to support the design of the ESBWR HSI. An initial working process is shown in Figure 4.1.6-2.
- Identifying and selecting HRA elements and key actions that impact the quantitative risk estimates.
- Clarifying the role of operators, through applicability of the HSI to support key operator tasks, emergency procedures and training, and to protect the plant from accident challenges.
- Clarifying the role of operators by obtaining design information related to factors that affect human performance.
- Iterating with the probabilistic risk assessment, task analysis, and operating experience data to reevaluate the impact of operator actions on measures of risk as a function of changes to the HSI (e.g., modeling the impact on human reliability of proposed HSI designs in different modes of operation and transitions between modes.)
- Updating and integrating the quantification of HRA elements as needed using available data, information interface, performance shaping factors (PSFs) and quantification models.
- Evaluating the effect of operator actions on uncertainties and sensitivities associated with the event sequence.
- Providing input to the HFE Issue Tracking System (HFEITS).

[[

]]

4.1.7 HSI Design

4.1.7.5 Overview

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

identified, refined, and established. The purpose is to ensure consistency with accepted HFE guidelines, principles, and methods. The result is a safe, simple, and standardized plant design.

[[

]]

The HSI design methodology establishes standardization and consistency in applying HFE guidelines, principles, and methods. The process and the rationale for the HSI design are documented and managed under General Electric Energy Nuclear (GEEN) Quality Assurance (QA) [2.1(1)] and the sections of this MMIS and HFE Implementation Plan.

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

The Nuclear Regulatory Commission's guidance document NUREG-0700, breaks the HSI into three basic elements:

- Information Displays.
- User-Interface Interaction and Management.
- Controls.

Those elements are delineated into seven system functions, which are:

1. Alarms.
2. Safety Function and Parameter Monitoring.
3. Group-View Displays.
4. Soft-Controls.
5. Computer-Based Procedures.
6. Computerized Operator Supports.
7. Communication.

NRC guidance documents discuss workstation and workplace design as well as HSI support. The ESBWR HSI implementation plan takes into account and uses as practical and appropriate the NUREG guidance that is provided as baseline HSI plan development.

The HSI Design Implementation Plan establishes:

- The methods and criteria for HSI design in accordance with accepted human factors practices and principles.
- That the HSI design:

  - Implements the information and control requirements developed through the operational analyses, including the displays, controls, and alarms necessary for the execution of those tasks identified in the task analyses as being critical tasks.
  - Defines the basis for a style guide for alarms, displays, and controls as defined the ESBWR operational analyses.
- The methods for comparing the consistency of the HSI human performance, equipment design, and associated workplace factors with those modeled and evaluated within the completed task analysis.
- The HSI design criteria and guidance for control room operations during periods of maintenance and test.
- The test and evaluation methods for resolving HFE/HSI design issues. These test and evaluation methods include the criteria to be used in selecting HFE/HSI design and evaluation tools.

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

The HSI design includes features, which facilitate operator activities intended to maintain the operators' vigilance. Features of the HSI are designed using methods that are based upon applicable industry research and publications. The bases for the features, including a review of the experience of selected HSI features are a part of the documented design.

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

Human factors principles are followed and the color-coding, mimics, labeling, and demarcation are applied consistent with the main control room consoles.

4.1.7.5 Purpose

This HSI plan develops the process by which the ESBWR HSI design requirements are identified, refined, and established. The purpose is to ensure consistency with accepted HFE guidelines, principles, and methods. The result is a safe, simple, and standardized plant design.

This plan systematically delineates the requisite HFE principles necessary to translate functional and task requirements to the design of alarms, displays, controls, and other aspects of the control and instrumentation systems and HSI. Figure 3.2.4-1 shows where this HSI Design Implementation Plan fits into the overall HFE Process.

The primary goal for HSI designs is to facilitate safe, efficient and reliable operator performance during all phases of normal plant operation, abnormal, and emergency conditions. Maintenance, test, and inspection activities are also considered. To achieve the operator performance goals, information, displays, controls, and other interface devices in the control room and other plant areas are designed and implemented in a manner consistent with good HFE practices. The goals can be summarized as fulfilling the following:

- Maximize plant capacity/output power levels.

- Achieve and maintain high reliability.
- Achieve and maintain high availability.
- Maintain high levels of safety.
- Maintain high levels of operator awareness of the plant and equipment states.
- Minimize the likelihood of human errors.
- Integrate fault tolerance and fault recovery into the systems (both from potential human and equipment errors).

4.1.7.5 Scope

The scope of this HSI Design Implementation Plan establishes:

1. The methods and criteria for designing the HSI in accordance with accepted human factors guidelines, principles, and methods.
2. HSI information and control requirements. These requirements will address the information control needs to:
   a. Support critical tasks identified through the operational analyses.
   b. Identify the displays, controls, and alarms necessary for the execution of those tasks.
   c. Ensure identified plant parameters used for calculation of operational limits are presented as alarms, displays, and controls.
   d. Eliminate errors associated with risk-important human actions.
   e. Identify error-likely situations.
3. Methods for comparing the consistency of the HSI human performance, equipment design, and associated workplace factors with those identified and evaluated through the operational analysis.
4. HSI design criteria and guidance for operations during periods of maintenance and test.
5. Test and evaluation methods to identify HFE/HSI design issues.
6. Documentation for any human engineering discrepancies (HEDs) as well as strategies for HED resolution.

[[

]]

4.1.8 Procedure Development

4.1.8.5 Overview

Procedures are key to plant safety because they support and guide personnel interactions with plant systems and with responses to plant-related events. Procedures used to operate the plant include:

- Normal Operating Procedures.
  - General Plant Procedures (GPPs).
  - System Operating Procedures (SOPs).
  - Calibration, Inspection, and Testing Procedures.
  - Maintenance and Modification Procedures.
  - Radiation Control Procedures.
- Abnormal Operating Procedures.
  - Alarm Response Procedures (ARPs).
  - Abnormal Operating Procedures (AOPs).
- Emergency Operating Procedures.
  - Emergency Operating Procedures (EOPS).
  - Severe Accident Management Guidelines (SAMGs).
- Administrative Procedures.

Procedures are an integral part of the Human-System Interface (HSI) development for the ESBWR and are issued as controlled procedures. The Combined Operating License Owner's Group (COLOG) maintains the controlled versions of the standard procedures throughout the plant operating life.

Human factor improvements in plant procedures help prevent or mitigate potential human error. Procedure development supports improvements in the Human System Interface (HSI), plant hardware (e.g. in ergonomic layout), training, and other areas. The approach to reducing human error is to simplify the information reaching the operating personnel and to enable control room personnel to have a clear understanding of the plant status at any time. Through the HSI and procedures, operating personnel control the plant under normal, abnormal, and emergency conditions.

[[

]]

In the ESBWR, opportunities for human factor improvements in the way procedures are used are enhanced through both the passive design and the use of digital computer systems. Digital control, computer, and monitoring systems have advanced capabilities for monitoring progress in implementing procedure steps based on the controlling cue for a procedure, equipment status, and monitored variables. For example, computers can call up procedures for routine testing based on an established schedule. Additionally, computers can present the procedures that operators need to use for checking plant conditions and taking recovery if specific variables exceed preset conditions. Such Computer-Based Procedures (CBPs) are carefully designed, verified, and installed to ensure that residual faults and design errors do not mask or prevent any required safety action.

4.1.8.5 Purpose

The purpose of the procedures development plan is to provide the processes, methods, and criteria for generating procedures and verifying that the integrated plant procedures are consistent with accepted HFE practices and principles. The HFE design team ensures that human factor principles are incorporated into the development and updating of procedures using applicable guidance from Section 13.5 of NUREG-0800 [2.2.1(5)(6)][2.5 (9)] and NUREG-0711 [2.5(2)].

The procedure development process shows how the HFE design team uses the outputs from operational analysis and the HSI design to develop initial ESBWR procedures. These procedures are inputs to other steps in the overall HFE process (as shown in Figure 3.2.4-1) where enhancements are identified resulting in revisions to the procedures. Such improvements reduce the potential for human error and produce procedures that are compatible with the ESBWR Emergency Procedure Guidelines (EPGs), design, and the operating philosophy for the HSI.

At the end of the overall MMIS and HFE implementation process, the design engineers and procedure writers provide approved procedures ready for verification. The MMIS implementation plan includes V&V steps that provide assurance that all functions and tasks assigned to be human actions or human backup are included in the integrated procedures. The MMIS implementation process also includes validation of the procedures using mockups, part-task simulators, and full-scope simulator facilities to simulate operations, transients, and accidents. The HFE design team provides evidence of the acceptable incorporation of HFE principles through sign off on the procedures.

4.1.8.5 Scope

The scope of this implementation plan is to describe the process for ESBWR plant operating procedure development stressing the interface with other HFE tasks. The procedures include normal, abnormal, and emergency operating procedures used by the control room operators to manage plant operation and safety.

Normal, abnormal, and emergency operating procedures that match the HSI design are provided to the COLOG and the licensees at the end of the overall process. The MMIS design implementation includes steps that verify all functions and tasks assigned to human action or human backup (as a result of operational analysis) are included in the normal, abnormal, or emergency operating procedures. This includes procedures used to accomplish normal operation, maintenance, radiation control, calibration, inspection and testing, and emergency

actions performed at the operator interface in the Main Control Room (MCR), the Remote Shutdown Systems (RSSs), and risk significant Local Control Stations (LCSs). The MMIS implementation process also includes validation of plant procedures using mockups, walk-throughs, part-task and full-scope simulator facilities.

Procedure development evaluation includes verification and validation covering a full range of risk significant plant operating modes, including startup, normal operations, abnormal operations, transient conditions, low power, and shutdown conditions. The HFE evaluation also addresses risk significant personnel tasks during periods of maintenance of plant systems and equipment including the HSI equipment. As the maintenance, radiation control, and calibration, inspection, and testing procedures become available, they are validated through mockups, walk-throughs, part-task and full-scope simulator facilities.

