



**GE Energy
Nuclear**

**NEDO-33226
Class I
eDRF# 0000-0046-8503
October 2005**

LICENSING TOPICAL REPORT

ESBWR I&C SOFTWARE MANAGEMENT PLAN (DRAFT)

(Conditional Release – pending closure of design verifications)

Copyright 2005 General Electric Company

**Prepared for:
ESBWR Certification & Implementation**

NON PROPRIETARY INFORMATION NOTICE

This is a non proprietary version of the document NEDE-33226P, which has the proprietary information removed. Portions of the document that have been removed are indicated by an open and closed bracket as shown here [[]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT PLEASE READ CAREFULLY

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

Table of Contents

1	Introduction.....	1
	1.1 Purpose and Scope	1
	1.2 Software Developed by Vendors	2
2	Organization and Responsibilities.....	2
	2.1 I&C Organizational Units	2
	2.2 I&C Organizational Resources	3
	2.3 Organizational Responsibilities	4
3	Definitions, Acronyms and Abbreviations.....	6
4	Applicable Documents	10
	4.1 Supporting and Supplemental Documents.....	10
	4.1.1 Supporting Documents	10
	4.1.2 Supplemental Documents	11
	4.2 Codes and Standards	12
	4.2.1 American Society of Mechanical Engineers (ASME) Codes.....	12
	4.2.2 Institute of Electrical and Electronic Engineers (IEEE) Standards	12
	4.2.3 International Standards	12
	4.2.4 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides (Reg Guide).....	12
	4.2.5 NUREG	13
5	Software Engineering Process	13
	5.1 Planning	14
	5.1.1 Equipment Design Requirements - SDDs, LDs and P&IDs and IO/FX/Setpoint Database	16
	5.1.2 Management Plans.....	16
	5.1.2.1 Software Management Plan.....	16
	5.1.2.2 Project Plan.....	16
	5.1.2.3 Software Configuration Management Plan.....	17
	5.1.2.4 Verification and Validation Plan.....	17
	5.1.2.5 Software Safety Plan.....	17
	5.1.3 Planning Baseline Review Record	18
	5.2 Design Definition.....	19
	5.2.1 Hardware/Software Specification.....	22
	5.2.2 Software Requirements Specification (SRS)	23
	5.2.3 System Block Diagram	24
	5.2.4 Instrument Performance Specification (with Software Requirements)	25

5.2.5 Sub-System Schematic.....	27
5.2.6 Data Communications Protocol.....	27
5.2.6.1 External Data Communications Protocol Specification(s).....	27
5.2.7 Software Test Plan	27
5.2.8 User's Manual	28
5.2.9 Support Software and Tools	29
5.2.10 Third Party Software.....	30
5.2.11 Adaptation of Previously Developed Software.....	31
5.2.12 Safety Analysis of Design Definition	32
5.2.13 Design Definition Baseline Review Record.....	33
5.2.14 Safety Analysis of Concept Definition.....	33
5.3 Software Design.....	33
5.3.1 Software Design Specification.....	35
5.3.2 Internal Data Communication Protocol Specification	35
5.3.3 Validation Test Procedures and Test Cases Specification	36
5.3.4 Software Conventions and Guidelines Document.....	36
5.3.5 Safety Analysis of Software Design	37
5.3.6 Software Design Baseline Review Record.....	37
5.4 Software Coding	37
5.4.1 Coding	39
5.4.1.1 Software Source Code	39
5.4.1.2 Code Reviews	40
5.4.2 Software Module Testing	40
5.4.2.1 Module Test Reports	41
5.4.3 Safety Analysis of Software Coding	42
5.4.4 Software Coding Baseline Review Record.....	42
5.5 Integration Test	42
5.5.1 Integration Testing.....	44
5.5.2 Integration and Installation Test Report.....	44
5.5.3 Safety Analysis of Integration Test	45
5.5.4 Integration Test Baseline Review Record.....	46
5.6 Validation Test.....	46
5.6.1 Validation Testing.....	47
5.6.2 Validation Test Report	47
5.6.3 Safety Analysis of Validation Test.....	47
5.6.4 Validation Test Baseline Review Record	48
5.7 Change Control	48
5.7.1 Change Control Objective and Scope	49

Appendices

Appendix A: Document Formats.....	55
A.1 Hardware/Software Specification (HSS)	55
A.2 Software Requirements Specification (SRS)	56
A.3 Instrument Performance Specification (IPS)	57
Appendix B: Requirement Standards.....	60

