MFN 09-520

Enclosure 2

ESBWR Licensing Topical Report
ESBWR Software Quality Assurance Program Manual
NEDO-33245, Revision 4

Public Version

HITACHI

GE Hitachi Nuclear Energy

NEDO-33245
Revision 4
Class I
DRF 0000-0049-7141
July 2009

Licensing Topical Report

ESBWR – SOFTWARE QUALITY ASSURANCE PROGRAM MANUAL

Copyright 2006, 2009 GE-Hitachi Nuclear Energy Americas LLC

All Rights Reserved

NON-PROPRIETARY INFORMATION NOTICE

This is a non-proprietary version of NEDE-33245P which has the proprietary information removed. Portions of the document that have been removed are indicated by open and closed double square bracket as shown here [[ ]].

IMPORTANT NOTICE REGARDING THE 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 GEH with respect to information in this document are contained in contracts between GEH and participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than those participating entities and for any purposes other than those for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

Table of Contents

1. INTRODUCTION 1
1.1 OVERVIEW 1
1.2 PURPOSE AND SCOPE 1
1.3 ACRONYMS, ABBREVIATIONS AND DEFINITIONS 2
1.4 SOFTWARE DEVELOPED BY VENDORS 2
1.5 SOFTWARE CLASSIFICATION 2
2. APPLICABLE DOCUMENTS 6
2.1 SUPPORTING DOCUMENTS 6
2.2 CODES AND STANDARDS 6
2.2.1 NUREG 6
2.2.2 Code of Federal Regulations 6
2.2.3 U.S. Nuclear Regulatory Commission Regulatory Guides 6
2.2.4 Institute of Electrical and Electronics Engineers 7
2.3 SUPPLEMENTAL DOCUMENTS 8
2.4 ADDITIONAL IEEE STANDARD GUIDANCE 13
2.5 INTERNATIONAL STANDARDS 14
3. SOFTWARE QUALITY ASSURANCE PLAN 15
3.1 PURPOSE AND SCOPE 15
3.2 MANAGEMENT ORGANIZATION 15
3.2.1 Organization 15
3.2.2 Activities 15
3.2.3 Qualification and Responsibilities 16
3.2.4 Organizational Interfaces 20
3.2.5 Scheduling and Planning 20
3.2.6 Approval Authority 21
3.3 DOCUMENTATION 21
3.4 STANDARDS, PRACTICES, CONVENTIONS AND METRICS 21
3.4.1 Standards, Practices and Conventions 21
3.4.2 Metrics 22
3.5 REVIEWS AND AUDITS 22
3.5.1 Reviews 22
3.5.2 Audits 23
3.6 PROBLEM REPORTING AND CORRECTIVE ACTION 24
3.6.1 Problem Reporting 24
3.6.2 Corrective Action 24
3.7 TOOLS, TECHNIQUES AND METHODOLOGIES 25
3.7.1 Tools 25
3.7.2 Techniques and Methodologies 27
3.8 CODE AND MEDIA CONTROL 27
3.9 VENDOR AND ACQUIRED SOFTWARE CONTROL 28
3.9.1 Vendor Control 28
3.9.2 Commercial Off-the-Shelf Software 29
3.9.3 Previously Developed Software 29
3.10 RECORDS COLLECTION, MAINTENANCE, AND RETENTION 29
3.11 TRAINING 29
3.12 RISK MANAGEMENT 29
4. SOFTWARE SAFETY PLAN 30
4.1 PURPOSE AND SCOPE 30
4.2 SOFTWARE SAFETY MANAGEMENT 30

4.2.1 Organization and Responsibilities ... 30
4.2.2 Qualifications and Training ... 31
4.2.3 Software Life Cycle ... 31
4.2.4 Documentation Requirements ... 31
4.2.5 Software Safety Program Records ... 32
4.2.6 Software Configuration Management Activities ... 33
4.2.7 Software Quality Assurance Activities ... 34
4.2.8 Software V&V ... 34
4.2.9 Tool Support and Approval ... 34
4.2.10 Previously Developed or Purchased Software ... 35
4.2.11 Subcontract Management ... 35
4.2.12 Process Certification ... 35
4.3 SOFTWARE SAFETY ANALYSES ... 35
4.3.1 Software Safety Preparation Analysis ... 36
4.3.2 Software Safety Requirements Analysis ... 36
4.3.3 Software Safety Design Analysis ... 38
4.3.4 Software Safety Code Analysis ... 42
4.3.5 Software Safety Test Analysis ... 45
4.3.6 Software Safety Installation Analysis ... 53
4.3.7 Software Safety Change Analysis ... 55
4.4 POST DEVELOPMENT ... 57
4.5 TRAINING ... 57
4.6 DEPLOYMENT ... 57
4.6.1 Installation ... 57
4.6.2 Startup and Transition ... 57
4.6.3 Operations Support ... 58
4.7 MONITORING ... 58
4.8 MAINTENANCE ... 58
4.9 RETIREMENT AND NOTIFICATION ... 58
4.10 PLAN APPROVAL ... 58
5. SOFTWARE VERIFICATION AND VALIDATION PLAN ... 59
5.1 PURPOSE AND SCOPE ... 59
5.1.1 Purpose ... 59
5.1.2 Scope ... 59
5.2 V&V OVERVIEW ... 59
5.2.1 Organization ... 59
5.2.2 V&V Schedule ... 59
5.2.3 Software Integrity Level Scheme ... 60
5.2.4 Resources Summary ... 60
5.2.5 Roles and Responsibilities ... 60
5.2.6 Tools, Techniques, and Methods ... 60
5.3 V&V ACTIVITIES AND TASKS ... 63
5.3.1 Management of V&V Activities ... 64
5.3.2 Planning Phase V&V Activities ... 68
5.3.3 Requirements Phase V&V Activities ... 76
5.3.4 Design Phase V&V Activities ... 84
5.3.5 Implementation Phase V&V Activities ... 91
5.3.6 Test Phase V&V Activities ... 105
5.3.7 Installation Phase V&V Activities ... 112
5.3.8 Operations and Maintenance Phase V&V Activities ... 121
5.3.9 Acquired Software and Vendor V&V Tasks ... 127

5.4 V&V REPORTING 129
5.4.1 Independent Verification Package 129
5.4.2 Design Review Report 129
5.4.3 Test Report 129
5.4.4 Anomaly Report 129
5.4.5 Baseline Review Record 130
5.4.6 Managerial Review Report 130
5.4.7 V&V Final Report 131
5.5 V&V ADMINISTRATIVE REQUIREMENTS 131
5.5.1 Anomaly Resolution and Reporting 131
5.5.2 Baseline Change Assessment and Task Iteration Policy 131
5.5.3 Deviation Policy 132
5.5.4 Control Procedures 132
5.5.5 Standards, Practices, and Conventions 132
5.5.6 Test Documentation Requirements 133
6. SOFTWARE CONFIGURATION MANAGEMENT PLAN 134
6.1 PURPOSE AND SCOPE 134
6.1.1 Purpose 134
6.1.2 Scope 134
6.2 SOFTWARE CONFIGURATION MANAGEMENT 134
6.2.1 Organization 134
6.2.2 SCM Responsibilities 135
6.2.3 Applicable Policies, Procedures, and Directives 137
6.2.4 SCM Schedule 137
6.3 SOFTWARE CONFIGURATION MANAGEMENT RESOURCES 137
6.3.1 SCM Tools 137
6.3.2 SCM Techniques 138
6.4 SCM TASKS 138
6.4.1 Configuration Identification 138
6.4.2 Configuration Control 139
6.4.3 Configuration Status Accounting 144
6.4.4 Configuration Audits 144
6.4.5 Baseline Reviews 145
6.5 SOFTWARE RELEASE PROCEDURES 146
6.6 SOFTWARE PRODUCT RELEASE 146
6.7 VENDOR CONTROL 146
6.7.1 Software Developed by Vendors for the Project 146
6.7.2 Acquired Software 147
6.8 RECORD COLLECTION AND RETENTION 147
7. SOFTWARE TEST PLAN 148
7.1 PURPOSE 148
7.2 SCOPE 148
7.2.1 Test Hierarchy 148
7.2.2 Test Activities 148
7.2.3 Vendor Test Submittal 150
7.3 SOFTWARE VALIDATION TEST – INDEPENDENT VERIFICATION AND VERIFICATION TEAM (IVVT) 150
7.4 SYSTEM FACTORY ACCEPTANCE TEST 151
7.5 [[ ]] TEST 151
7.6 SITE ACCEPTANCE TEST 152
7.7 TEST DOCUMENTATION 152