The details of the scope are described as follows:

- Procedure development process incorporates human tasks through the following:
  - Identification of procedure tasks from the areas of normal, abnormal, and emergency operations.
  - Evaluation of procedures for a full range of plant operating modes, including startup, low-power, normal operations, shutdown, abnormal, transient, and emergency operating conditions.
  - Inclusion of Human Actions (HAs) that have been found to affect plant risk by means of Human Reliability Analysis (HRA)/Probabilistic Risk Assessment (PRA) importance in the appropriate procedures.
  - The generation of procedures that are linked to controls in the HSI.
- The procedure development process addresses issues such as the following:
  - Procedure content and layout adheres to recommendations in the procedure writer's guides.
  - Procedures exist to address the safety-related cues from the HSI.
  - Parameter readings for variables named in procedures match the scales and units in the HSI (as presented at the MCR, RSSs, and risk significant LCSs).
  - System and component names in the procedure match the names in the HSI and plant (e.g., it is easy to select the correct procedure).
  - Procedures match assumptions used for HRA quantifications of the Human Error Probability (HEP).

The procedure development process receives inputs from the operational analysis process, which incorporates inputs from the HRA/PRA, Baseline Record Review (BRR), Operating Experience Review (OER), and Design Control Document (DCD). Additional procedures development input comes from the HSI design process and in the form of feedback from the training development, V&V, and Human Performance Monitoring (HPM) processes. Outputs of the procedure development process support the training development process and the V&V process as well as provide feedback to the HSI design process.

The procedures generated by the process incorporate the following:

- HFE principles and guidance.
- Pertinent system design requirements.
- Technical accuracy.
- Content that is both explicit and comprehensive.
- Ease of use.
- Validation.

The validated procedures are called the Integrated Operating Procedures (IOPs). The IOPs within the scope of the HFE evaluation process include instructions for addressing normal, abnormal, and emergency conditions. Administrative procedures provide administrative control over activities that are important to the safe operation of the plant.

Additionally, procedures are revised as HPM analysis identifies enhancements necessary for safe operation of the plant and are maintained and updated as the plant is modified.

1. Normal Operating Procedures

Five types of normal operating procedures address conditions where operators control the plant when the plant systems are operating as expected. The five types of normal operating procedures are:

- General Plant Procedures (GPPs) - apply to startup, shutting down, shutdown, power operation and load changing, process monitoring, and fuel handling.
- System Operating Procedures (SOPs) - apply to energizing, filling, venting, draining, starting up, shutting down, changing modes of operation, and other instructions appropriate for operation of systems important to the safe operation of the plant.
- Calibration, Inspection and Testing Procedures - apply to the process of demonstrating that systems and components are capable of satisfactory performance in the future. Specific calibration, inspection, and tests are listed in the station's technical specifications and procedures are generated to support the performance of each required test.
- Maintenance and Modification Procedures - apply to repairing or replacing equipment or performing preventative maintenance designed to improve the reliability of the equipment.
- Radiation Control Procedures - apply to the monitoring and release of solids, liquids, and gasses, access controls, area radiation monitoring, and the program for keeping dose As Low As Reasonably Achievable (ALARA).

2. Abnormal Operating Procedures

AOPs address conditions during operation that involve an unplanned or undesired event or occurrence involving a Structure, System, or Component (SSC). These procedures provide steps to resolve the undesired event. For example, these procedures may call for the use of redundant plant systems and safety functions while the undesired event condition is being evaluated and

resolved. The procedures are not individually listed in a table because the AOPs and ARPs are numerous and correspond to the number of alarms.

- Abnormal Operating Procedures (AOPs) - apply when operating variables depart from a normal range by providing instructions for restoring the variable. Each safety-related alarm has its own written response procedure, which typically contains:
  - Meaning of the alarm.
  - Source of the signal and its alarm setpoint.
  - Actions that occur automatically.
  - Initial operator action.
  - Long-range operator actions
- Alarm Response Procedures (ARPs) - apply when a specific alarm indicates that a plant variable exceeds a warning or safety set point level. ARPs provide instructions for restoring components or systems to a normal condition (e.g., with no other or minor alarms pending).

The Alarm Response procedures comply with Section 4.5 of NUREG-0700 [2.5(3)] (plus errata). If application of the AOP is not successful in correcting the plant variable and a safety parameter is exceeded or the plant trips from a manual action or automatic signal, EOPs apply.

3. Emergency Operating Procedures

EOPs provide instructions for mitigating the consequences of transients and accidents that cause plant parameters to exceed reactor protection system or engineered safety features actuation set points.

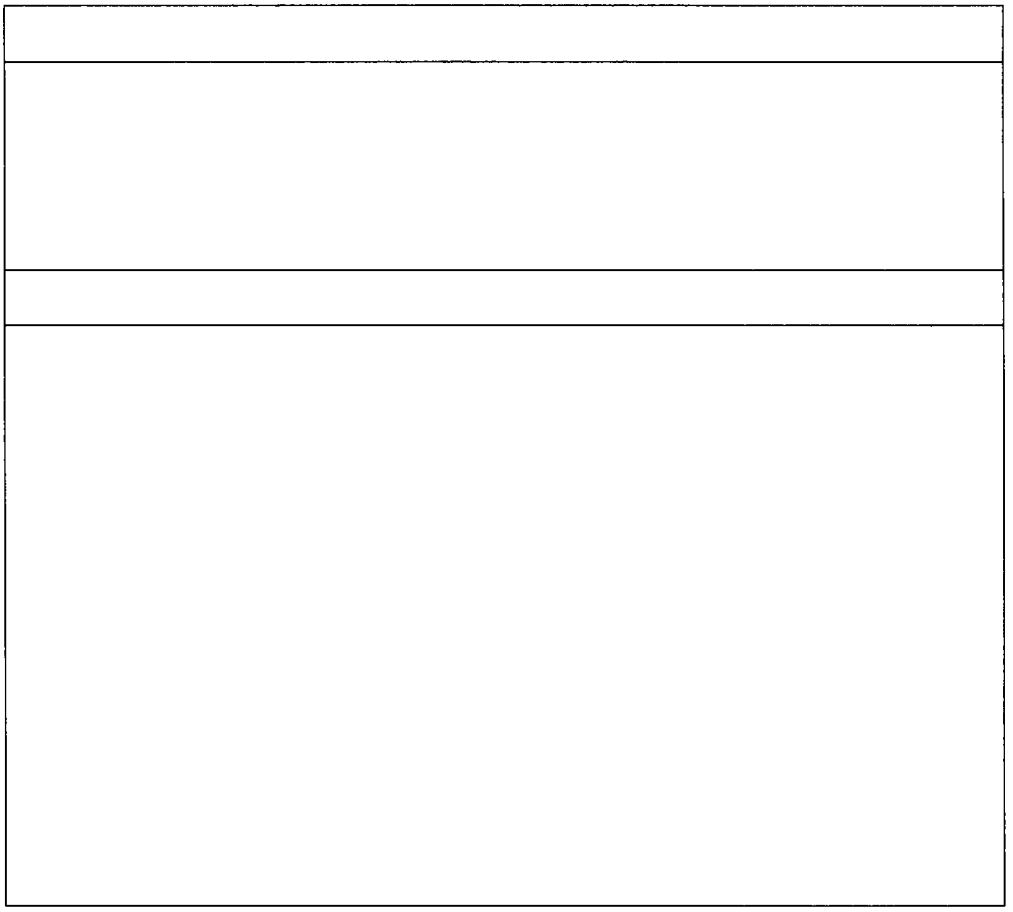
- Emergency Operating Procedures (EOPs) - The EOPs are developed from ESBWR standard Emergency Procedure Guidelines (EPGs) that establish the engineering basis, strategies, and intent for managing plant transients and trip events. Any changes in the plant specific EOPs must conform to the EPGs and the EOP writer's guide.
- Severe Accident Management Guidelines (SAMGs) – The SAMGs are developed from ESBWR standard Severe Accident Guidelines (SAGs) that establish the engineering basis, strategies, and intent for managing plant accidents that necessitate the flooding of containment. Any changes in the plant specific SAMGs must conform to the SAGs and the EOP writer's guide.

EOPs and SAMGs comply with all applicable guidance and requirements in EPG/SAG Rev 2, NUREG-0899 [2.5(5)], and NUREG-0737 [2.5(4)].

4. Administrative Procedures

Administrative procedures provide administrative control over activities that are important to the safe operation of the plant. The scope of administrative procedures addressed in the HFE procedure development is addressed in the Procedures Development Implementation Plan [2.3.1(9)].

[[



]]

4.1.9 Training Development

4.1.9.5 Overview

Training of plant personnel is a key factor in ensuring safe and reliable operation of nuclear power plants. The ESBWR training program provides assurance that plant personnel have the knowledge, skills, and abilities to properly perform their roles and responsibilities. In this way, training supports the safety culture of the plant organization including operations, maintenance, engineering, radiation control personnel, and other plant staff.

Training program development information is gathered through coordination among training development and other elements of the Human Factors Engineering (HFE) design process. For example, Task Analysis (TA) provides a systematic analysis of safety-related job and task requirements that are then used to shape training requirements. These plant operator tasks become an integral part of the Human-System Interface (HSI) training for safely managing ESBWR events.

Human factor improvements in the HSI, coupled with effective training in their use, help to prevent and mitigate human error. To support the objective of eliminating human error, training ensures that plant personnel clearly understand information presented by the HSI. Thorough

understanding of HSI data presentations ensures the information can be used to assess plant status at any time.

A similar understanding of the HSI controls and the use of procedures enable plant personnel to control plant operation under normal, abnormal, and emergency conditions. As shown in Figure 3.2.4-1, the ESBWR is designed using a systematic process for integrating human factor engineering principles into the system design using focused inputs and processes. The foundation for human factored training is established in the DCD, chapter 18, and is supported by DCD chapters 13 and 19. The HFE methods employed by the ESBWR project yield the core fundamentals of the training program. The series of human factors subject matter plans provide the substance for training program development.