List of Tables

Table 1 Planning Phase Output Documents.....	15
Table 2 Design Definition Phase Output Documents.....	21
Table 3 Software Design Phase Output Documents.....	34
Table 4 Software Coding Phase Output Documents.....	39
Table 5 Integration Test Phase Output Documents	43
Table 6 Validation Test Phase Output Documents	47
Table 7 Change Control Phase Output Documents	49

List of Figures

Figure 1 I&C Software Life Cycle Phases vs. ESBWR SRP Software Life Cycle Phases.....	51
Figure 2 I&C Software Life Cycle Phases and Hierarchy of Documentation Development.	52
Figure 2 I&C Software Life Cycle Phases and Hierarchy of Documentation Development (Continued)	53
Figure 3 Verification and Validation Process.....	54

1 Introduction

This Software Management Plan (SMP) provides the technical and administrative direction necessary to implement the design activities as outlined in the supporting documentation listed in Section 4.1.1 of this plan. This document also establishes the design and quality standards for the software-based products produced for the ESBWR Instrumentation and Control Systems (I&C¹).

The software-based products covered in this plan encompass all instrumentation and control systems which perform the monitoring, control 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 as defined in Overall Requirements section (Section 3) of the M-MIS and HFE Design Implementation Plan [4.1.1(2)]². [[

]]

1.1 Purpose and Scope

This plan (SMP) outlines the approach to be followed during the software engineering process (planning, design definition, software design, software coding, integration testing, validation testing and change control) for Quality Class S and Quality Class N-R I&C software-based products. A commercially accepted software engineering process shall be used for Quality Class N-G software-based products. [[

¹ The functions are the same as for M-MIS as defined in the Overall Requirements section (Section 3) of the M-MIS Design and HFE Implementation Plan.

² Section numbers referenced in this manner refer to the codes and standards documents listed in the Applicable Documents section (Section 4) of this SMP.

]]

[[

]]

1.2 Software Developed by Vendors

[[

]]

2 Organization and Responsibilities

2.1 I&C Organizational Units

The I&C organization is part of the ESBWR Engineering organization which includes other engineering disciplines and project configuration management, and other support units. The ESBWR Engineering group interfaces with GEEN's Quality organization. The I&C organization also interfaces with the related "Project Quality Unit(s)" under the GEEN Quality organization. The I&C Organization typically includes: I&C System Design unit, I&C Product

Application unit, Data Communication and Human Factor Engineering (HFE) unit, Software Safety and Licensing unit, and Software Quality Unit. The lead of each unit reports to the manager of the I&C Organization.

I&C System Design: responsible for I&C system design and requirements; *Data Communication and Human Factor Engineering (HFE)*: responsible for HFE design, plant data communication system design, specific control software design, and simulator design;

I&C Product Application Unit: responsible for detailed software and hardware design and implementation, and communication interface design; this unit has interfaces with I&C System Design Unit, with Data Communication and HFE Unit, with Software Safety and Licensing Unit, and Software Quality Unit. It also interface with the Project Quality Unit under GEEN Quality Organization on Software QA program development and implementation.

Software Safety and Licensing: responsible for software safety analysis and licensing, and the supervision of the implementation of software development according to software design process plans; this unit has interface with the I&C Product Application Unit and with the Software Quality unit. It also has interface with Project Quality Unit under GEEN Quality Organization.

Software Quality: responsible for development of software life cycle process plans and software QA program. It has interfaces with I&C Product Application Unit and Software Safety Unit. Software Quality personnel does not report to the lead of the I&C Product Application Unit.

The software design verification and validation personnel will be independent from the software designers of the I&C Product Application Unit personnel.

Specific responsibilities of the key personnel are described in Section 2.3, Organization Responsibilities. Interfaces with subcontractors and suppliers are described in the specific responsibilities of Section 2.3.

Detailed I&C and ESBWR project and engineering organization structure and organization chart are included in the staffing plan.

2.2 I&C Organizational Resources

[[

]]

2.3 Organizational Responsibilities

The primary duties of the organization covered by the SMP, and of individuals within the organization are defined below. The Manager/Technical Leads of Control / Electrical Systems and ESBWR Configuration Management are defined within SDP [4.1.2(7)] under Project Responsibilities.