7.7.1 Test Plans 153
7.7.2 Test Design Specifications 155
7.7.3 Test Case Specifications 156
7.7.4 Test Procedure Specifications 156
7.7.5 Test Item Transmittal Report 157
7.7.6 Test Log 158
7.7.7 Test Incident Reports 159
7.7.8 Test Summary Reports 160
8. SQAPM MAINTENANCE 162
9. TABLES & FIGURES 163
APPENDIX A – SOFTWARE PLANS CONFORMANCE REVIEW 199
APPENDIX B ACRONYMS AND ABBREVIATIONS 209
APPENDIX C DEFINITIONS 215
APPENDIX D SOFTWARE CHARACTERISTICS 225

List of Tables

Table 1.5-1 Software Classification 3
Table 4.3.2.1-1 Software Safety Requirements Analysis Tasks and Outputs 37
Table 4.3.3.1-1 Software Safety Design Analysis Tasks and Outputs 39
Table 4.3.4.1-1 Software Safety Code Analysis Tasks and Outputs 43
Table 4.3.5.1-1 Software Safety Test Analysis Tasks and Outputs 46
Table 4.3.6.1-1 Software Safety Test Analysis Tasks and Outputs 54
Table 4.3.7.1-1 Software Safety Change Analysis Tasks and Outputs 55
Table 5.3.1.1-1 SVVP Generation V&V Activities and Outputs 64
Table 5.3.1.3-1 V&V Management Review Activities and Outputs 65
Table 5.3.1.4-1 Management and Technical Review Support Activities and Outputs 66
Table 5.3.1.5-1 Organizational Interfaces & Supporting Processes Activities and Outputs 66
Table 5.3.1.6-1 Acquisition Support V&V Activities (Acquisition Process) and Outputs 67
Table 5.3.2.1-1 Concept Documentation Evaluation Activities and Outputs 69
Table 5.3.2.2-1 Software Plans Evaluation Activities and Outputs 70
Table 5.3.2.4-1 Hardware, Software and User Requirements Allocation Analysis Activities and Outputs 71
Table 5.3.2.5-1 Traceability Analysis Activities and Outputs 72
Table 5.3.2.6-1 [[ ]] and SAT Plan Generation Evaluation Activities and Outputs 73
Table 5.3.2.7-1 Hazard Analysis Activities and Outputs 73
Table 5.3.2.8-1 Risk Analysis Activities and Outputs 74
Table 5.3.2.9-1 Acquisition V&V Activities and Outputs 74
Table 5.3.2.10-1 Configuration Management Assessment Activities and Outputs 76
Table 5.3.3.1-1 Requirements Traceability Analysis Activities and Outputs 77
Table 5.3.3.2-1 Software Requirements Evaluation Activities and Outputs 78
Table 5.3.3.3-1 UIS Evaluation Activities and Outputs 80
Table 5.3.3.4-1 Interface Analysis Activities and Outputs 82
Table 5.3.3.6-1 Risk Analysis Activities and Outputs 83
Table 5.3.3.7-1 Configuration Management Assessment Activities and Outputs 84
Table 5.3.4.1-1 Traceability Analysis Activities and Outputs 85
Table 5.3.4.2-1 Software Design Evaluation Activities and Outputs 86
Table 5.3.4.3-1 Test Plans Generation and Verification Activities and Outputs 88
Table 5.3.4.4-1 Interface Analysis Activities and Outputs 89

Table 5.3.4.6-1 Risk Analysis Activities and Outputs 90
Table 5.3.4.7-1 Configuration Management Assessment Activities and Outputs 91
Table 5.3.5.1-1 Traceability Analysis Activities and Outputs 92
Table 5.3.5.2-1 Source Code and Source Code Documentation Evaluation Activities and Outputs 93
Table 5.3.5.3-1 Interface Analysis Activities and Outputs 96
Table 5.3.5.5-1 Software Functional Test Execution and Verification Activities and Outputs .. 97
Table 5.3.5.6-1 Software Functional Test Report Verification Activities and Outputs 100
Table 5.3.5.7-1 Software Build Description Evaluation Activities and Outputs 101
Table 5.3.5.8-1 Software Validation and SFAT Test Design, Test Cases and Test Procedure Specifications Evaluation Activities and Outputs 102
Table 5.3.5.9-1 Risk Analysis Activities and Outputs 104
Table 5.3.5.10-1 Configuration Management Assessment Activities and Outputs 105
Table 5.3.6.1-1 Traceability Analysis Activities and Outputs 106
Table 5.3.6.2-1 Software Validation Test Execution Activities and Outputs 106
Table 5.3.6.3-1 Software Validation Test Report Evaluation Activities and Outputs 107
Table 5.3.6.4-1 [[ ]] and SAT Test Design, Case and Procedure Specifications Evaluation Activities and Outputs 109
Table 5.3.6.5-1 Hazard Analysis Activities and Outputs 110
Table 5.3.6.6-1 Risk Analysis Activities and Outputs 110
Table 5.3.6.7-1 Configuration Management Assessment Activities and Outputs 111
Table 5.3.6.8-1 Software O&M and Software Training Manual Evaluation Activities and Outputs 112
Table 5.3.7.1-1 System Factory Acceptance Test Execution Activities and Outputs 113
Table 5.3.7.2-1 System Factory Acceptance Test Report Evaluation Activities and Outputs .. 114
Table 5.3.7.3-1 [[ ]] and Site Acceptance Test Execution Activities and Outputs 115
Table 5.3.7.4-1 [[ ]] and Site Acceptance Report Evaluation Activities and Outputs 116
Table 5.3.7.5-1 Installation Configuration Audit Activities and Outputs 117
Table 5.3.7.6-1 Installation Configuration Table Generation and Evaluation Activities and Outputs 118
Table 5.3.7.7-1 Installation Checkout Activities and Outputs 119
Table 5.3.7.8-1 Risk Analysis Activities and Outputs 119
Table 5.3.7.9-1 Configuration Management Assessment Activities and Outputs 120

Table 5.3.7.10-1 V&V Final Report Generation Activities and Outputs 121
Table 5.3.8.1-1 Evaluation of New Constraints Activities and Outputs 122
Table 5.3.8.2-1 Proposed Change Assessment Activities and Outputs 122
Table 5.3.8.3-1 SVVP Revision Activities and Outputs 123
Table 5.3.8.4-1 Anomaly Evaluation Activities and Outputs 123
Table 5.3.8.5-1 Regression Analysis Activities and Outputs 124
Table 5.3.8.6-1 Migration Assessment Activities and Outputs 125
Table 5.3.8.7-1 Retirement Assessment Activities and Outputs 126
Table 5.3.8.8-1 Risk Analysis Activities and Outputs 126
Table 5.3.8.9-1 Task Iteration Activities and Outputs 127
Table 6.4.2.2-1 Reasons for Change Request 140
Table 6.4.2.2-2 Change Process Steps 141
Table 9-1a Software Life Cycle Tasks, Responsibilities and Documentation-Planning Phase.. 163
Table 9-1b Requirements Phase 164
Table 9-1c Design Phase 166
Table 9-1d Implementation Phase 170
Table 9-1e Test Phase 173
Table 9-1f Installation Phase 176
Table 9-1g Operations and Maintenance Phase 179
Table 9-2 V&V and SSA Tasks Assigned to Each Software Class 180
Table 9-3 Problems and Corrective Action Reporting 186
Table 9-4 Configuration Items 192

List of Figures

Figure 1. Software Class Evaluation Process 4
Figure 2. (Deleted) 16
Figure 3. Example of A Traceability Matrix Structure 26
Figure 4. Baseline Review Record 197
Figure 5. Software Library Structure 198

SUMMARY OF CHANGES FROM PREVIOUS REVISION

ITEM	LOCATION	CHANGE
Entire Document		
1.	Entire document	Revised entire document to correct the industry documents reference to incorporate RAI 7.1-128 comment.
2.	Entire document	Revised entire document to remove the Organization Chart and applicable references to incorporate RAI 7.1-129 comment.
3.	Entire document	Revised to clarify the purposes to incorporate RAI 14.3-402 comment.
4.	Entire document	Corrected typographical and grammatical errors, consistent use of document titles and acronyms, list numbering, font synchronization and paragraph formatting to improve clarity and readability of SQAPM.
5.	Entire document	Removed ESBWR references (where appropriate) to make this SQAPM more generic.
6.	Entire document	Revised organizational titles and roles (where appropriate) to make this SQAPM more generic.
7.	Entire document	Standardized SMPM-cited references (where appropriate) throughout this SQAPM.
8.	Entire document	Standardized terminology and appropriate use for V&V, Independent Verification, Verification and Validation
9.	Entire document	Corrected and standardized mixed cases (title, upper, lower) throughout this SQAPM.
10.	Entire document	Clarified the use of the word "all" throughout this SQAPM.
11.	Entire document	Deleted "Unit" from "Module/Unit Test" throughout this SQAPM.
12.	Entire document	Corrected the term "Software Conventions and Guidelines" to "Software Coding and Conventions Guidelines Document".
13.	Entire document	Revised the term "Intra system" to "Intra-System".
14.	Entire document	Replaced "GEH Self Assessment, Corrective Action and Audits" with "Corrective Action Process".