Training modules are developed using industry best practices to reflect the ESBWR design and operating philosophy and its unique characteristics such as natural circulation and passive cooling. As the details of the HSI are finalized, the Verification and Validation (V&V) process supports an integrated evaluation of the HSI, procedures, and training. To ensure complete integration and consistency, human factors principles are applied to the development of HSI hardware, software, procedures, and training. Mock-ups, part-task simulators, and full-scope simulators are used to validate the integrated design.

4.1.9.5 Purpose

The training development plan presents the processes, methods, and criteria for systematically incorporating information from the HFE design process into the training program for ESBWR personnel. The ESBWR training program is based on the following five systematic training activities:

- Systematic analysis of the tasks and jobs that are triggered by cues from the HSI design, operational analysis, procedures, or feedback from V&V, design implementation, and human performance monitoring.
- Development of learning objectives derived from analysis of requisite performance.
- Design and implementation of training based on the learning objectives.
- Evaluation of trainee mastery of the learning objectives during training.
- Evaluation and revision of the training based on the performance of trained personnel in the job setting.

The plan addresses methods, processes, and criteria for verifying that plant training is consistent with accepted ESBWR HFE practices and principles. The HFE team uses the training development process to ensure that human factor principles are incorporated into the development and updating of training. Through this process, applicable guidance of Section 13.5 of NUREG-0800 [2.2.1(5)(6)][2.5(9)] and NUREG-0711 [2.5(2)] are addressed. The training development process demonstrates how the HFE team uses results from other HFE tasks and feedback from the other HFE plans to institute training improvements. The goal of training process improvements is to reduce the potential for human error in keeping with the ESBWR design and operating philosophy.

Training development generates training modules, approved by the HFE team, that match the ESBWR HSI design and procedures. The V&V of training results ensures that all functions and tasks assigned to plant personnel are included in the integrated training program and have been mastered by plant personnel. Additionally, the overall HSI implementation process validates the training for normal operations, transients, and emergencies using mockups, part-task, and full-scope simulators. The HFE team provides evidence of the acceptable incorporation of HFE principles through sign off on training modules and documentation of the identification and resolution of HFE issues.

4.1.9.5 Scope

The training program provides training for both licensed and non-licensed plant staff. Training and retraining programs incorporate operating experience. The training programs include all phases of plant operation including preoperational and low-power operation. The ESBWR HFE design organization is responsible for providing information on operator tasks that impact plant safety at the component, system, and integrated plant level and incorporating them into the training program.

The HFE training development implementation plan describes how training information and issues developed through other HFE activities become inputs to specific elements of the training program. Information and issues relevant to the development of operator training are identified early in the HFE program during the operational analysis process, which includes functional analysis, allocation of functions, and task analysis. As the HFE Design process continues, other HFE activities including Staffing and Qualifications, Procedures Development, V&V, and HPM identify other training inputs.

The following items provide a systematic approach for training elements that are developed and supported by the HFE design team:

- General training approach - uses results of the systematic job/task analysis performed by the HFE team and described in the procedures.
- Organization of training - addresses training modules that are required by the NRC, basic knowledge, and operational training on ESBWR systems. Training includes normal, postulated abnormal, and emergency conditions using plant specific procedures and full scope simulator.
- Learning objectives - are derived from an analysis of desired post-training performance including content required by the NRC, lessons learned from operating plants experiences, plant specific ESBWR features, and special issues collected in the Human Factor Engineering Information Tracking System (HFEITS).
- Content of training program - includes design and implementation of training based on the learning objectives according to:
  - The schedule and content of NRC guidelines.
  - Key safety actions that are required for functions, systems, and tasks as defined and allocated in operational analysis.

  - Risk-important human actions needed to manage accident sequences defined by the Human Reliability Analysis /Probabilistic Risk Analysis (HRA/PRA).

- Evaluation of training - addresses evaluation of trainee mastery of the learning objectives including performance assessment of unique HRA/PRA scenarios on the plant full-scope simulator.
- Periodic re-qualification training - incorporates evaluation and revision of the training program based on the performance of trained personnel in the job setting. The scope and frequency of retraining focuses on the training elements provided at the end of the HSI implementation process and risk significance of subject matter.

The overall scope of training is defined by the training development process and supported by the HFE design team. The HFE training scenario inputs include:

- Normal operation training modules – normal training includes specific operational activities (for example, start up, normal, and shutdown operations, maintenance, testing and surveillance actions) that exercise the use of System Operating Procedures (SOPs), technical specifications, and pre-initiator actions in the HRA/PRA.
- Abnormal operation training modules – postulated transients or abnormal events and key HRA/PRA sequences that occur during specific plant conditions, such as normal operation, startup, shutdown, and refueling, that exercise decision making and use of Abnormal Operating Procedures (AOPs) and Integrated Operating Procedures (IOPs).
- Emergency operation training modules – design basis accidents and key HRA/PRA sequences that occur during specific plant conditions, such as normal operation, startup, shutdown, and refueling, that exercise decision making and use of Emergency Operating Procedures / Severe Accident Guidelines (EOPs/SAGs).
- Key human action response modules – inputs to the accident training modules are defined for cues from the HSIs (for example, in the main control room, remote shutdown station, local control stations) using emergency, abnormal, and system operating procedures.

Training addresses:

- Plant personnel including licensed and non-licensed personnel whose actions may affect plant safety.
- Plant functions and systems with emphasis on those that are risk-important.
- The full range of plant conditions (for example, normal, abnormal, emergency.)
- HSIs (for example, main control room, remote shutdown panel, risk-important local control stations, display space navigation, operation of "soft" controls) over the full range of plant conditions. Emphasis is placed on those that are risk-important.
- Specific operational activities (for example, operations, maintenance, testing, startup, shutdown, and refueling,).
- Key actions as required by cues from the HSI (for example, MCR, RSS, and LCSs.).

[[

]]

4.1.10 HF Verification and Validation

4.1.10.5 Overview

Verification is the process of determining and documenting that an implemented design (a product, process, procedure, method, etc.) meets its specifications. Verification answers the question: Was the design implemented appropriately?

Validation is the process of determining and documenting that the design effectively serves the purpose for which it was intended. Validation answers the question: Was the appropriate design implemented?

The subject of the HF V&V is the design of the ESBWR human system interface (HSI) elements. HSIs are the controls, displays, annunciators, procedures, data processing, and communication systems to accomplish operation and maintenance tasks and actions as defined by task analysis (TA), emergency operating procedures (EOPs), other procedures, probabilistic risk assessment (PRA) analysis, and human reliability analysis (HRA).

The validity of the MCR, RSS, and LCS HSI designs are determined on the basis of:

- ESBWR operator performance (human error, situation awareness, vigilance).
- Physical and cognitive workload imposed on the ESBWR operators.
- Tolerance to human errors (omitting required actions, committing wrong actions) and machine faults (hardware and software).

4.1.10.5 Purpose

The purpose of this activity is to verify and validate that the HSI supports operator tasks and important actions identified from the project's operational analysis. Verification and validation (V&V) is one element of NUREG-0711, Rev 2 Human Factors Engineering (HFE) Program Review Model. V&V, in the context of HFE, assures that the design of Human-System Interfaces (HSIs):

- Are complete.

- Conform to HFE principles.
- Are operable.
- Are free of safety issues and human performance issues.
- Are correctly implemented in a final, "as built" form.

The Human Factors V&V implementation plan addresses the following elements for the conduct of the HFE V&V:

- Program management.
- Requirements and objectives.
- Trainees as participants (including provisions for audits and witnessing).
- Methods and procedures.
- Test conditions, data collection, and analysis.
- Acceptance criteria and performance measures.
- Documenting, reporting, and integrating results.

4.1.10.5 Scope

1. The following HSIs and associated design elements are verified and validated in the HF V&V:
   - Human-System Interfaces (i.e., controls, displays, and alarms including use of Safety Parameter Display System).
   - Layout/configuration and anthropometrics of workstations (including installed equipment such as phones and radios).
   - Automation features.
   - Display navigation (efficient information retrieval and access to controls).
   - Crew Communications (i.e., methods and equipment).
   - Procedures (hardcopy and electronically displayed).
   - Operator work environment (e.g., lighting, space, air conditions, floor design, noise mitigation).
   - Provisions for routine tests and maintenance (i.e., cleaning touch-screen displays, testing alarm windows, replacing mimic components). The scope of the program encompasses the design bases (e.g., ESBWR Design Control Document (DCD) requirements), standard design features of the ESBWR MCR, and the results of ESBWR HFE analyses.
2. Facilities within the scope of the program include, but are not limited to, the MCR, the RSS, and locations of LCSs critical to plant safety. The Reactor Building or Fuel Building, the Radwaste Building, the TSC, and the EOF are included to the extent they directly involve actions critical to plant safety (e.g., as defined through Task Analysis, PRA/HRA, safety analyses, etc.).

3. HSIs within the scope of the program include HSIs used for operations, accident management, maintenance, test, inspection, and calibration interfaces (including procedures).
4. Plant staff positions addressed in the program include those positions identified by the Staffing and Qualifications Plan [2.3.1(5)].
5. The implementation of the HF V&V activity is predicated on the use of the following test and evaluation environments, as discussed in the HF V&V implementation plan:
   - Mockup.
   - Part-Task Simulator (single category replacing the GE Test System and Baseline simulators described in the HF V&V implementation plan).
   - Full Scope Simulator (FSS).
6. The validation activity supports training program development, although the link between validation activities and training support is not directly the scope of the V&V process.
   - The training team and operators in training perform various verification and validation tasks.
   - Training benefits from the development of the V&V simulator scenarios.
   - The information collected during the validation process acts as performance benchmarks for the various scenarios.
7. Responsibilities of the design organizations for the V&V program and the roles and responsibilities of the V&V team are defined in the HF V&V implementation plan.

[[

]]

4.1.11 Design Implementation

4.1.11.5 Overview

The Design Implementation Plan addresses the final "as-built" implementation of the Human Factors Engineering (HFE) guidance into ESBWR standard plant design. The standard design includes standardized Human System Interfaces (HSIs), procedures, and training. The ESBWR Combined Operating License Owners Group (COLOG) is responsible for establishing and maintaining the standard plant design and good human factors practice.