- | | |
|----------------------------|---|
| Engineering Manager | - The person who is responsible for directing the engineering activities of the ESBWR Project and is the final authority for software based product release. This person is also responsible for the communication with the customer throughout the software engineering process on all matters requiring customer review and/or approval. |
|----------------------------|---|

Responsible Engineering Technical Lead	- A person with the overall responsibility for a set of I&C software-based products. Each I&C software-based product is assigned a RETL, including those developed by vendors. RETL interfaces and supervises vendor's product.
Responsible Technical Project Engineer	- The person with overall technical responsibility for ensuring that the hardware and software design of a software-based product meet the specified requirements.
Responsible Engineer	- The person responsible for a given technical item (e.g., the design and development of the documentation).
Responsible Configuration Control Engineer	- The person assigned responsibility for the configuration management of the I&C software-based products {see SCMP [4.1.2(1)]}.
Responsible Software Safety Engineer	- The person with overall responsibility for ensuring the safety qualities of all the software being developed for I&C, including the integration of the software with the final hardware platform {see SSP [4.1.2(5)]}.
Responsible Verifier(s)	- The Responsible Verifier(s) is an individual who meets the independence as described in GEEN EOP 42-6.00 [4.1.2(3b)] for verifications or EOP 42-6.10 for deferred verifications of design process and the accompanying documents.
Baseline Review Team	- The team responsible for judging adherence to the process for the documentation being baselined. The members of this team are appointed by the BRT Lead; they must be independent from the designers responsible for the documentation {see SCMP [4.1.2(1)]}.
Baseline Review Team Lead	- The person responsible for organizing the baseline review process. This person is appointed by the Manager/Technical Lead, Control/Electrical Systems {see SCMP [4.1.2(1)]}.

3 Definitions, Acronyms and Abbreviations

Acronyms and Abbreviations:

BRT	Baseline Review Team
CI	Configuration Item
DCIS	Distributed Control & Information Systems
DRF	Design Record File
ECN	Engineering Change Notice
EMI	Electromagnetic Interference
EOP	Engineering Operating Procedure
GE	General Electric Company
GEEN	GE Energy Nuclear (Previously GENE)
HFE	Human Factors Engineering
HSI	Human System Interface
HSS	Hardware/Software Specification
I/A	Intelligent Automation
I/O	Input/Output
IP	Installation Plan
IPS	Instrument Performance Specification
LD	Logic Diagram
M-MIS	Man-Machine Interface System
MCR	Main Control Room
N/A	Not Applicable
O&MP	Operation & Maintenance Plan (Change Control)
P&ID	Piping and Instrumentation Diagram

PDM	Project Design Manual
PP	Project Plan
PMM	Project Management Manual
PPM	Project Procurement Manual
RCCE	Responsible Configuration Control Engineer
RE	Responsible Engineer
Reg Guide	Regulatory Guide
RETL	Responsible Engineering Technical Lead
RSSE	Responsible Software Safety Engineer
RTPE	Responsible Technical Project Engineer
SBD	System Block Diagram
SCMP	Software Configuration Management Plan
SDD	System Design Description
SDS	Software Design Specification
SMP	Software Management Plan
SRP	Standard Review Plan
SRS	Software Requirements Specification
SSA	Software Safety Analysis
SSP	Software Safety Plan
STP	Software Test Plan
VVP	Verification and Validation Plan
Utility	Utility
US NRC	United States Nuclear Regulatory Commission
V&V	Verification and Validation

The following definitions apply throughout this document:

Algorithm - A finite set of well-defined rules for the solution of a problem in a finite number of steps.

Baseline - A items that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures.

Baseline Review and Oversight - A formal review, conducted at the end of each software life cycle phase, and requested by the Responsible Technical Project Engineer (RTPE). The baseline review process is under the control of the Baseline Review Team. The Baseline Review Team (appointed by the I&C Discipline Engineer) performs the review. These reviews are intended to confirm adherence to the SMP (this plan), SCMP [4.1.2(1)] and VVP [4.1.2(2)]. All Baseline Reviews are performed and documented in accordance with the Software Configuration Management Plan (SCMP).

Oversight including performance indicators is also performed during each software life cycle phase, RTPE is informed shortly after findings and observations are confirmed and BRT Lead issues an Oversight Report to the RTPE and all direct and indirect project management having a need to know shortly after the end of each software life cycle phase.

Baseline Review Team - See Section 2.3

Baseline Review Team Lead - See Section 2.3

Black-box Testing - A system/software test methodology that is derived from external specifications and requirements of the system. Methods for black-box testing include random testing and testing at boundary values. It verifies the end results at the system level, but does not check the implementation techniques, nor does it assume that all statements in the program are executed.