ITEM	LOCATION	CHANGE
15.	Entire document	Replaced "system" with "software product" (where applicable).
16.	Entire document	Standardized section and subsection usage.
Section 1		
17.	Section 1.2	Changed "Software Testing Requirements" to "Software Test Program" for SQA activities.
Section 2		
18.	Section 2.3	Added new LTR, "ESBWR Cyber Security Program Plan" and associated document number.
19.	Section 2.3	Deleted IEEE Standard Glossary of Software Engineering Terminology and IEEE 610.12-1990.
20.	Section 2.4	Added IEEE 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology.
Section 3		
21.	Section 3.1	Referenced Section 7.0 for test results adherence to acceptance standards.
22.	Subsection 3.2.3.2	Revised to clarify relationship between SQA, SPE and Development organizations.
23.	Subsection 3.2.3.4	Added relevant software classes to SPE teams.
24.	Subsection 3.2.3.4.2	Clarified IVVT's responsibilities with regard to a design's safety and security.
25.	Subsection 3.2.3.4.4	Clarified the SST Task Lead responsibilities.
26.	Subsection 3.2.3.5	Removed CM traceable records and added relevant records.
27.	Subsection 3.2.3.6	Clarified Design Team's responsibilities.
28.	Subsection 3.2.4	Clarified Project Manager's responsibilities.
29.	Subsection 3.4.1	Added "Secure Coding Practices" as a software coding guideline for consistency with the SMPM.
30.	Subsection 3.7.1.6	Added Software Validation Test (SVT) as a valid software test.
31.	Subsection 3.7.2	Added Software Test Plan (STP) and associated section reference.

ITEM	LOCATION	CHANGE
32.	Subsection 3.9.1	Changed "vendor's verification process" to "vendor's QA program." to improve clarity.
33.	Subsection 3.9.3	Removed "and dedication" to "evaluation process" for better accuracy.
34.	Subsection 3.11	Changed "V&V tasks" to "quality tasks" to improve clarity.
Section 4		
35.	Subsection 4.1	Deleted statement regarding precedence of safety over budget and schedule inasmuch as that is the entire philosophy of the SQAPM.
36.	Subsection 4.2.1	Clarified the responsibilities of the SPE Manager and SST Task Lead regarding SSA activities.
37.	Subsection 4.2.4	Streamlined subsection to clarify documentation requirements for Software Configuration Management, Configuration Management Plan, Software Quality Assurance, Software Safety Requirements, Software Safety Design, Test Documentation and Software IV&V.
38.	Subsection 4.2.6	Removed entire subsection, "Software Safety Program Records" because this is duplicated in section 4.5.
39.	Subsection 4.2.7	Replaced the phrase "predecessor document" with "SQAPM Section 8.0" since the SSP is a part of the SQAPM and its maintenance process.
40.	Section 4.3	Revised for consistency with IEEE 1228.
41.	Section 4.3 *(Tables)*	Reformatted and streamlined entire section from four columns to two columns to improve legibility. Revised to comply with IEEE 1228 with various changes in Tasks, Inputs and Outputs.
42.	Subsection 4.5	Revised text on safety training requirements and systematic training approaches.
43.	Subsection 4.4.3	Changed "Software Safety Modules" to "Software Product" throughout subsection.
44.	Subsection 4.6.2	Changed "Startup Procedure" to "Installation Plan" because the Installation Plan is more inclusive for addressing requirements for product startup whereas a procedure just gives the steps needed to implement requirements for startup.

ITEM	LOCATION	CHANGE
45.	Subsection 4.6.3	The Operations Support paragraph has been revised to clarify and make specific references to the O&M Manual.
46.	Subsection 4.8	Removed paragraph on re-implementing software lifecycle per the SMPM for software maintenance and included a cross-reference to SMPM subsection 5.12.3 for consistency. This is where such maintenance is discussed.
47.	Subsection 4.10	For SSP approval, SQAPM section 3,2,3,1 on approval is referenced because the SSP is an integral part of the overall SQAPM.
Section 5		
48.	Subsection 5.1.2	Revised to clarify the scope for the SVVP.
49.	Subsection 5.2.3	Revised to clarify the Software Integrity Level Scheme.
50.	Subsection 5.2.4	Removed staffing and budget reference for the SPE Manager responsibilities because they are beyond the scope of the SQAPM.
51.	Subsection 5.2.6.1	Added four new evaluation confirmations for V&V Tool usage for consistency with subsection 4.2.9.
52.	Subsection 5.2.6.2.1	Clarified the four GEH verification methods consistent with GEH Engineering Operating Procedures..
53.	Subsection 5.2.6.2.2	Clarified IVVT's responsibilities for code review data sheets.
54.	Subsection 5.2.6.2.3	Clarified the module and integration portions of the SFT.
55.	Subsection 5.2.6.2.4	Clarified Design team responsibilities for SVT.
56.	Subsection 5.2.6.2.5	Add new adherences for Baseline Reviews.
57.	Section 5.3 *(including subsections)*	Revised to clarify V&V activities and outputs for consistency with IEEE 1012.

ITEM	LOCATION	CHANGE
58.	Section 5.3	Revised to clarify statement for software product/service acquisition in accordance with vendor software.
59.	Section 5.3 *(Tables)*	Reformatted and streamlined entire section from four columns to two columns to improve legibility. Reformatted and revised V&V Inputs, V&V Tasks and V&V Outputs for each V&V activity.
60.	Section 5.3 *(Tables)*	Expanded V&V Outputs with specific/individual deliverables.
61.	Subsection 5.3.9	Revised to clarify "V&V" activities for support for Software support tools.
62.	Subsection 5.4.1	Revised to clarify documentation formats for Independent Verification Package.
63.	Subsection 5.4.4	Revised to clarify anomaly observations and reporting.
64.	Subsection 5.4.5	Clarified V&V and SSA Summary criteria and removed the TPE responsibility statement on assuring design meets requirements in the Baseline Review Record since these responsibilities are assigned to the RE in subsection 6.2.1.
65.	Subsection 5.4.7	Revised to clarify V&V Final Report documentation requirements.
66.	Subsection 5.5.1	Revised first paragraph for Anomaly Resolution and Reporting to be consistent with subsection 5.4.4.
67.	Subsection 5.5.2	Revised to clarify that V&V tasks to be repeated are dependent on the complexity of change and the software classification.
68.	Subsection 5.5.6	Changed title to "Test Documentation Requirements" to be consistent with section 7.0.
Section 6		

ITEM	LOCATION	CHANGE
69.	Subsection 6.3.1	Removed out-of-scope statement regarding HFE unresolved issues in SCM Tools section.
70.	Subsection 6.4.2.1	Removed redundant control statement of software product design.
71.	Subsection 6.4.2.2	Removed ESBWR certified design change statement regarding MMIS/HFE IP reference as this is outside the scope of the SQAPM.
72.	Subsection 6.4.2.2.4	Revised to clarify change request tracking tool.
73.	Subsection 6.4.5	Removed statement on O&M and Retirement phases baseline record reviews as the baseline review process for these two phases is the same as the other phases.
74.	Subsection 6.4.5	Added new CySA task statement for baseline reviews for consistency with the SMPM.
Section 7		
75.	Section 7.2	Added new scope section to clarify the scope of the STP.
76.	Subsection 7.2.3	Revised title to "Vendor Test Submittal" to be consistent with the discussion in this subsection.
77.	Section 7.3	Added Design Team SVT responsibility for consistency with the SMPM.
78.	Section 7.4	Added Quality Hold Point - QCE statements for the SFAT.
79.	Section 7.5	Added Quality Hold Point - QCE statements for the [[ ]].
80.	Section 7.5	Clarified team members in Section 7.5.
81.	Section 7.6	Added Customer Witness Point requirement for the SAT.
82.	Section 7.6	Clarified team members in Section 7.6.
83.	Section 7.7	Revised entire section for Test Documentation to be consistent with IEEE 829.
84.	Subsection 7.7.1	Revised entire subsection for Test Plans to be consistent with IEEE 829.
85.	Subsection 7.7.2	Revised title to Test Design Specifications to be consistent with IEEE 829.