[[

]]

The HFE aspects of the ESBWR standard plant including design of the HSIs, standard plant procedures, and standard plant training documentation, are verified and validated using the Full Scope Simulator (FSS) during the HFE Verification and Validation (HF V&V) process. The Design Implementation activity is performed to assure that the "as-built" HFE design conforms to the design that was used in the ESBWR standard plant HF V&V efforts.

[[

]]

4.1.11.5 Purpose

The purpose of the design implementation activity is to:

1. Confirm that the final HSIs, procedures, and training (as-built) HFE design conforms to the ESBWR standard plant design resulting from the HFE design process and HF V&V activities. Any identified human engineering discrepancies (HEDs) are assessed and properly addressed.
2. Verify aspects of the design that may not have been evaluated previously in the HF V&V process. This includes any hardware/software, new or modified displays that were absent from the simulator-based integrated HF V&V process, and any physical or environment (for example, noise, lighting, so forth) differences between those present at the HF V&V process and the "as-built" Main Control Room (MCR).
3. Verify resolution of remaining HEDs and open items from the Human Factors Engineering Issue Tracking System (HFEITS).
4. Transfer design implementation responsibility to the COLOG.
5. Transfer responsibility for HFEITS to COLOG.

4.1.11.5 Scope

The "as-built" confirmations, verifications, and validations described in the Design Implementation plan apply to the initial COL plants associated with the ESBWR design effort. Thereafter, the COL applicant and the COLOG are responsible for:

- Regulatory obligations of design implementation.
- Application of the "as-built" confirmation to all stations, panels, components, and elements managed under the ESBWR HFE program.

The ESBWR standard plant design against which the "as-built" comparison is made is derived from the revised HSI design and the standard plant procedures and training documents. These include the corrections and improvements from the HF V&V process. The ESBWR standard plant design remains the intellectual property of General Electric.

[[

]]

4.1.12 Human Performance Monitoring

4.1.12.5 Overview

The HPM plan links human factors engineering (HFE) results developed during design with methods for monitoring human performance during operation by the licensee. HPM employs diverse programmatic inputs and an integrated system of evaluation. The human performance

monitoring implementation plan (HPMIP) as shown in Figure 4.1.12-1 illustrates how the HFE activities are performed during the design support of the ESBWR operations.

The COL Owners Group (COLOG) provides a means for consistently maintaining safety performance levels established through staffing, training, procedures, and design as described in the ESBWR Design Control Document (DCD) [2.1(2)]. Individual ESBWR licensees' programs may vary in content and level of detail; however, the standards established by the COLOG are followed.

4.1.12.5 Purpose

The objective of the ESBWR HPM is to ensure that no safety degradation occurs due to changes in design, procedures, training, or staffing. The HPMIP incorporates a strategy for monitoring the performance of personnel and equipment that is integrated with existing programs. Preservation and improvement of human performance and economic efficiency are predicated on the continued and coordinated operation of a standardized fleet.

HPM integration with existing programs provides an assurance that the ESBWR HFE design bases remain valid during the operational phase of the plant. These programs include

- Corrective Action Program (CAP).
- Maintenance Rule (MR).
- Human Reliability Analysis/Probabilistic Risk Assessment (HRA/PRA).
- In-service Inspection / In-service Testing (ISI/IST).

This HPM builds upon the HFE design activities that are carried forward into the operational phase. The ESBWR licensees' CAP, procedures, and training programs are incorporated to support the HPM process.

[[

]]

4.1.12.5 Scope

Completion and documentation of the initial plant HFE/HSI design verification by the ESBWR licensee provides a basis for HPM when plant operations begin. For example, HPM establishes benchmarks for human performance from specific tasks defined in the function allocation and task analysis, and verified during simulator testing in the HF V&V phase.

The monitoring of performance relative to these benchmarks ensures sufficient margin to fulfill assumptions supporting the General Design Criteria (GDC). The HPM strategy provides a reasonable assurance that the ability to interface among various HSIs within each facility is maintained effectively throughout the ESBWR operational phase in the following areas:

- Main control room (MCR).
- Remote shutdown station (RSS).
- Risk-important local control stations (LCS).
- Emergency support centers (emergency operating facility (EOF) and technical support center (TSC).

There are three entities that are tasked with developing and implementing the HPM plan during the ESBWR operating phase:

- GE.
- ESBWR licensee.
- COLOG.

The responsibilities of these organizations are described in the HPM Implementation Plan.

[[

[

]]

4.2 Software Development Process

4.2.1 ESBWR I&C Software Management Plan

4.2.1.5 Overview

The Software Management Plan (SMP) describes the software development process, the design documentation and design outputs to be followed and produced by the Instrumentation and Controls (I&C) design team and governs the design for the digital computer-based instrumentation and control software for the ESBWR, herein referred to as software products.

4.2.1.5 Purpose

The purpose of the SMP is to establish the managerial process, the software life cycle phases and the technical direction for the design and development activities of the software products.

The software life cycle phases are:

- Planning
- Requirements
- Design
- Implementation
- Test
- Installation
- Operations and Maintenance
- Retirement

4.2.1.5 Scope

The scope of the SMP includes software products as defined in section 1.2.4 with the software classifications of software Class Q, N3 and N2 as defined in SMP, Appendix C [2.3.1(13)] and SQAP [2.3.1(14)].

The software plans included in the SMP are:

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

4.2.1.5 Method

1. Management Priorities, Monitoring and Control

The objective of project management is to coordinate the development of project deliverables and to assure that the deliverables meet the COL applicant expectations for nuclear safety, quality, cost and schedule. The key elements for a successful project delivery are:

- Integrity – Integrity for all aspects of project performance is practiced at all times.
- Quality – Compliance with the software development and quality assurance process defined in the SMP and the SQAP [2.3.1(14)], and the applicable industry codes and standards.
- Occupational safety – Safe work habits are practiced at all times.
- Outputs – Deliverables meet the quality, schedule and budget requirements as specified by the project work plans.

GE Energy Nuclear (GEEN) project management policies and requirements are used to control and execute the software project. These requirements are:

a. Project Initiation

Project initiation begins after the contract has been awarded or an internal project is authorized. A preliminary schedule is developed which considers project resource availability and is consistent with the approved project work scope and budget.

b. Project Planning and Scheduling

[[

]]

Project planning kickoff meetings with the COL applicant, herein referred to as licensee are conducted to confirm that the contractual requirements are implemented. Risk assessment and risk management are performed and documented as part of the project work plan.

[[ ]]. The project work plan is updated as changes occur in the work scope and design inputs and outputs at the discretion of the PM.

The software development plan describes the software life cycle phases used in the design and development of the software products, design outputs for each software life cycle phase, which includes: software safety analysis (SSA), independent verification and validation (IV&V), and configuration management of the design outputs for each life cycle phase.

The phase baseline reviews are conducted for each software product or logical group at the end of each life cycle phase as is described in the SQAP. The reports are prepared in accordance with the SQAP.

c. Project Execution

Project execution activities include the initiation of material requisitions for services and materials. Project kickoff meetings are conducted with the project team to acquaint

the team with the activities and requirements specified in the project work plan. The project team consists of the PM, design team, Software Project Engineering (SPE) team member(s) and vendor. Project meetings (i.e., weekly, more frequent if needed to) is conducted with the project team and the external organization (licensee or vendor) to:

- Monitor the project progress,
- Identify critical path items/activities,
- Milestone dates for these items/activities,
- Identify the required level of manpower and resources needed throughout the project, and
- Identify project team and vendor performance problems to the appropriate leadership as soon as they are recognized.

[[

]]. Project progress report is prepared by the PM to ensure timely and appropriate reporting of project status and progress.

d. Project Controls

Project control activities include measurement and monitoring of project execution so adjustment can be made for schedule delays, unexpected changes in work scope, or quality issues stemming from internal or vendor performance challenges.

[[

]]

e. Post-Delivery Closeout

The objective of Post-Delivery Close out is to finalize the project and complete the delivery in accordance with the contract, closure of project paperwork, closeout of vendors' contract, and turnover of the project to the licensees.

Software project deliverables may include a combination of hardware, software, and design outputs. The project deliverables are identified in the licensee contracts. The project work plan specified the project deliverables and the milestone dates associated with the project delivery.

2. Risk Management

Risk Management is the process of identifying, controlling, and mitigating events that while may affect the project cost and/or schedule ensuring that nuclear safety and security are maintained. [[ ]].

3. Security

The design and development of software products are performed in a secured environment in accordance with Regulatory Guide 1.152 [2.2.3(2)].

a. Administrative control of access, which includes controls of both physical and electronic access, is setup for the design and test facility

b. The development platform for software products have installed isolation from external networks as one level of protection

c. Safety-related software products are designed to include security features to assure the software products are secure from electronic vulnerabilities. Security requirements to be considered during the design and development of the software products include but not limited to:

- Physical access control, and connectivity to external networks
- Ability to prevent unauthorized, undesirable, and unsafe intrusions to contaminate of software products with viruses such as Trojan horses and embedded bomb codes.

4.2.1.5 Implementation

The SMP defines additional methods, tools, procedures, and metrics for the activities described in Section 4.2.1.4.

4.2.1.5 Results

The activities and results of the SMP are the issuance of the SMP and the design documentation and design outputs described in the SMP.

4.2.2 ESBWR I&C Software Development Plan

4.2.2.5 Overview

The software development plan (SDP) describes the technical project development process for software products.

4.2.2.5 Purpose

The purpose of the SDP is to:

- Establish the standards, methods, tools, and procedures for the software design and development process.
- Define the activities performed for each phase of the software development.
- Define how requirements are traced to lower levels of the engineering from planning phase to test phase.
- Specify how the safety requirements are documented, evaluated, reviewed, verified, and tested during the design process to minimize unsafe, unknown, unreliable and abnormal conditions.
- Describe the organization and responsibilities of individuals or groups involved in the design and software functional test processes.
- Provide a structure for test and review guidance for software functional testing during the software life cycle.