Code Review (Code Analysis) - Software source code presented to project personnel for comment or approval.

- | | |
|--------------------------------------|--|
| Configuration Item | - An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process. |
| Design Record File | - Design Record File [4.1.2.(3c)] is the formal controlled information record for in-progress and completed engineering work which is retained and from which information can be retrieved. |
| Design Reviews | - Formal, design adequacy evaluations which are performed by knowledgeable persons other than those directly responsible and accountable for the design in accordance with GEEN EOP 40-7.00 [4.1.2(3a)]. Design reviews are used to verify that product designs meet functional, contractual, safety, regulatory, industry codes and standards, and company requirements. |
| Embedded System | - A computer system that is part of a larger system and performs some of the requirements of that system. |
| Internal Verification and Validation | - The V&V activities performed by the responsible design organization in accordance with GEEN EOPs 40-7.00 (Design Reviews) [4.1.2(3a)] or 42-6.00 (Independent Design Verification) [4.1.2(3b)] or equivalent to ensure the quality of the design process and the associated documents produced. These V&V activities are referred to herein as the <i>Internal V&V</i> . |
| Instrument | - A hardware device used for analytical or control functions and usually containing an embedded microprocessor(s). |
| Quality Class N-G | - ESBWR Project General Grade classification {see ESBWR Project Quality Assurance Plan [4.1.1(4)]}. |
| Quality Class N-R | - ESBWR Project Reliability-Critical classification {see ESBWR Project Quality Assurance Plan [4.1.1(4)]}. |
| Quality Class S | - ESBWR Project Safety related classification {see ESBWR Project Quality Assurance Plan [4.1.1(4)]}. |
| Software Life Cycle | - The period of time that begins when a software product is conceived and ends when the software is no longer available for use (see Section 5). |

Software Module	- The smallest segment of code known and controlled by the operating system (also called routine, procedure, function or subprogram).
Software Package	- A collection of software modules (e.g., subroutines, main control tasks) brought together to form a single software product.
Software Source Code	- Computer instructions and data definitions expressed in a form suitable for input to an assembler, compiler, or other translator.
Software Unit	- See Software Module.
Software-based System	- A computer system composed of specified programs that are run on commercially available hardware and/or operating systems.
Traceability Matrix	- A matrix that records the relationship between two or more product specifications (i.e., design documentation) of the development process (e.g., a matrix that records the relationship between the requirements and the design of a given software component).
Validation	- The testing process that ensures the software-based product meets its intended use and is compliant with system functional, performance and interface requirements.
Verification	- See Internal Verification and Validation
White-box Testing	- A software test methodology at the software module level in which test cases are derived from the internal structure of the program. It shall execute all the statements or branches in the program to check on how the system is implemented. Some methods of white-box testing are statement coverage, branch coverage and path coverage.

4 Applicable Documents

4.1 Supporting and Supplemental Documents

4.1.1 Supporting Documents

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

Document Title	Document Number
1. Project Design Manual	
2. Man-Machine Interface System and Human Factors Engineering Implementation Plan	NEDE-33217
3. Man-Machine Interface System Review Implementation Plan	NEDE-33218
4. Quality Assurance Plan	NEDC-33181
5. Project Procurement Manual	
6. Project Management Manual	NEDC-33216

4.1.2 Supplemental Documents

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

Document Title	Document Number
1. Software Configuration Management Plan	NEDE-33227
2. Verification and Validation Plan	NEDE-33228
3. GEEN Engineering Operation Procedures	NEDE-21109
a. 40-7.00 Design Review	
b. 42-6.00 Independent Design Verification	
c. 42-10.00 Design Record File	
d. 55-2.00 Engineering Change Control	
e. 40-3.00 Engineering Computer Programs	
f. 55-3.00 Field Deviation Disposition Request	
g. 45-2.00 Procurement of Engineering Services	
h. 25-5.00 Work Planning and Scheduling	
4. Software Safety Plan	NEDE-33230

Document Title	Document Number
5. Software Quality Assurance Plan	
6. Standard Review Plan (SRP), Chapter 7, Appendix 7-A, Branch Technical Position HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems	
7. Software Development Plan	NEDE-33229
8. Software Conventions and Guidelines	

4.2 Codes and Standards

The following codes and standards are applicable to the ESBWR I&C Software Management Plan to the extent specified herein. The applicable date/revision of the code or standard is specified in the ESBWR Certification Tier 2, Tables 1.9-n.