ITEM	LOCATION	CHANGE
86.	Subsection 7.7.2	Revised entire subsection for Test Design Specifications to be consistent with IEEE 829.
87.	Subsection 7.7.3	Revised title to Test Case Specifications to be consistent with IEEE 829.
88.	Subsection 7.7.3	Revised entire subsection for Test Case Specifications to be consistent with IEEE 829.
89.	Subsection 7.7.4	Added new subsection, Test Procedure Specifications to be consistent with IEEE 829.
90.	Subsection 7.7.5	Added new subsection, Test Item Transmittal Report to be consistent with IEEE 829.
91.	Subsection 7.7.6	Added new subsection, Test Log to be consistent with IEEE 829.
92.	Subsection 7.7.7	Added new subsection, Test Incident Reports to be consistent with IEEE 829.
93.	Subsection 7.7.8	Added new subsection, Test Summary Reports to be consistent with IEEE 829.
94.	Subsection 7.2.3	Revised title to "Vendor Test Submittal" to be consistent with IEEE 829.
Section 8		
95.	Section 8.0 SQAPM Maintenance	Deleted statement on NRC notification for SQAPM changes because this is implicit in and redundant to the requirements of the GEH Corrective Action Process invoked in the preceding paragraph.

Tables		
96.	Table 1.5-1	Formatted table by bulleting table items for improved legibility.
97.	Table 9-1a	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
98.	Table 9-1b	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
99.	Table 9-1c	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
100.	Table 9-1d	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
101.	Table 9-1e	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
102.	Table 9-1f	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
103.	Table 9-1g	Clarified Design Tasks, Design Task Inputs, Design Task Outputs, Quality Tasks and Organizations to be consistent with tasks and outputs described within the text of the SQAPM.
104.	Table 9-2	Revised Table 9-2 to be consistent with changes made to sections 4.3 and 5.3. See items 40, 41, 58, 59 and 60.
105.	Table 9-3	Minor reformatting on Table 9-3 for improved clarity.

106.	Table 6.4.2.2-2	Added "Responsible Verifier" as a responsible individual in the change process steps for consistency with roles and responsibilities of other personnel (e.g., RE, SST and IVVT, RM and BRT).
Figures & Appendices		
107.	Figure 1	Changed the term "RTM" to "RTA" for accurate reference.
108.	Figure 3	Reformatted figure for improved legibility.
109.	Appendix A	Item #25 – clarified compliance of hardware activities to IEEE 603 as addressed within DCD chapter 7.
110.	Appendix A	Item #31 – removed deviation statement on IEEE 1228 because section 4.3 of this SQAPM had been specifically revised for IEEE 1228 compliance.
111.	Appendix B	Added new acronyms and deleted unused acronyms for consistency with the body of this SQAPM.
112.	Appendix C	Revised definition for code to be consistent with IEEE 610.12.
113.	Appendix C	Added definition for Critical Digital Asset to be consistent with SMPM.
114.	Appendix C	Added definition for module testing to be consistent with IEEE 610.12
115.	Appendix C	Added Requirements Analysis definition to be consistent with IEEE 610.12.
116.	Appendix C	Updated definition for Requirements Traceability Analysis for consistency with SMPM.
117.	Appendix C	Changed Unit Testing definition to "see module testing" since these are redundant one to another.
118.	Appendix C	Revised definition for Verification and Validation to be consistent with IEEE 610.12.

1. INTRODUCTION

1.1 OVERVIEW

The SQAPM describes the Software Quality Assurance (SQA) activities to be performed during the software life cycle phases of the Nuclear Safety-Related (Quality Class Q) and Nonsafety-Related (Quality Class N3 and N2) digital computer-based I&C system, hereafter referred to as "software product".

The SQAPM meets the acceptance criteria specified in Chapter 7 of NUREG 0800, Standard Review Plan (SRP) [2.2.1] and Branch Technical Position (BTP) HICB-14 R4, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems [2.2.1], except where specified in Appendix A.

In addition, the SQAPM meets the requirements specified in the ESBWR Man-Machine Interface System and Human Factors Engineering Implementation Plan (MMIS/HFE IP) [2.1(1)] for a Software Quality Assurance Program Manual (SQAPM) to be prepared.

1.2 PURPOSE AND SCOPE

The purpose of the SQAPM is to:

- Establish an SQA program in full compliance with 10 CFR 50, Appendix A, General Design Criteria for Nuclear Power Plants and IEEE 603 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations [2.2.4].
- 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 the GE Hitachi Nuclear Energy (GEH) Quality Assurance Program, which is in full compliance with 10 CFR 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plant and Fuel Processing Plants [2.2.2].

The objectives of the SQA program are to ensure that:

- The design teams comply with:
  - Regulatory-compliant Policies and Procedures (P&Ps) to guide software development
  - The Engineering Operating Procedures (EOPs)
  - The requirements described in this SQAPM
  - The Software Management Program Manual (SMPM) [2.3(1.a)] (hereafter referred to as SMPM)
- The design documentation and design outputs for each software life cycle phase defined in the SMPM [2.3(1.a)] are adequate (i.e., correct and complete).
- The final software products are high quality, acceptable for installation, and ready for reliable operation in a nuclear power plant.

The SQAPM defines the SQA activities, methods, and tools necessary to execute these objectives. The SQAPM also specifies the following:

- Verification and Validation (V&V) activities [Section 5.0, Software V&V Plan (SVVP)]
- Software Safety Analysis (SSA) [(Section 4.0 Software Safety Plan (SSP)]
- Software Configuration Management (SCM) [Section 6.0 Software Configuration Management Plan (SCMP)]
- Software Test Program [Section 7.0 Software Test Plan (STP)]

This SQAPM shall be in force during all phases of the software life cycle.

The applicable software products (software and firmware) covered by this SQAPM encompass the I&C systems, as specifically defined in the MMIS/HFE IP [2.1] (Subsection 1.2.4 only), 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.

1.3 ACRONYMS, ABBREVIATIONS AND DEFINITIONS

Acronyms and abbreviations are defined in Appendix B.

Definitions are provided in Appendix C.

1.4 SOFTWARE DEVELOPED BY VENDORS

Software products developed by GEH vendors shall comply with this SQAPM. If a vendor elects to follow its established SQA program, then the SQA program as defined in the purchase order (Section 3.9, Vendor and Acquired Software Control) shall be reviewed and approved by the SQA Manager to assure compliance with the requirements specified in this SQAPM.

1.5 SOFTWARE CLASSIFICATION

Software shall be assigned the appropriate Software Classification as described in Table 1.5-1.

If the software performs safety-related functions, which are specified per the Safety-related Classification determination process [2.3(2.t)], then it shall be classified as Software Class "Q."

Other software shall be considered nonsafety-related and will be divided into two sub-classes "N3" and "N2." A criticality analysis shall be conducted for nonsafety-related software. If there is a failure mode, which could challenge safety-related systems, then the software shall be classified as "N3."

The remaining Software shall be classified as "N2." This software is nonsafety-related system software whose failure cannot adversely affect a safety-related function.

The Software Classification is determined as shown in Figure 1. This scheme is based on IEEE Std. 1012, IEEE Standard for Verification and Validation Plans [2.2.4].

Table 1.5-1 Software Classification

Classification	Description
Software Class Q	Software performs safety-related functions as specified by the Safety-Related Classification determination process [2.3(2.t)].
Software Class N3	Nonsafety-related systems software whose failure could challenge safety-related systems as defined below: • Software whose inadvertent response to stimuli, failure to respond when required, response out-of-sequence could result in an accident or transient as defined in the Design Control Document, Chapter 15 [2.1] • Software that is intended to mitigate the result of an accident • 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

[[ ]]

Figure 1. Software Class Evaluation Process

[[

]]

2. APPLICABLE DOCUMENTS

Applicable documents include supporting documents, codes and standards, and supplemental documents. 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 input documents in the production of this program. These documents form the design basis for the activities stated in this plan. This document governs, in the event of any differences noted between the SQAPM and the ESBWR Composite Design Specification.

- ESBWR Man-Machine Interface System and HFE Implementation Plan (MMIS/HFE IP), NEDO-33217
- ESBWR Composite Design Specification (A11-5299), 26A6007
- ESBWR Composite Design Specification "Standard Review Plans and Regulatory Guides" (A11-5299), 26A6007AB
- ESBWR Composite Design Specification Industry Codes and Standards (A11-5299), 26A6007AC
- ESBWR DCD, Chapter 7, I&C Systems, 26A6642AW
- ESBWR DCD, Chapter 15, Safety Analysis, 26A6642BP

2.2 CODES AND STANDARDS

The following codes and standards are used in conjunction with this plan.

2.2.1 NUREG

The following codes and standards are applicable to the activities specified within this plan. This Plan conforms to planning requirements of these codes and standards except as explicitly noted in Appendix A.