- Provide the requirements and guidelines necessary to prepare, execute, and document software tests.
- Address software test documentation.
- Address metrics to include error tracking and resolution.

4.2.2.5 Scope

The SDP describes the software engineering development for each phase of the software products life cycle process. The phases include planning, requirements, design, implementation, test, installation, operations & maintenance (O&M) and retirement. The SDP also addresses the preparation, execution, and documentation of software testing for software products. The SDP conforms to RG 1.173 [2.2.3(8)] and IEEE 1074 [2.2.4(9)].

4.2.2.5 Method

Software engineering is a set of formal elements (methods, tools, documents, practices, standards and procedures) applied during each phase of the software life cycle. The software life cycle phases defined in this plan conform to and are based on RG 1.152 [2.2.3(2)], RG 1.173 [2.2.3(8)] and IEEE 1074 [2.2.4(9)]. A well-defined software engineering process, implemented in a traceable, planned, and orderly manner is key for the development and maintenance of high quality software.

The software life cycle phases [[ ]] are defined as follows:

1. Planning Phase. - During the planning phase, the project scope and methodologies, needed to support the development of the software products are established and defined. The planning activities include evaluation of system and licensee requirements, identification of resources, and development of project schedule and software safety analysis to determine software safety classification.

   [[ ]]

2. Requirements Phase – During the requirements phase, the detailed functional and performance requirements of the software products, design constraints, and acceptance criteria are defined. [[

   ]]

3. Design Phase – During the design phase, the software requirements are transformed into architectural and detailed representation of software. [[

   ]]

4. Implementation Phase – During the implementation phase, the software design is transformed into software source or application codes. The implementation phase activities also include software code review, software functional test.

Software functional test is conducted to validate the software source or application codes using a structured test approach. Software-software and software-hardware (typically, prototype hardware is used at this time) integration is performed during software functional testing.

[[ ]]

5. Test Phase – During test phase, software validation testing is conducted on the integrated software, when installed in the target or prototype hardware functions as intended and do not perform any unintended functions.

[[

]]

6. Installation Phase – [[

]] Installation must be performed in accordance with the approved installation procedure. Site Acceptance Test (SAT) and installation checkout are conducted to confirm the operation of the integrated software products.

[[

]]

7. Operations & Maintenance 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 software product in the O&M manual. [[

]]

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, effect on existing software products that are to remain operational in the operating environment, disposition of the retired software product including security disposition. This 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.

[[ ]]

4.2.2.5 Implementation

The design documentation and design outputs for each software life cycle phase are specified in Section 4.2.2.4.

4.2.2.5 Results

The following reports are completed for the phases identified:

- The planning phase baseline review report documents successful completion of this phase
- The requirements phase baseline review report documents successful completion of this phase.
- The design phase baseline review report documents successful completion of this phase.
- The implementation phase baseline review report documents successful completion of this phase.
- The test phase baseline review report documents successful completion of this phase.
- The installation phase baseline review report documents successful completion of this phase.
- The site acceptance test (SAT) is a [[ ]] test that is performed at the licensee site. The results are documented in the SAT report.[3]]]

[[

]]

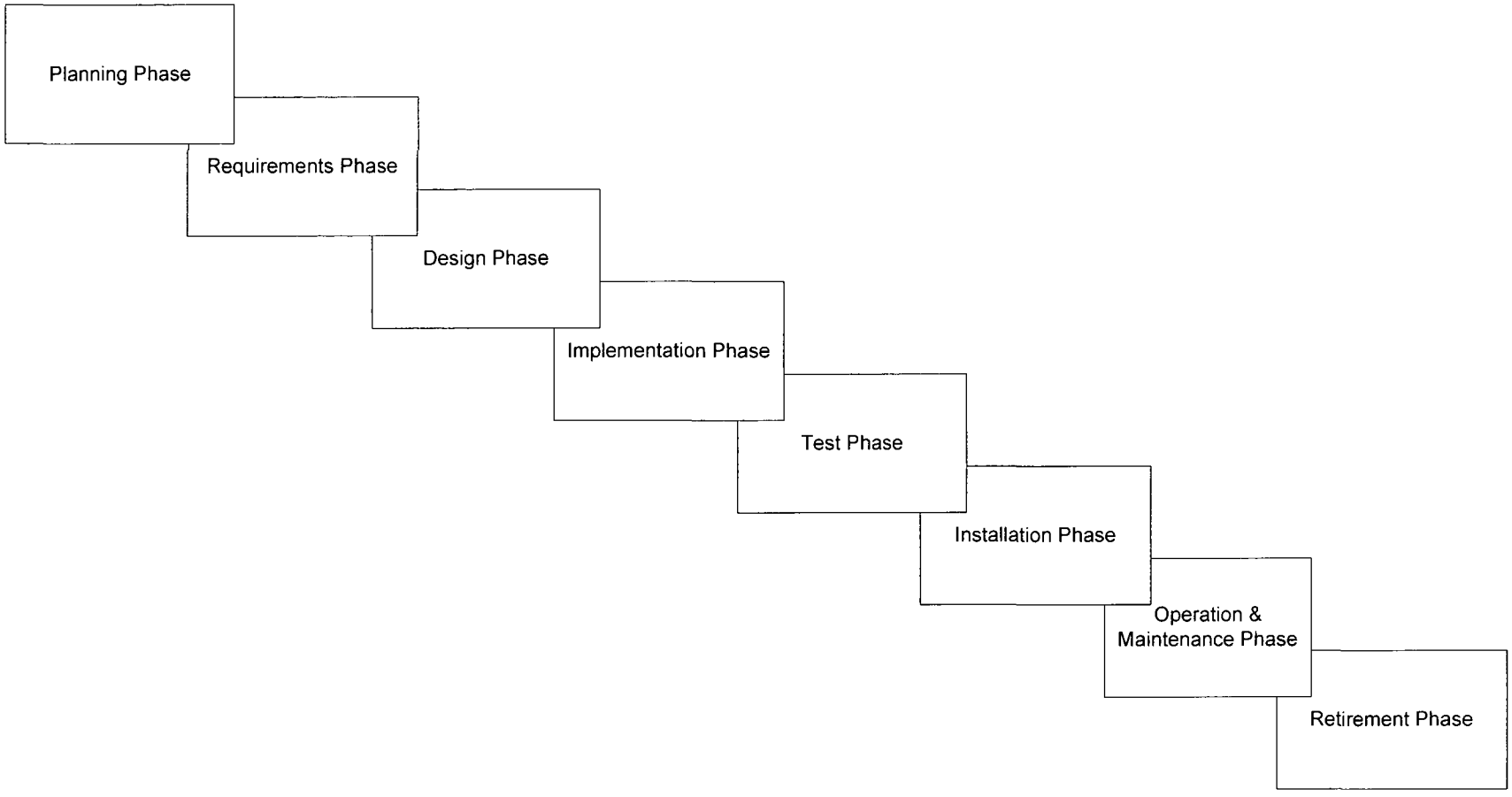


Figure 4.2.2-1. Software Life Cycle Process Overview

4.2.3 ESBWR I&C Software Integration Plan

4.2.3.5 Overview

The software integration plan describes the software functional test (SFT) to be conducted during the implementation phase.

4.2.3.5 Purpose

The purpose of this plan is to:

- Describe the organization and responsibilities of individuals or groups involved in the SFT activities.
- Describe SFT management, such as schedule, resources, security, risks and contingency planning, anomaly and problem reporting and training needs.
- Provide a structure for SFT.
- Provide the requirements and guidelines necessary to prepare, execute, and document SFTs.
- Define required SFT documentation and the test deliverables.
- Define measurements and metrics for error tracking and resolution, and to assess the success or failure of the software integration and test effort.

The approach to software integration and testing activities is carried out in a deliberate and methodical manner.

For testing activities, deviations from the test plan (e.g. FAT Plan) must be justified and approved in accordance with the software integration plan.

4.2.3.5 Scope

The system test boundaries are defined by the SFT plan. Variations in system boundaries as specified in the procurement package are included in the SFT plan.

Functional testing requiring inter-system communication, for instance, end-to-end validation testing involving functionality from more than one system, and validation of communication links crossing procurement package boundaries will be tested.

4.2.3.5 Method

1. Organization and Management

The software integration plan describes the organization and management functional responsibilities. [[

]]

The software integration plan details the functional responsibilities for management of the software testing activities including:

- Management and organizational interfaces.
- Scheduling and planning.
- Resources.
- Training.
- Reviews.

The software integration plan details the roles and responsibilities for individuals involved in the software testing activities including the following:

- The responsible technical project engineer (RTPE).
- Software functional test engineer i.e., responsible test engineer (RTE).
- Test personnel qualifications.

2. Procedures

The software testing includes functional testing, and validation testing of newly developed software, and modifications to any previously developed software. [[

]] The software integration plan specifies software test guidelines including sections describing the key elements required for performing the following test activities:

- Test preparation.
- Test design.
- Test execution.
- Test summary.

4.2.3.5 Implementation

The ESBWR software integration plan defines additional methods, tools, procedures, and metrics for the software integration plan activities. [[

]]

4.2.4 ESBWR I&C Software Installation Plan

4.2.4.5 Overview

The software installation plan (SIP) describes the software installation process and activities that are performed during the installation phase.

The SIP addresses software product only. The installation of programmed firmware into hardware is considered to be outside the scope of this plan.

4.2.4.5 Purpose

The purpose of the SIP is to:

- Define the installation phase activities.
- Describe installation procedures.
- Describe software installation management, such as (but not limited to) schedule, resources, security, risks and contingency planning, anomaly and problem reporting, and training needs.
- Provide the requirements and guidelines necessary to prepare, execute and document software installation.

4.2.4.5 Scope

The scope of the SIP is to address software installation strategy and techniques. The activities and procedures for the creation of documentation necessary for the licensee to install software in the systems are discussed.

4.2.4.5 Method

The SIP defines and establishes the procedural requirements for the following installation activities:

1. Software Installation Procedure

A software installation procedure is produced for each software package. A combined procedure may be produced for multiple packages within a single system, but each system or logical group of systems should have its own installation procedure.