4.2.1 American Society of Mechanical Engineers (ASME) Codes

1. ASME NQA-1

4.2.2 Institute of Electrical and Electronic Engineers (IEEE) Standards

1. IEEE 1058.1, Software Project Management Plans
2. IEEE 1228, Software Safety Plans
3. IEEE 829, Standard for Software Test Documentation
4. IEEE 7-4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.

4.2.3 International Standards

1. ISO-9000-3, Quality management and quality assurance standards - Guidelines for the application of ISO 9001 to the development, supply and maintenance of software

4.2.4 U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides (Reg Guide)

1. Reg. Guide 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants
2. Reg. Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

3. Reg. Guide 1.170, Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants
4. Reg. Guide 1.171, Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants
5. Reg. Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

4.2.5 NUREG

1. NUREG/CR-6101-1993, Software Reliability and Safety in Nuclear Reactor Protection Systems

5 Software Engineering Process

[[

]]

5.1 Planning

[[

]]

Input Documents:

[[

Table 1 Planning Phase Output Documents

[[

[illegible]

[[

11

⁴ M-MIS = Man-Machine Interface System and HFE = Human Factors Engineering.

5.1.1 Equipment Design Requirements - SDDs, LDs and P&IDs and IO/FX/Setpoint Database

[[

]]

5.1.2 Management Plans

5.1.2.1 Software Management Plan

[[

]]

5.1.2.2 Project Plan

[[

]]

5.1.2.3 Software Configuration Management Plan

[[

]]

The individual(s) responsible for the software configuration management process shall be identified. The SCMP is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.1.2.4 Verification and Validation Plan

[[

]]

The activities defined in the VVP help assure the software quality of the software-based products. The VVP is a configurable item, and is subject to verification and configuration management as specified in the VVP (itself) [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.1.2.5 Software Safety Plan

[[

]]

IEEE 1228, Software Safety Plans [4.2.2(7)], presents an acceptable format for the Software Safety Plan [4.1.2(5)]. The Software Safety Plan is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.1.3 Planning Baseline Review Record

[[

]]

5.2 Design Definition

[[

11

Table 2 Design Definition Phase Output Documents

[[

[illegible]

Quality goals:

- All design requirements shall be verifiable and traceable to the input documents.

5.2.1 Hardware/Software Specification

[[

]]

5.2.2 Software Requirements Specification (SRS)

[[

]]

5.2.3 System Block Diagram

[[

]]

The SBD is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.2.4 Instrument Performance Specification (with Software Requirements)

[[

]] The IPS is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.2.5 Sub-System Schematic

[[

]]

5.2.6 Data Communications Protocol

[[

]]

5.2.7 Software Test Plan

[[

]] The Software Test Plan
is a configurable item, and is subject to verification and configuration management as specified
in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.2.8 User's Manual

[[

The User's Manual is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.2.9 Support Software and Tools

[[

]] The Support Software/Tool Report and the associated documentation of the support software/tool shall be included in the Support Software/Tool Documentation Package and filed in the software project DRF. The support software/tool and its documentation package shall be included as part of the appropriate software life cycle phase baseline review and placed under configuration control {see SCMP [4.1.2(1)]}.

5.2.10 Third Party Software⁵

[[

⁵ Third party software refers to the purchased software libraries or package used as part of the development of a software-based product, not the software procured from vendors, such as the Non Essential DCIS vendor.

]] The Third Party Software Evaluation Report and the associated documentation shall be included in the Third Party Software Documentation Package and shall be kept in the software project DRF.

The Third Party Software Documentation Package shall be included as part of the appropriate software life cycle phase baseline review, and placed under configuration control {see SCMP [4.1.2(1)]}.

5.2.11 Adaptation of Previously Developed Software

[[

]] The supplemental documentation shall be verified in accordance with the methods defined in the VVP [4.1.2(2)] and controlled, filed in the software project DRF and included as part of the in the appropriate baseline review.

5.2.12 Safety Analysis of Design Definition

[[

]] The analysis reports are configurable items, and are subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.2.13 Design Definition Baseline Review Record

[[

]]

The Design Definition Baseline Review Record shall be maintained by the BRT Lead and a duplicate hardcopy shall be filed in the software project DRF {see SCMP [4.1.2(1)]}.