- NUREG 0800, Standard Review Plan (SRP), Chapter 7
- Branch Technical Position (BTP) HICB-14 R4, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

2.2.2 Code of Federal Regulations

- 10 CFR 50, Appendix - B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants

2.2.3 U.S. Nuclear Regulatory Commission Regulatory Guides

The following codes and standards are applicable to the activities specified within this plan. This Plan conforms to planning requirements of these codes and standards except as explicitly noted in Appendix A.

- RG 1.152-2006, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
- RG 1.168-2004, Verification, Validation, Reviews, and Audits For Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169-1997, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.170-1997, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.171-1997, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.172-1997, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173-1997, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

2.2.4 Institute of Electrical and Electronics Engineers

The following codes and standards are applicable to the activities specified within this plan. This plan conforms to planning requirements of these codes and standards except as explicitly noted in Appendix A.

Where these Institute of Electrical and Electronics Engineers (IEEE) Standards provide recommended implementation techniques and methods, this program makes specific commitments only to those requirements restated hereafter. The ESBWR Project Work Plans shall capture the detailed implementation attributes in accordance with Work Planning and Scheduling [2.3(2a)]. Future exceptions or deviations from the recommendations specified in the IEEE standards shall require management approval as defined in the SMPM [2.3(1.a)] and this SQAPM, and are potentially subject to NRC notification. The NRC notification process is addressed in the MMIS/HFE Implementation Plan [2.1].

- IEEE 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- IEEE 603-1991 including correction sheet dated January 30, 1995, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- IEEE 828-1990, Standard for Software Configuration Management Plans
- IEEE 829-1983, Standard for Software Test Documentation
- IEEE 830-1993, IEEE Recommended Practice for Software Requirements Specifications
- IEEE 1008-1987, IEEE Standard for Software Unit Testing
- IEEE 1012-1998,Standard for Software Verification and Validation
- IEEE 1028-1997, Standard for Software Reviews

- IEEE 1042-1987, Guide to Software Configuration Management
- IEEE 1074-1995, IEEE Standard for Developing Software Life Cycle Processes

2.3 SUPPLEMENTAL DOCUMENTS

The following supplemental documents are used in conjunction with the SQAPM and enable the performance of the activities stated in Appendix A.

Reference Number	Applicable LTRs	Document Number
1.a	ESBWR Software Management Program Manual (SMPM)	NEDO-33226
1.b	ESBWR Cyber Security Program Plan	NEDO-33295

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	**Document Title**	**Abstract**
2.a	Work Planning and Scheduling	Defines the process and responsibilities for developing and documenting work plans and schedules for customer-contracted design work and authorized projects. Four key purposes of a Project Work Plan are to define project scope, develop a schedule, monitor progress, and control resources.
2.b	Product Data Management System (PDMS)	PDMS is the computer-based data system that stores, retrieves, and reports data relevant to the engineering definition of products and services offered and provided to customers. It provides current listings of the engineering documents under formal GEH change control (i.e., engineering controlled documents) that have been approved for issue or application to specific standard, requisition, fuel, and operating plant projects.
2.c	Supplier Design Services Document Review	Defines responsibilities and procedural requirements for review, approval, and control of documentation from suppliers for design services. Supplier submitted documents are entered as elements of the design basis in the Product Data Management System as engineering controlled documents or Design Record Files.
2.d	Engineering Test	Defines the process for specifying, performing, evaluating, and documenting engineering tests.

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	**Document Title**	**Abstract**
2.e	Design Review	Defines responsibilities and procedural requirements for conducting formal, design adequacy evaluations. Design Reviews are used to verify that product designs meet customer, functional, contractual, safety, health, environmental, regulatory, industry codes and standards, and corporate requirements.
2.f	Design Process	Defines the process for performing, documenting, and certifying design activities. Design activities include developing or modifying the design of systems, hardware and software, and the performance or modification of licensing studies, engineering evaluations, analyses, calculations and document preparation (e.g., specifications, drawings, reports).
2.g	Design Record File	Defines the process for the generation of a Design Record File, which is a formal, controlled information record for in-progress and completed engineering work.
2.h	Material Requests	Details responsibilities and procedural requirements for the release of technical, engineering, customer, and quality requirements that define material, equipment, labor, services and related data to meet GEH contract/purchase order, code, and regulatory requirements.
2.i	Independent Design Verification	Details roles and responsibilities for reviewing and substantiating a design to provide independent and documented confirmation that the design meets specified requirements.
2.j	Deferred Design Verification	Defines the process for deferring design verification and for clearing previous deferrals. The process applies to cases where a design, or portion of a design, must be released prior to completion of verification.
2.k	Document Initiation or Change by Engineering Review Memorandum/ Engineering Change Notice	Establishes the requirements for the initiation of or change to engineering controlled documents by use of the Engineering Review Memorandum/Engineering Change Notice. The process ensures traceability, configuration, and quality assurance of engineering documents are maintained through the current document revision, status, and final disposition.

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	**Document Title**	**Abstract**
2.l	Procurement Initiation and Control	Specifies the requirements for procurement of material, equipment, and services, including the application of technical, engineering, customer, and quality requirements to purchase orders. Defines the requirements for establishing and maintaining the Approved Suppliers List.
2.m	Supplier Supporting Document Review	Defines responsibilities and procedural requirements for review and acceptance of supporting documents submitted by suppliers of material, equipment and services to satisfy GEH Purchase Order requirements.
2.n	Deviation Disposition Requests from Suppliers	Establishes the requirements and procedure for processing Deviation Disposition Requests submitted by suppliers to obtain a disposition of deviations from the technical requirements of GEH Purchase Order requirements.
2.o	Supplier Change Request	Defines supplier responsibility and procedural requirements for the submittal of a Supplier Change Request to obtain an exception or change to GEH Purchase Order requirements.
2.p	Engineering Change Control	Establishes the process used to control and authorize changes to engineering controlled documents to: Assure that total impact is considered before a change is approved and that the affected documents are identified and changed as approved Provide authority for a change and identify all pertinent interfaces and organizations responsible for these interfaces Provide accurate and traceable records of a change
2.q	Field Deviation Disposition Request	Establishes a process to document and disposition the technical position for field deviations to GEH-supplied hardware, software, or services. Responsible individuals evaluate Field Deviation Disposition Requests to assure that the proposed field action meets safety, technical, quality, application and commercial requirements.

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	**Document Title**	**Abstract**
2.r	Change Control Board	Defines the requirements and procedures applicable to the operation of a Change Control Board that is responsible for reviewing proposed changes to design or product configuration documents. Establishment of a Change Control Board and application of this procedure are at the discretion of project management for any particular project or group of projects.
2.s	Quality Record Computer Data	Prescribes the requirements, procedures, and responsibilities for the control, retention, and retrieval of quality record computer-based data maintained within the central computing facility of GEH. It includes, but is not restricted to, textual data, computer databases, computer program source data, and binary computer programs.
2.t	Safety-Related Classification	Defines the requirements used to identify structures, systems, components, parts, and technical services that are safety-related. Safety-related structures, systems, components, and parts provide safety-related functions necessary to assure: The integrity of the reactor coolant pressure boundary; or The capability to shut down the reactor and maintain it in a safe shutdown condition; or The capability to prevent or mitigate the consequences of accidents that could result in potential off site exposures comparable to 10 CFR 50.34(a)(1) or 10 CFR 100.11 guideline exposures, as applicable.
2.u	Dedication of Commercial Grade Items	Establishes the requirements and responsibilities for dedicating commercial grade items procured for use in safety-related applications.

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	**Document Title**	**Abstract**
2.v	Corrective Action Process	Specifies the responsibilities for actions to promptly identify, record, and correct Conditions Adverse to Quality to assure that these conditions do not affect the quality of products or services. Defines the requirements and responsibilities for conducting ongoing self assessments, focused self assessments, and internal audits of organizations within GEH.
2.w	Control of Nonconforming Material	Describes the methods by which nonconforming material is documented and controlled at GEH.
2.x	Quality and Technical Training	Defines the roles and responsibilities to assure personnel proficiency in quality and technical related activities. The Quality and Technical Training program: Ensures personnel are trained and proficient in assigned quality and technical tasks. Documents qualifications for technical positions, including minimum education, experience, and any special training requirements. Records training assignments in a centralized controlled training database.
3.a	Project Risk Management Procedure	Implements the project risk management requirements of GEH Policy. Provides a controlled process for risk management to maintain positive control of work situations, especially during critical tasks or activities.
3.b	Project Management Policy	Provides requirements for the single Project Management process across all GEH. The process components include project initiation, planning, scheduling, execution, controls, and post-delivery closeout.
3.c	Quality Policy and Quality System Requirements	Establishes the requirements of the GEH business quality system. Defines requirements necessary to implement the quality policy and to demonstrate, by performance both inside and outside GEH, total dedication to the attainment of quality leadership and customer satisfaction.