2. Software Installation Reporting

A software installation report is produced for each software installation procedure. A combined report may be produced for multiple packages within a single system, but each system or logical group of systems should have its own installation report.

For site installation, the licensee produces and controls software installation reports as part of the licensee's change control, configuration management, and installation control processes.

3. Installation Configuration Tables

Where applicable, installation configuration tables are produced. The tables include all of the functional characteristics defined in the procedure section of the SIP to ensure that the software is correctly configured for the operating safety system.

For site installation, the licensee produces and controls installation configuration tables as part of the licensee's change control, configuration management, and installation control processes.

4. Operations and Maintenance Manuals

The software operation and maintenance manuals are produced for each system or logical group of systems. Software O&M manuals include installation details necessary for the end user to install the software on the system intended for use by the software product.

5. Training Manuals

The software system training manuals for each system or logical group of systems are produced. The software system training manuals are based on design documents and the O&M manuals and provide the basis for training the Licensee.

4.2.4.5 Implementation

The ESBWR software installation plan defines additional methods, tools, procedures, and metrics for the activities described in Section 4.2.4.4.

4.2.4.5 Results

The method used for installation documentation and problem reporting is described in installation reports. [[

]]

4.2.5 ESBWR I&C Software Operations and Maintenance Plan

4.2.5.5 Overview

The software operation and maintenance plan (SOMP) defines the software process and activities used to operate and maintain the software product during plant operation.

4.2.5.5 Purpose

The SOMP defines requirements, methods and considerations for developing the system O&M manual. This plan also addresses maintenance procedures and activities to enhance, modify, and maintain software once the software is installed in the plant.

4.2.5.5 Scope

The scope of the SOMP is to address the activities for software product for the operations and maintenance phase. The guidance for these activities is generally provided to the licensee through the operation and maintenance manual. Activities addressed by the SOMP are

consistent with guidance provided within the SMP. The software quality assurance requirements are addressed in the SQAP.

4.2.5.5 Method

1. Activities

The plans, procedures, processes, and activities for software corrections and for software enhancements in the O&M phase are the same as those used in the planning, requirements, design, implementation, test, and installation phases.

The SOMP defines and establishes the procedural requirements for the activities to be performed during the O&M phase of the software life cycle, including sections describing:

- Operation phase activities.
- Maintenance phase activities.
- Operation phase procedures.
- Maintenance phase procedures.

2. Methods and Tools

Methods and tools to perform software operation and maintenance are defined in the O&M manual for each software package/system, or logical group of systems. The O&M manual includes a description of the facilities required to maintain the delivered software. The O&M manual lists and describes the software, hardware and associated documentation required to maintain the delivered software. Maintenance tools are qualified to the level associated with the safety significance of the software.

4.2.5.5 Implementation

The ESBWR software operations and maintenance plan defines additional methods, tools, procedures, and metrics for the activities described in Section 4.2.5.4.

4.2.5.5 Results

The method used for documentation and problem reporting during the O&M phase is defined in respective system O&M manuals. The content that the O&M manual addresses is described in the SOMP.

4.2.6 ESBWR I&C Software Training Plan

4.2.6.5 Overview

This software training plan (STrngP) describes the software training activities to be carried out before and during the operation of software equipment produced for the plant. Software training is performed prior to delivery of the software (system start-up and post turnover) and during the O&M phase of the software life cycle. The STrngP addresses the management, implementation and resource characteristics as addressed in BTP-14 [2.2.1(2)].

4.2.6.5 Purpose

The purpose of the STrngP is to define:

- Requirements and methods to use while developing the training manual.
- Training needs of appropriate plant staff, including operators, I&C engineers and technicians.
- A general description of the training facilities.
- The organization supporting the training effort including interfaces and responsibilities.

4.2.6.5 Scope

The scope of the STrngP is to address the training requirements and documentation for each system or logical group of systems needed to ensure proper operation and use of the software within the overall system. These training requirements include (safe) proper usage (i.e, personal safety, system security) use of the equipment for the users, operators, maintenance personnel, and management personnel. This STrngP describes the approach for identifying training requirements for use in developing the related training documents.

4.2.6.5 Method

1. ESBWR Training Organization

The STrngP provides a description of the ESBWR training organization supporting the software product training effort as well as organizational interfaces and responsibilities of the training organization personnel.

2. Training Activities

The STrngP defines the training activities to be performed. Training activities include:

- Development and maintenance of training plans.
- Development and review of the training manual.
- Development of training courses.
- Development of Training.

Plant specific training procedures are plant specific training post development activities and are the responsibility of the licensee.

3. Software Training Manual Program

The software training manual is prepared in accordance with requirements specified in the STrngP. The training manual is completed and accepted by the licensee prior to the start of the training sessions.

4. Training Program

A comprehensive training program with a set of established training modules or programs is developed for the software products.

The specific training for system users as well as the general training requirements are defined in the STrngP including descriptions. Training is provided for the following generic types of system users:

- Plant operations.
- Maintenance.
- System administrator.
- General purpose user.
- Engineering.

4.2.6.5 Implementation

The ESBWR software training plan defines additional methods, tools, procedures, and metrics for the activities described in Section 4.2.6.4.

4.2.6.5 Results

Training metrics are measured, recorded, analyzed, and documented as defined in the software training plan.

4.2.7 ESBWR I&C Software Quality Assurance Plan

4.2.7.5 Overview

The SQAP describes the Software Quality Assurance (SQA) activities to be performed during the software life cycle phases of the ESBWR software class Q and software class N digital computer based I&C system; herein referred to as software product (software and firmware).

The SQAP meets the acceptance criteria specified in chapter 7 of NUREG 0800 [2.2.1(2)], with exceptions identified in the SQAP.

4.2.7.5 Purpose

The purpose of the SQAP is to:

- Establish a SQA program to monitor the software life cycle activities of the software products and to identify the organization responsible for the SQA program and its organizational boundaries.
- Supplement GE Nuclear Energy (GEEN) Quality Assurance Program, which is in full compliance with 10CFR 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plant and Fuel Processing Plants [2.1(1)].

The objectives of the SQA program are to ensure that:

1. The design teams follow:
   - The established GE Policies and Procedures (P&P).
   - The Engineering Operating Procedures (EOP).
   - The requirements described in the SQAP.

- The ESBWR I&C Software Management Plan (SMP).

2. The design documentation and design outputs for each software life cycle phase defined in the SMP are adequate (i.e., correct and complete)
3. The final software products are acceptable to be installed and ready for operation in a nuclear power plant.

4.2.7.5 Scope

The SQAP defines the SQA activities, methods, and tools by which to execute these activities. The SQAP also specifies the following:

- Required verification and validation (V&V) activities [Software V&V Plan (SVVP)].
- Software safety analysis (SSA) [(Software Safety Plan (SSP)].
- Software configuration management plan (SCMP).

The SQAP is applicable during all phases of the software life cycle.

The software products covered in the SQAP encompass all instrumentation and control systems that perform the monitoring, control, alarming and protection functions associated with all modes of ESBWR plant normal operation (i.e., startup, shutdown, standby, power operation, and refueling) as well as off-normal, emergency, and accident conditions.

Software products developed by vendors shall comply with NEDO-33245 SQAP or GE approved vendor plans.

Unless otherwise specified, the requirements specified in the SQAP are applicable for the Software Class Q, Software Class N3, and Software Class N2 software products.

4.2.7.5 Method

1. Organization

The functional responsibilities and authorities of the organizations within ESBWR Project who are responsible for the quality of the software products are defined. The organization of the ESBWR Project is shown in Figure 3.1.4-1.

The Quality organization is responsible for GEEN Quality Assurance (QA) program. The Quality organization is a managerially and financially independent organization. The Quality Manager, who reports to the President and CEO of GEEN, provides leadership for developing and overall coordination of the QA program objectives, including the software quality assurance program. The SQA organization has the overall responsibility for developing and maintaining the SQA program with support from the Software Project Engineering (SPE) organization. The SPE organization is responsible for the executing the technical aspect of software quality assurance program, which includes the following software quality assurance tasks:

- Independent verification and validation (IV&V) of software Class Q software.
- Software safety analysis.
- SCM.

The Software Project Engineering (SPE) organization is technically, managerially and financially independent from the software products design organization, in conformance with RG 1.168 [2.2.3(3)].

2. Activities

The following activities are performed throughout the software life cycle phases:

- Verification and validation of design documentation and outputs specified in the SMP.
- Software safety analysis of Software Class Q software and Software Class N3 software requirements.
- Software and system testing.
- Baseline review process.
- Software configuration management.
- Software audit.

The SQAP outlines the tasks and the individual or group responsible for conducting these tasks during the design and development of the software products.

3. Qualification and Responsibilities

The SQA Manager must be knowledgeable in the industry standard QA methodologies, proficient in establishing, maintaining, and improving QA Procedures, and experienced in technical project management.

The SPE members must be knowledgeable in the technologies and methods used in design development and are qualified to perform the specific software quality assurance tasks. [[

]]

Level of software quality assurance support varies during each software life cycle phase; thus, the membership to the SPE unit fluctuates with the level of needs. If necessary, the SPE and SQA Manager have the authority to contract third party organizations (i.e., consultants or experts in I&C software design and development for nuclear power plant) to support the software quality assurance activities.

Organizational interfaces and individual roles and responsibilities for the execution of the SQA program are defined in the SQAP including:

- Quality manager.
- Software quality assurance manager.
- NPP quality manager.
- I&C/Electrical engineering manager.
- Software project engineering.
- SPE manager.
- Independent verification & validation team.

- Baseline review team.
- Software safety team.
- Configuration management manager.
- Design team.

4. Scheduling and Planning

The SPE and SQA managers have the overall responsibility for scheduling and planning the tasks and activities described in the SQAP. The task lead for each team (SST, IVVT, BRT) is responsible for the management and planning activities for their respective teams. The task leads coordinate with the design teams concerning the timely receipt of design documentation to support the required tasks (SSA, IV&V, baseline review, and software audit). [[

]]

As the Quality tasks are performed by a cross-functional team, a project workflow is established to ensure the required tasks are accurately identified, and the quality task schedule is aligned with the established integrated project schedule.