5.2.14 Safety Analysis of Concept Definition

[[

]] The analysis report is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.3 Software Design

[[

]]

Output documents, verification documents and verification methods:

Table 3 Software Design Phase Output Documents

[[

]]

Quality goals:

[[

]]

5.3.1 Software Design Specification

[[

]] The SDS is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.3.2 Internal Data Communication Protocol Specification

[[

]] It shall also include a timing analysis. The Internal Data Communication Protocol Specification is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.3.3 Validation Test Procedures and Test Cases Specification

[[

]] The Validation Test Procedures and Test Cases Specification is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.3.4 Software Conventions and Guidelines Document

[[

]]

The Software Conventions and Guidelines document is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.3.5 Safety Analysis of Software Design

[[

]] The analysis reports are configurable items, and are subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.3.6 Software Design Baseline Review Record

[[

]] The Software Design Baseline Review Record shall be maintained by the BRT Lead and a duplicate hardcopy shall be filed in the software project DRF {see SCMP [4.1.2(1)]}.

5.4 Software Coding

[[

]]

Output documents, verification documents and verification methods:

Table 4 Software Coding Phase Output Documents

[[

Quality goals:

[[

•

]]

5.4.1 Coding**5.4.1.1 Software Source Code**

[[

]] The storage and configuration management requirements of the software source code are outlined in the SCMP [4.1.2(1)].

5.4.1.2 Code Reviews

[[

]]

5.4.2 Software Module Testing

[[

]]

5.4.2.1 Module Test Reports

[[

]]

5.4.3 Safety Analysis of Software Coding

[[

]]

The analysis reports are configurable items, and are subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.4.4 Software Coding Baseline Review Record

[[

]] The

Software Coding Baseline Review Record shall be maintained by the BRT Chairperson and a duplicate hardcopy shall be filed in the software project DRF {see SCMP [4.1.2(1)]}.

5.5 Integration Test

[[

]]

Output documents, verification documents and verification methods:

Table 5 Integration Test Phase Output Documents

[[

Quality goals:

- [[

5.5.1 Integration Testing

[[

]]

5.5.2 Integration and Installation Test Report

[[

]] The Integration and Installation Test Report is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

[[

]]

5.5.3 Safety Analysis of Integration Test

[[

]] The analysis report is a configurable item, and is subject to verification

and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.5.4 Integration Test Baseline Review Record

[[

]] The
Integration Test Baseline Review Record shall be maintained by the BRT Lead and a duplicate
hardcopy shall be filed in the software project DRF {see SCMP [4.1.2(1)]}.

5.6 Validation Test

[[

]]

Output documents, verification documents and verification methods:

Table 6 Validation Test Phase Output Documents

[[

Quality goals:

[[

]].

5.6.1 Validation Testing

[[

]]

5.6.2 Validation Test Report

[[

]] The Validation Test Report is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.6.3 Safety Analysis of Validation Test

[[

]] The analysis report is a configurable item, and is subject to verification and configuration management as specified in the VVP [4.1.2(2)] and SCMP [4.1.2(1)] respectively.

5.6.4 Validation Test Baseline Review Record

[[

]]
The Validation Test Baseline Review Record shall be maintained by the BRT Lead and a duplicate hardcopy shall be filed in the software project DRF {see SCMP [4.1.2(1)]}.

5.7 Change Control

[[

]]

Output documents, verification documents and verification methods:

Table 7 Change Control Phase Output Documents

[[

]]

Quality goals:

[[

]]

5.7.1 Change Control Objective and Scope

[[

⁶ The revised documentation may include an abbreviated version of the Software Validation Test Procedure to test the modified sections of the software package.

⁷ May be a supplemental or "delta" report.

--

[[
]]

Figure 1 I&C Software Life Cycle Phases vs. ESBWR SRP Software Life Cycle Phases

⁸ Not applicable to essential DCIS as it is microprocessor based.

[[

]]

**Figure 2 I&C Software Life Cycle Phases and Hierarchy
of Documentation Development.**

II

]]

**Figure 2 I&C Software Life Cycle Phases and Hierarchy
of Documentation Development (Continued)**

[[

]]

Figure 3 Verification and Validation Process

Appendix A: Document Formats

A.1 Hardware/Software Specification (HSS)

[[

A.2 Software Requirements Specification (SRS)

[[

]]

A.3 Instrument Performance Specification (IPS)

[[

]]

Appendix B: Requirement Standards

Application	Requirement Standards
1. Quality Class S Application or Systems	Reg Guide 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants [4.2.4(1)]
2. Quality Class N-R Application or Systems	ISO-9000-3, Quality management and quality assurance standards - Guidelines for the application of ISO 9001 to the development, supply and maintenance of software [4.2.3(1)]
3. Quality Class N-G Application or Systems	