GE Hitachi Nuclear Energy Procedures and Policies		
Reference Number	**Document Title**	**Abstract**
3.d	Nuclear Energy Quality Assurance Audit Requirements	Establishes the requirements and processes for a comprehensive audit program to verify the implementation and effectiveness of the GEH Quality System. The audit program requirements apply to hardware, software and service products and to all personnel who perform quality-related activities on them.
3.e	Reporting of Defects and Noncompliance Under 10 CFR Part 21	Defines the requirements and responsibilities within GEH for ensuring compliance with the requirements of 10 CFR 21, "Reporting of Defects and Noncompliance."

Reference Number	Document Title	Document Number
4.	Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications	EPRI TR-106439

2.4 ADDITIONAL IEEE STANDARD GUIDANCE

The following IEEE Standards provide additional guidance for the implementation activities. Conformance of this plan to these activities has been evaluated. Selected sections/topics from these IEEE Standards are excluded from commitment because either they provide conflicting requirements with other Standards or the level of detail is not appropriate for this plan. Clarifications and justifications for such exclusions are provided in Appendix A.

- IEEE 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology
- IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans
- IEEE 1016-1998, IEEE Recommended Practice for Software Design Descriptions
- IEEE 1058.1-1987, IEEE Standard for Software Project Management Plans
- IEEE 1219-1998, IEEE Standard for Software Maintenance
- IEEE 1228-1994, IEEE Standard for Software Safety Plans
- IEEE 12207-1996, IEEE/Electronic Industries Alliance (EIA) Standard for Software Life Cycle Processes

2.5 INTERNATIONAL STANDARDS

- International Standards Organization (ISO) 9001:2000, Quality Management Systems - Requirements

3. SOFTWARE QUALITY ASSURANCE PLAN

3.1 PURPOSE AND SCOPE

The purpose of this Software Quality Assurance Plan (SQAP) is to define the management organization, techniques, procedures, and methodologies used to assure the delivery of software meets specified requirements for the I&C Systems. The use of this SQAP will help assure the following:

- That software development, evaluation and acceptance standards, are implemented, documented, and followed.
- That the results of software quality reviews and audits will be given to appropriate management within the scope of the SQAPM. This provides feedback as to how the development effort conformed to development standards.
- That test results adhere to acceptance standards in Section 7.0.

3.2 MANAGEMENT ORGANIZATION

3.2.1 Organization

This subsection defines the functional responsibilities and authorities of the Project organizations that are responsible for the quality of the software products.

The Quality organization is responsible for GEH 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 GEH, provides leadership for development 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 executing the technical aspects of the SQA program, which includes the following SQA tasks (hereafter referred to as quality tasks):

- Independent Verification and Validation (IV&V) of Software Class Q software
- Software Safety Analysis (SSA)
- Software Configuration Management (SCM)

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

3.2.2 Activities

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

- Independent Verification and Validation (IV&V) of design documentation and outputs for Class Q software specified in the SMPM [2.3(1.a)]
- Verification and Validation (V&V) of design documentation and outputs for Class N3 and N2 software specified in the SMPM [2.3(1.a)]
- Safety analysis of Software Class Q software and Software Class N3 software

- Software and system testing
- Baseline reviews
- Configuration control
- Audits

Table 9-2 outlines the tasks and the individual or group responsible for conducting these tasks during the design and development of the software products.

3.2.3 Qualification and Responsibilities

The SQA Manager shall be knowledgeable in the industry standard QA methodologies and proficient in establishing, maintaining, and improving SQA Procedures and experience in technical project management. The SPE members shall be knowledgeable in the technologies and methods used in design development and are qualified to perform the specific software quality tasks.

[[

]]

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

Figure 2. (Deleted)

3.2.3.1 Software Quality Assurance Manager

The SQA Manager, who interfaces with the SPE Manager, has the overall responsibility and authority of the SQA Program. The SQA Manager is responsible for:

- Approving this SQAPM
- Approving the validated software
- Issuing stop work order if the audit or assessment findings indicate violation of the quality and/or safety requirements
- Organizing the software auditing activities and maintaining the software audit plan
- Participating in baseline reviews
- Scheduling and coordinating software audits (both internally and externally) with the New Plant Project (NPP) Quality Team and/or the Nuclear Quality Assurance Team to ensure effectiveness of the audit being conducted
- Reporting audit results to the responsible project leadership (e.g., SPE Manager, Engineering Manager, Project Management Team) and the Quality Manager

3.2.3.2 New Plant Project Quality Manager

The New Plant Project (NPP) Quality Manager has the overall responsibility and authority of the Quality Program for New Units Engineering. The NPP Quality Manager shall coordinate with the SQA Manager concerning the audit of the software products. The NPP Quality Manager is responsible for:

- Quality assurance requirements for the design and production of the software products. This includes but is not limited to:
  - Hardware production
  - Hardware qualification
  - Shipping and packaging
  - Final product quality certification
  - Release for shipping approval
- Organization of the auditing activities and maintenance of the audit plan
- Ensuring independence of the SQA and SPE Organizations from the Design Organization.

The NPP Quality Manager shall either reserve authority, or shall formally designate a Quality Control Engineer (QCE) to reject or order stop work when such action is deemed necessary to assure the quality or safety of the software product.

The NPP Quality Manager is also responsible for assuring that adequate resources are available to support the QA program and quality initiatives for improvement of processes for product and service offerings including:

- Reporting to top management on the performance of the quality assurance system
- Ensuring the promotion of awareness of quality requirements throughout the organization

3.2.3.3 I&C Design Engineering Manager

The I&C Design Engineering organization, hereafter referred to as the Design Team, is described in the SMPM [2.3(1.a)]. The I&C Manager has the overall responsibility to ensure the design and development of the software products are performed in accordance with the SMPM [2.3(1.a)] and the required GEH procedures and policies. This includes the approval of the design documentation, timely and effective control of work in process, and the quality of delivered software products.

3.2.3.4 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 responsible for executing the quality tasks described in this SQAP (Subsection 3.2.2). A Task Lead is assigned by the SPE Manager to lead each of the following SPE teams:

- Independent Verification and Validation Team (IVVT, Software Class Q)

- Software Safety Team (SST, Software Class Q and N3)
- Baseline Review Team (BRT, Software Class Q, N3 and N2)

3.2.3.4.1 SPE Manager

The SPE Manager has the overall responsibility and authority for the implementation of the quality tasks during the software life cycle. The SPE Manager is responsible for:

- Coordinating with the SQA Manager in organizing the quality tasks
- Approving the IV&V, SSA, or baseline review outputs and documentation
- Rejecting the design outputs and documentation, as recommended by the Task Lead(s), if serious defects are identified during SSA and/or IV&V (e.g., the requirements and/or design are incomplete, inconsistent, and not traceable to upper-level documents)
- Staffing of BRT, SST, and IVVT
- Appointing the Task Lead to BRT, SST, and IVVT
- Communicating open issues to Engineering organizations and the Project Management Team, and Quality Manager
- The overall management, including schedule and budget of SPE, to ensure continued effectiveness and support of the quality tasks described in this SQAPM

3.2.3.4.2 Independent Verification & Validation Team

The IVVT is responsible for performing and managing IV&V tasks on the Software Class Q design documentation and design outputs to:

- Ensure the design meets the specified requirements
- Confirm the quality, safety, reliability, availability, maintainability, testability, security, and performance of the design
- Ensure the software products meet their intended use and do not perform unintended functions

The IVVT Task Lead is responsible for:

- Organizing the IV&V tasks and coordinating the IV&V schedule with the Design Team
- Assigning IV&V tasks to IVVT members
- Managing the conduct of IV&V tasks, and reviewing and approving the IV&V reports prepared by IVVT members
- Ensuring that the IV&V is performed in accordance with the SVVP described in Section 5.0

3.2.3.4.3 Baseline Review Team

The BRT is responsible for performing the baseline review to assess the adequacy of the software design process and control of configuration items (CIs) in accordance with the Software

Configuration Management Plan (SCMP) (Section 6.0). The BRT shall issue a Baseline Review Record (BRR) for each baseline review conducted.

The BRT Task Lead is responsible for:

- Coordinating and scheduling the baseline review meetings with the Design Team and the SQA Manager
- Organizing the baseline review process
- Assigning tasks to BRT members
- Managing the conduct of BRT tasks
- Ensuring that baseline review tasks and activities are performed in accordance with the SCMP described in Section 6.0
- Approving the baseline configuration items
- Coordinating the release of configuration items into the Configuration Management System (CMS)

3.2.3.4.4 Software Safety Team

The Software Safety Team (SST) is responsible for performing the SSA to assure the safety characteristics of the software products being developed, including the interface between the hardware and software. The SST has the authority to enforce safety requirements in the software requirements specification (SRS), the design, and the implementation of the software.