The schedule includes:

- The duration of the SQAP.
- The major milestones of the project related to the quality tasks.
- The sequence and dependencies of the quality tasks and the relationship of key quality tasks to project milestones.
- The absolute dates of schedule events.

5. Approval Authority

The NPP Quality manager, the SQA manager, and the SPE manager have approval or rejection authority for functions under his/her responsibilities.

Upon the rejection of a software product or the issuance of a stop work order, corrective actions are established, which may include a correction or amendment of the design process, revision to the software plans, re-design, re-implementation, or re-testing of the software product. The design team is required to complete the corrective actions and identify preventive actions to avert the occurrence of similar defects.

6. Tools, techniques, and methodologies

Tools, techniques, and methodologies to execute the activities in the SQAP are described in the SQAP [2.3.1(14), Section 12] and include:

- Commitment tracking system.
- Checklist.
- Requirements traceability matrix.
- Product data management system (PDMS).

- Design record file (DRF).
- Discrepancy tracking system.

7. Vendor and Acquired Software Control.

Procedures for control of vendor selection and qualification and vendor software control are established in the SQAP [2.3.1(14), Section 14].

8. Records Collection, Maintenance, and Retention

The collection, maintenance and retention of design documentation, design outputs and quality records, such as audit reports, SSA reports, and test reports is described in the SQAP [2.1.3(14), Section 10.8].

9. Training

Training requirements for the personnel supporting quality tasks is established in the SQAP [2.3.1(14), Section 16].

10. Risk Management

The process for risk management for the quality program is addressed in the SQAP [2.3.1(14), Section 17].

11. SQAP Maintenance

The responsibilities and procedures for the maintenance of the SQAP are outlined in the SQAP [2.3.1(14), Section 18].

12. Metrics

Software Metrics are sets of data that are systematically collected and analyzed in order to provide software quality process feedback to the software development processes. This feedback mechanism provides a means by which the software development processes can change over time to facilitate continuous process improvement with the primary objective of producing high quality defect free software products. Specific metrics will be defined for each software platform or product line and for each software classification.

The metrics program shall focus on the software functional and process characteristics listed in Appendix D. These characteristics will be used to derive a core set of metrics relating to the development process and the design documentation and outputs, such as requirements and design documents, code, and test documentation.

The SPE will be responsible for collecting and analyzing metric data for the software Class Q and N3 software products.

4.2.7.5 Implementation

The ESBWR software quality assurance plan defines additional methods, standards, practices, conventions, and metrics for the activities described in Section 4.2.7.4.

4.2.7.5 Results

1. Technical Review

Technical reviews are performed to ensure the software product being designed and developed meet its intended use and identifies discrepancies from required design inputs, and codes and standards. Technical reviews may also provide recommendations of alternatives and examination of various alternatives.

2. Managerial Review

[[

]]. The review team assesses opportunities for improvement and the need for changes to the SQA program and quality objectives. [[

]] The review is documented in the managerial review report, which includes decisions and actions needed to assure continued effectiveness of the SQA program.

3. Project Closeout Review

The responsible project manager schedules a post-delivery closeout review to formally terminate the activities of a project, such as closing any CARs associated with the project and project design record file (DRF), setting up warranty administration and review, and conducting a licensee closeout meeting to solicit feedback, which includes collecting lessons learned and metrics during the project. [[

]]

4. Functional Audit

Functional audits are conducted to assure that the requirements specified in the system design specification (SDS) and SRS have been met by checking the applicable requirements traceability matrix (RTM). The functional audit is performed during baseline review and is documented in the baseline review record. The functional audit is performed for the software class Q software products and recommended for software class N3 and N2 software products.

5. Physical Audit

The physical audit is conducted to verify that the appropriate CI items, which include software build description or software installation procedure, accurately and completely describe the "build" parameters of the software such that a duplicate version of the object code can be recreated. The physical audit is performed as part of test baseline review and is documented in the test baseline review record. The physical audit is performed for software class Q software products and recommended for software class N3 and N2 software products.

6. In-Process Audits

The SQAP requires SQA audits to be performed on the design organizations (both internal and external) working on the ESBWR project. The SQA audit is performed (by the SQA) to ensure compliance with the codes and standards specified in this SQAP. The SQA audit evaluates the adequacy and completeness of the required reviews and V&V activities. [[ ]]

An audit report is prepared at the conclusion of each software audit. The audit report summarizes the audit activities and results, observations, conditions adverse to quality (CAQs), discrepancies, non-compliances to the required quality and engineering procedures, and recommended corrective actions. A CAR is initiated to manage the identified CAQs, discrepancies, and non-compliances in accordance with the procedures specified in the SQAP.

4.2.8 ESBWR I&C Software Verification & Validation Plan

4.2.8.5 Overview

The SVVP establishes the V&V tasks for the software designed and developed for software products. The SVVP satisfies the requirements of RG 1.168 [2.2.3(3)]. RG 1.168 endorses IEEE Std. 1012, [2.2.4(6)] and IEEE Std. 1028, [2.2.4(7)].

4.2.8.5 Purpose

The purpose of this plan is to outline the specific V&V steps required during the software development process to ensure that:

- Developed software meets its specified requirements, performs its intended functions correctly, and does not perform any unintended function.
- The final software product meets the contract requirements, required international, national, industry and regulatory standards, and licensing commitments.
- The final software product is correct, complete, accurate, meets traceability of requirements and design specified in the design documents and outputs.

Software V&V activities are integrated throughout the software life cycle to facilitate the timely detection of errors and to ensure the quality of the software product.

4.2.8.5 Scope

The SVVP outlines the formal set of standards and procedures necessary to comprehensively verify software class Q and software class N3 and N2 software products during all phases of the software life cycle. The software life cycle phases in the SVVP correspond with those defined in the SMP [2.3.1(13)].

The scope of V&V tasks addresses the software V&V activities and includes the activities to analyze and test the software with respect to its hardware interfaces and user interactions. V&V activity is limited to software prepared by GEEN and GEEN vendors for the project.

4.2.8.5 Method

1. Verification and Validation Overview

The management and organization of the software V&V activities are described in the SQAP [[

2. V&V Tools

Tools used to support the V&V tasks are evaluated. The evaluation results are documented in the tool evaluation report. [[

3. Verification

Verification is performed to determine whether or not the design document/output for a given software life cycle phase fulfill (i.e., is traceable) the requirements [[

]]

4. Code Review

Code reviews are performed to verify that the software correctly implements the specified design [[

]]

5. Software Functional Test

The software functional test includes the software module/unit test and the software integration test. [[

]]

6. Software Validation Test

The software validation test is performed to validate that the software product is operational and conforms to the functional and performance requirements [[

]]

7. Baseline Reviews

Baseline reviews are formal, independent evaluations of the software design and development activities performed at the completion of software life cycle phases. [[

]]

8. Requirements Traceability Analysis

Requirements traceability analysis (RTA) is performed for software class Q, N3 and N2 software requirements. [[

]]

9. Audit Support

In Process audits are described in the SQAP {2.3.1(14)}.

[[

]]

10. Walk-Through

Design walk-through is a static analysis technique used during the design and development of the software product [[

]]

4.2.8.5 Implementation

The ESBWR Software Verification & Validation Plan describes the inputs, tasks, and outputs for the V&V activities and tasks to be performed for life cycle phases. [[

]]

4.2.8.5 Results

[[

]]

4.2.9 ESBWR I&C Software Safety Plan

4.2.9.5 Overview

Safety is the most important consideration, taking precedence over budget and schedule. The SSP meets the guidelines specified in NUREG-0800, Chapter 7, BTP HICB-14 [2.2.1(2)], and the requirements outlined in IEEE Std. 1228, Section 4.4 [2.4(13)].

4.2.9.5 Purpose

The SSP establishes the processes and activities intended to ensure that the safety concerns of the software products are properly considered during the software development and are consistent with the defined system safety analyses as defined by RG 1.173, [2.2.3(8)].

4.2.9.5 Scope

SSA is performed on the software for software class Q and N3 and software products.

[[

9. Training

The software training plan is described in Section 9.0 of the SMP.

10. Installation

Installation is described in Section 7.0 of the SMP. Installation V&V tasks and the SAT are described in the SQAP.

11. Startup and Transition

Prior to starting up the newly installed software product, pre-operational tests are conducted to demonstrate the installed software product operates as intended, and if applicable, the required setpoints (e.g., trip and alarm) are established. The pre-operational test is conducted in accordance with an approved (by the licensee) test plan and procedure. The pre-operational test is usually the licensee's responsibility and is supported by qualified engineers who are knowledgeable in the installed software product and plant operation.

The startup procedure addresses the requirements for safely starting the new system, and if an old system is to be replaced, for making a safe transition from the old system to the new system. At a minimum, the following are addressed:

- Fallback modes for the new system.
- Startup of backup components and subsystems.
- Startup of the new system.
- Parallel operation with backups.
- Parallel operation of the old system and the new system.
- Subsystem vs. full system operation.
- Switchover to full system operation.
- Validation of results from the new system.
- Cross validation of results between the old system and the new system.

- Fallback in the case of failure of the new system, including fallback to an old system if one exists.

12. Operations support

The Software O&M manual and user interface specification provide for the safety-critical software. The software O&M manual and user interface specification are described in the SMP.

13. Monitoring

The licensee is responsible for monitoring the operation of the safety-critical software within the software product. Safety concerns that are detected during operation are documented and reported in accordance with the plant's problem reporting procedures.

[[

]]

14. Maintenance

Software maintenance is specified in the software O&M manual. The software O&M manual is described in the SMP.

15. Retirement and Notification

Retirement and notification are described in the SMP.

4.2.9.5 Implementation

The ESBWR software safety plan defines additional methods, tools, procedures, and metrics for the activities described in Section 4.2.9.4.

4.2.9.5 Results

A software safety analysis report documents the results of the SSP activities. As a minimum, the software safety analysis report shall include the following:

- Name and description of the software evaluated.
- System.
- Software classification.
- Purpose and scope.
- Reference inputs.
- Software safety analysis body of report.
- Anomalies noted.
- Conclusion.
- Responsible engineer.
- Approving authority.

[[

]]

4.2.10 ESBWR I&C Software Configuration Management Plan

4.2.10.5 Overview

The software configuration management plan (SCMP) establishes the SCM activities for software designed and developed for the software products. The SCMP satisfies the requirements of RG 1.169, [2.2.3(4)] that endorses IEEE Std. 828, [2.2.4(2)].

4.2.10.5 Purpose

The intent of the SCMP is to provide additional guidance and direction necessary to implement the SCM activities required during the software product design and development process. The SCMP supplements GEEN established configuration management procedures in system and hardware design. It establishes a formal set of standards and methodology used to administer and control the configurations of Software Class Q, and Software Class N3 and N2 software products and remains in effect throughout the software life cycle phase.

4.2.10.5 Scope

The scope of SCMP includes the following:

- SCM management.
- SCM activities.
- SCM schedule.
- SCM resources.

4.2.10.5 Method

1. SCM Management

The elements of the SCM management are described in the SCMP including:

- Organization.
- SCM responsibilities.
- Applicable policies, procedures, and directives.
- SCM schedule.
- SCM resources.

2. SCM Tasks

Descriptions of the processes and procedures are described for the SCM tasks including:

- Configuration identification.
- Configuration control including:
  - Design control.
  - Design change control.
  - Change requests and notification control.

  - Design interfaces control.
- Configuration status accounting.
- Configuration audits including:
  - Functional configuration audits.
  - Physical configuration audits.
- Baseline reviews.
  - Baseline item approval process
  - Baseline review record

4.2.10.5 Implementation

The ESBWR Software Management Plan defines additional methods, tools, procedures, and metrics for the activities described in Section 4.2.10.4.

- Software release procedures.
- Software product release.
- Vendor software and acquired software controls.
- Record collection and retention.

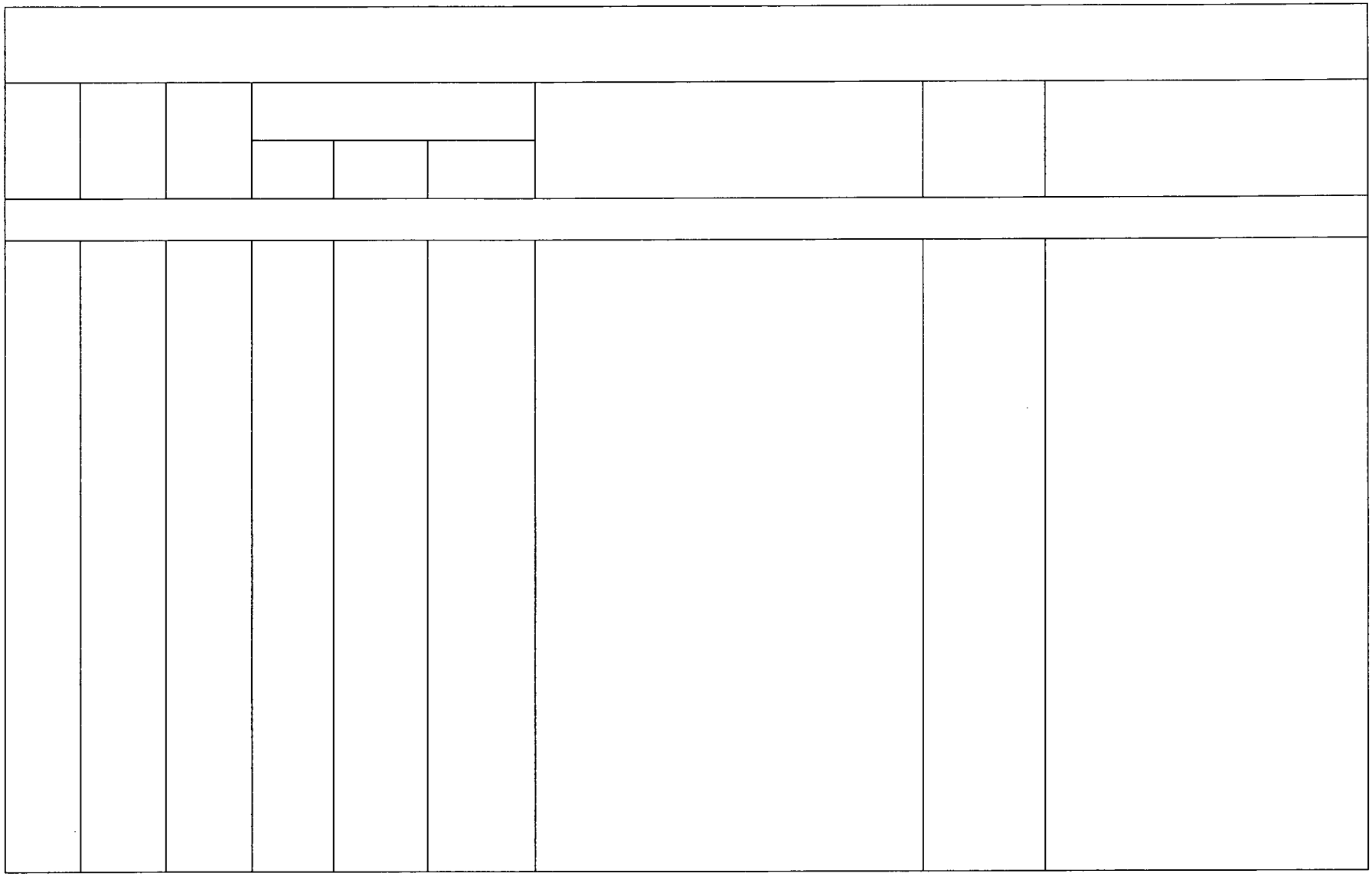
4.2.10.5 Results

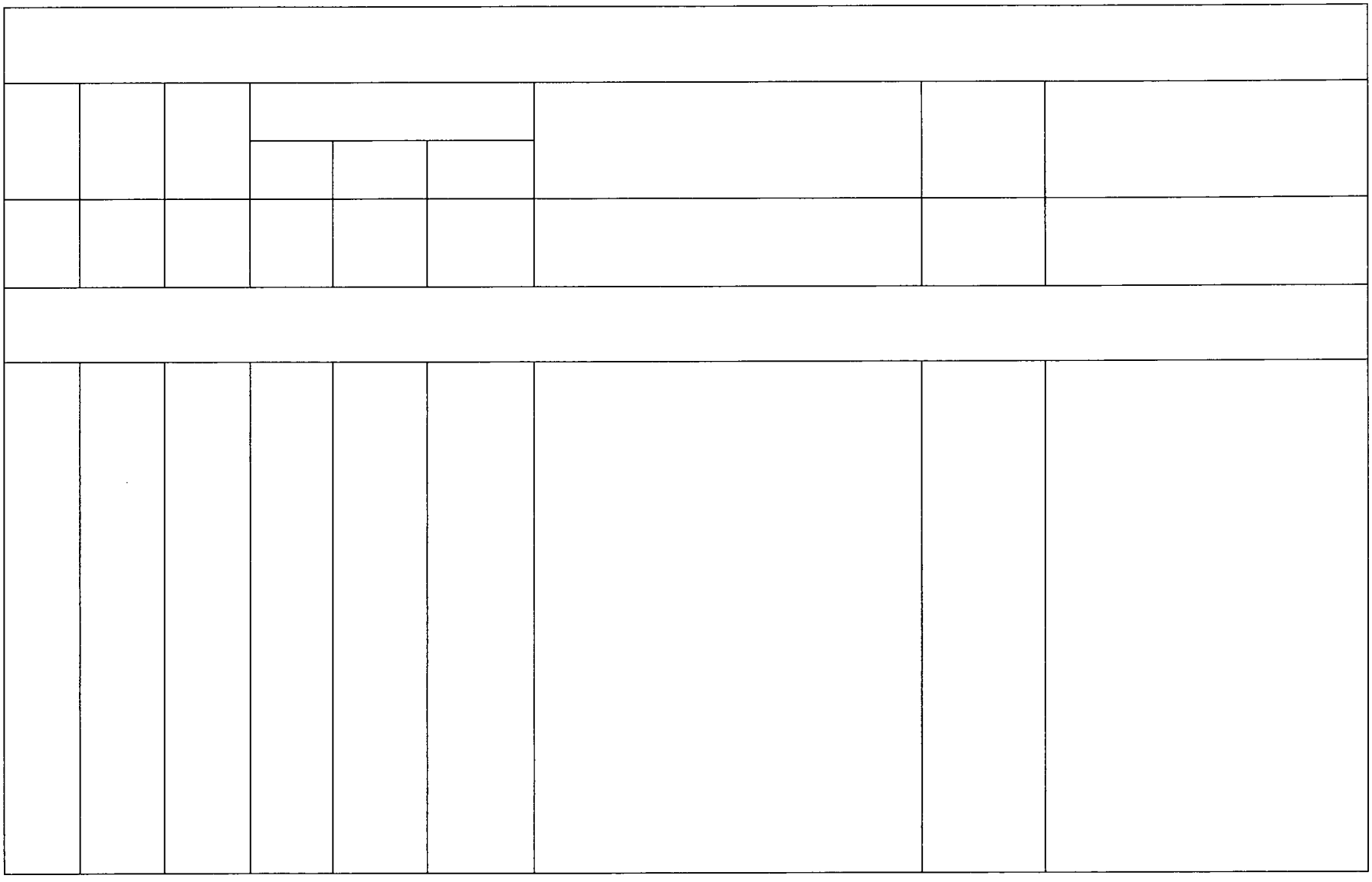
The results and outputs of the SCM activities are provided within the sections of the SCMP described in Section 4.2.10.4.

[[

[[

	]]





								]]