The SST is responsible for determining the Software Class (described in Section 1.5, Software Classification) of the software and performing SSA. The SST shall coordinate with the IVVT to evaluate the V&V efforts to determine if SSA can be used as a verification method.

The SST Task Lead is responsible for:

- Overseeing the overall conduct of the software safety program
- Organizing the software safety program and coordinating the SSA schedule with the IVVT and the Design Team
- Approving the SSA for Software Class Q and N3 software
- Assigning tasks to SST members
- Managing the conduct of SST tasks and approving SSA reports prepared by SST members
- Ensuring that SSA is performed in accordance with the SSP described in Section 4.0

3.2.3.5 Configuration Management Manager

The Configuration Management Manager (CMM) has the overall responsibility and authority for the CMS. CMM is responsible for defining the configuration management process and tools, as well as execution of the CMS to maintain and control traceable records of:

- Design Requirements and Inputs

- Design Activities
- Design Outputs
- Change Requests

3.2.3.6 Design Team

The Design Team is responsible for the design and implementation of the software products and the verification and validation of Software Class N3 and N2 software products. (The IVVT is responsible for the verification and validation of Software Class Q software products, and their independent verification and validation is described in section 5.) The responsible verifiers and testers shall be individual(s) or a group of individuals who are competent to perform verification and validation based on knowledge and experience. The V&V of Software Class N3 and N2 software products shall be conducted by qualified individual(s) or a group of individuals other than those who performed the design and development of the software product. These individuals may be from the Design organization, independent Software Project Engineering (SPE) or another independent third party which meets the requirements to perform the activity.

The independence criteria for V&V of Software Class N3 and N2 software products are defined in Independent Design Verification [2.3(2.i)]. The roles and responsibilities of the Design Team are described in the SMPM [2.3(1.a)].

3.2.4 Organizational Interfaces

The NPP Project Managers (PMs) are responsible for the commercial aspects of the software project. The detailed responsibility of the PM is described in the SMPM [2.3(1.a)].

The SQA Manager, with support of the NPP Quality Team, shall perform SQA audits on the external vendor organizations prior to contract agreement (Subsection 3.9.1, Vendor Control). Vendors responsible for producing software products within the scope of the SQAPM shall be in compliance with the requirements specified in this SQAPM and the regulatory requirements described in the SMPM [2.3(1.a)].

3.2.5 Scheduling and Planning

The SPE and SQA Managers have the overall responsibility for scheduling and planning the tasks and activities described in this SQAPM. The Task Lead for each team (SST, IVVT, and BRT) is responsible for the management and planning activities for their respective teams. The Task Leads shall coordinate with the Design Teams concerning the timely receipt of design documentation to support the quality tasks (SSA, IV&V, Baseline Review [BR], and software audit).

Schedule and project planning shall be documented in a Project Work Plan (PWP) in accordance with Work Planning and Scheduling [2.3(2.a)]. Each Task Lead is responsible for the preparation of a task-specific PWP.

While a cross-functional team performs the quality tasks, a project workflow shall be established to ensure the required tasks are accurately identified and the quality tasks schedule is aligned with the established integrated project schedule and milestones. The schedule shall:

- Cover the duration of the quality tasks

- Contain the major milestones of the project related to the quality tasks
- Include the sequence and dependencies of the quality tasks and the relationship of key quality tasks to project milestones
- Express milestones as absolute dates

3.2.6 Approval Authority

The NPP Quality Manager, the SQA Manager, and the SPE Manager have approval authority for functions within their responsibility.

Upon the rejection of a software product or the issuance of a stop work order, corrective actions shall be established that 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 shall be required to complete the corrective actions and identify preventive actions to avert the occurrence of similar defects.

3.3 DOCUMENTATION

The SMPM [2.3(1.a)] establishes the managerial process and the technical direction necessary to govern the design and development activities of the software products. The required design documents and design outputs to be prepared are defined in the SMPM [2.3(1.a)].

Tables 9-1a through 9-1g present the required design and quality tasks and the associated task outputs for each software life cycle.

3.4 STANDARDS, PRACTICES, CONVENTIONS AND METRICS

3.4.1 Standards, Practices and Conventions

The applicable EOPs and P&Ps used in guiding the design and development of software products are specified in Section 2.3, Supplemental Documents. If detailed instructions are needed, project or platform/product line specific work practice instructions, such as ESBWR Project Instructions Engineering Service Instructions, or Work Instructions are prepared to provide additional instructions as required. Software audits shall be conducted to monitor compliance to the policies and procedures used to guide the design and development of software products.

Software coding shall be implemented in accordance with the guidelines defined in the Software Coding Conventions and Guidelines Document required by the SMPM [2.3(1.a)], which at a minimum, shall include:

- Documentation standards
- Logic structure standards
- Coding standards
- Commentary standards
- Secure coding practices

Code review shall validate coding compliance to the guidelines outlined in the (applicable) Software Coding Conventions and Guidelines Document.

3.4.2 Metrics

Software Metrics are sets of data that are systematically collected and analyzed 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 Class Q and N3 software products.

3.5 REVIEWS AND AUDITS

3.5.1 Reviews

3.5.1.1 Technical Review

The purpose of the technical review is for a qualified individual, or a team of qualified individuals, to determine the suitability of the intended use of a design and identify discrepancies from design inputs, codes, and standards. It ensures the following:

- The design conforms to its specifications
- The design adheres to regulations, standards, guidelines, plans, and procedures applicable to the project
- The design is complete and correct
- For a document in revision, the changes have been implemented as specified in the change request or anomaly report

Technical review may be conducted through peer review or design review.

An individual other than the design document's Responsible Engineer (RE) shall conduct peer review. A peer review is considered an informal review and cannot be used to replace independent verification. The RE shall document and disposition the review comments. The review comments shall be filed in the project Design Record File (DRF).

Design review is performed in accordance with GEH Design Review [2.3(2.e)]. For Software Class Q design documents, an SPE member shall participate in the design review. The review results shall be documented in a design review report as described in Subsection 5.4.2, Design Review Report.

3.5.1.2 Managerial Review

The SPE Manager, the SQA Manager, and the Task Leads shall review the SQA program in accordance with Procedure Quality Policy and Quality System Requirements [2.3(3.c)], to ensure its suitability, adequacy, and effectiveness. The review team shall assess opportunities for

improvement to the SQA program and re-define the quality objectives. In addition to the review inputs required by Procedure Quality Policy and Quality System Requirements [2.3(3.c)], the review includes the effectiveness of V&V, SSA, and SCM tasks to monitor compliance with the defined requirements.

The review shall be documented in the Managerial Review Report [5.4.6]. The report shall include decisions and actions needed to assure continued effectiveness of the SQA program. Maintenance of the SQAPM is described in Section 8.0, SQAPM Maintenance.

3.5.1.3 Project Closeout Review

The responsible PM shall schedule a post-delivery closeout review to:

- Close any Corrective Action Requests (CARs) associated with the project and project Design Record File (DRF)
- Set up warranty administration and review
- Conduct a Licensee closeout meeting to solicit feedback, which includes collecting lessons learned and metrics during the project.

The post delivery closeout review shall be conducted in accordance with Project Management Policy [2.3(3.b)].

3.5.2 Audits

3.5.2.1 Functional Audit

The functional audits shall be conducted to assure that the requirements specified in the System Design Specification (SDS) and Software Requirements Specification (SRS) have been met by checking the applicable Requirements Traceability Matrix (RTM). The functional audit shall be performed during baseline review by the BRT and shall be documented in the Baseline Review Record. The functional audit shall be performed for the Software Class Q software products and is recommended for Software Class N3 and N2 software products.

3.5.2.2 Physical Audit

The physical audits shall be conducted to confirm that the appropriate CI, which includes Software Build Description (SBD), has accurately and completely described the "build" parameters of the software such that a duplicate version of the object code can be recreated. The physical audit shall be performed as part of Test Phase Baseline Review by the BRT and shall be documented in the Test Phase Baseline Review Record. The physical audit shall be performed for Software Class Q software products and is recommended for Software Class N3 and N2 software products.

3.5.2.3 In-Process Audits

This SQAPM requires SQA audits to be performed on the design organizations (both internal and external). The SQA audit shall be performed to ensure compliance with the codes and standards specified in this SQAPM. The SQA audit evaluates the adequacy and completeness of the required reviews, V&V, SSA, CySA and BR activities.

Nuclear Energy Quality Assurance Audit Requirements [2.3(3.d)], establishes the requirements and processes for a comprehensive audit program. This program confirms implementation of and compliance with the GEH quality system. It also determines the adequacy and effectiveness of the quality system.

An audit report shall be prepared at the conclusion of each software audit. The audit report shall summarize the following:

- Audit activities and results
- Audit observations
- Conditions Adverse to Quality (CAQs)
- Discrepancies
- Non-compliance with quality and engineering procedures
- Recommended corrective actions

A CAR shall be initiated to manage the identified CAQs, discrepancies, and non-compliances in accordance with the procedure specified in Corrective Action Process [(2.3(2.v)].

3.6 PROBLEM REPORTING AND CORRECTIVE ACTION

3.6.1 Problem Reporting

Discrepancies, deficiencies, anomalies, deviations or comments discovered during design and development (i.e. V&V, SSA and testing), installation, post delivery, and other CAQs shall be formally documented. Table 9-3 outlines the problem reporting process, including possible scenarios, responsible individuals, and documentation of reported problems.

Defects and non-compliance under 10 CFR Part 21 shall be reported in accordance with Reporting of Defects and Non-Compliance under 10 CFR Part 21 [2.3(3.e)].

3.6.2 Corrective Action

It is essential that the processes described in this SQAPM, the SMPM [2.3(1.a)], the required EOPs, P&Ps, and Corporate QA program be adhered to. Failure to comply with these processes shall be promptly identified and action shall be taken to eliminate or correct the nonconformities or CAQs to prevent recurrence. CAQs can be:

- Discovered during work performance and audit
- Complaint from licensees
- Findings from regulatory authorities
- Other external organizations (e.g., International Standards Organization (ISO)/American Society of Mechanical Engineers (ASME) Code authorities)

[[

]]

3.7 TOOLS, TECHNIQUES AND METHODOLOGIES

3.7.1 Tools

The SPE and Design Team organizations shall employ the use of tools as needed to execute the tasks specified in this plan. If V&V is performed on the output produced by the tools each time the tools are used, then the tools used in part to perform V&V tasks do not need to be qualified.

3.7.1.1 Commitment Tracking System

The Commitment Tracking System (CTS) is used to manage and record the identified CAQs and non-compliances to the established quality procedures, such as EOPs, P&Ps, and this SQAPM as defined in Section 2.0.

3.7.1.2 Checklist

A checklist may be used to support inspection, V&V, independent verification and software audits to ensure completeness of the design output being verified or inspected, and the process being audited. The checklists prepared to support software inspection, V&V and independent verification should include acceptance criteria for the design output. The NUREG 0800, SRP [2.2.1] divides the acceptance criteria into two sets:

- Functional characteristics (accuracy, functionality, reliability, robustness, safety, security, or timing). Not all characteristics occur for every design output.
- Process characteristics (completeness, consistency, correctness, style, traceability, un-ambiguity, or verifiability). Not all characteristics occur for every design output.

Software audits are conducted to independently evaluate the design team's compliance with the SQA requirements specified in this SQAPM and other applicable standards, regulations, guidelines, and procedures. The checklists prepared to support software audits should include queries to demonstrate compliance with the SQA requirements specified in this SQAPM and other applicable standards, regulations, guidelines, and procedures.

3.7.1.3 Requirements Traceability Matrix

The Design team is responsible for the preparation of Requirements Traceability Matrix (RTM). RTM can be prepared manually or using an automated tool.

The traceability matrix shall clearly show the linkage between each requirement imposed on the software by the input documents. The matrix shall allow traceability in both directions. It shall be updated at the completion of each software life cycle phase. The final matrix shall permit tracing from the system requirements through the software requirements, design, implementation, testing, and installation. Figure 3 shows an example of a traceability matrix structure.

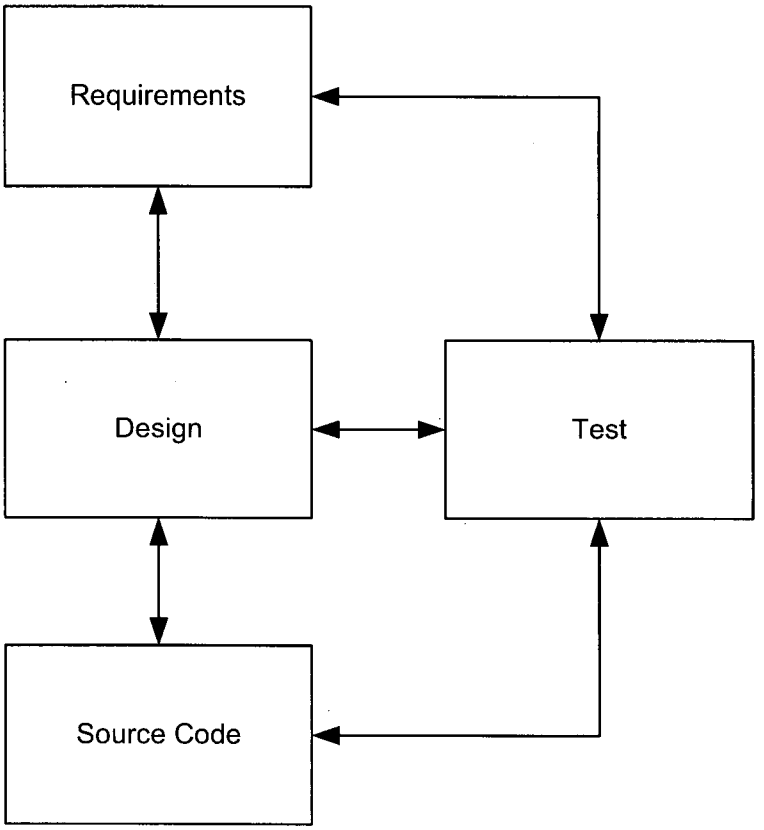

Figure 3. Example of A Traceability Matrix Structure

3.7.1.4 Product Data Management System

The Product Data Management System (PDMS) [2.3(2.b)] is an access-controlled, computer-based data storage and retrieval system that is used to manage data relevant to the engineering definition of products and services, including quality records. Previous and current revisions of the engineering documents that have been approved for issue are maintained within the system. Roles, responsibilities and procedures are defined within PDMS [2.3(2.b)].

PDMS is the GEH-official CMS for engineering and quality controlled documents. Internal and external vendors providing the software products are not required to utilize PDMS [2.3(2.b)]. However, an appropriate computer-based CMS shall be used.

3.7.1.5 Design Record File

A Design Record File (DRF) is the formal controlled information record for engineering work. DRF records include the following:

- Design of systems, hardware and software
- Performance of analyses, evaluations, calculations
- Documentation from licensing services

A DRF is an in-progress record, subject to change, that is contained in the PDMS until it becomes a permanent Quality Assurance record. A DRF shall be generated and maintained in accordance with Design Record File, [2.3(2.g)].

3.7.1.6 Discrepancy Tracking System

A Discrepancy Tracking System (DTS) will be initiated to manage and track the anomalies identified during software testing. The software tests included will be the Software Validation Test (SVT), System Factory Acceptance Test (SFAT), [[
]] and Site Acceptance Test (SAT) (if SAT is within GEH scope of responsibility). Information that will allow the RE to evaluate the anomaly shall be included in the Discrepancy Tracking System. This information includes:

- Name and Master Parts List (MPL) of the software product
- Project / Plant
- Software Classification
- Description of the anomaly, including effect and extent of the anomaly, clear explanation of observations, symptoms, workarounds, and any other pertinent information
- Severity of the anomaly
- Initiation date
- Affected documentation
- Affected design organization
- Corrective action and resolution statement
- Completion and approval status

If needed, reports can be generated to:

- Facilitate and monitor the anomaly disposition efforts
- Ensure that the required changes to the affected design documentation and output have been completed
- Support baseline review and management review efforts

3.7.2 Techniques and Methodologies

Techniques and methodologies used to support the quality tasks are described in the SVVP (Section 5.0), SSP (Section 4.0), SCMP (Section 6.0), and STP (Section 7.0).

3.8 CODE AND MEDIA CONTROL

The computer-based design outputs, such as software source code, Commercial Off-the-Shelf (COTS) software, support software, and software tools used to support the design and development of software products are CIs; and, as such, shall be controlled as specified in the SCMP (Section 6.0).

3.9 VENDOR AND ACQUIRED SOFTWARE CONTROL

3.9.1 Vendor Control

Vendor selection and qualification shall be performed under a prescribed process. At a minimum, the following requirements shall be evaluated:

- Ability to meet engineering, quality, and purchasing requirements
- Relevant experience in the design and development of similar products
- Awareness of and compliance with the applicable regulatory and industrial requirements
- Service, installation, and support capability and history of performance

Confirmation of this ability is determined by audit of the vendor's Quality Management System, including the Quality Assurance Program. The IVVT shall support the SQA Manager during vendor audit.

[[

]]

3.9.2 Commercial Off-the-Shelf Software

Commercial Off-the-Shelf (COTS) software is software commercially available to the public. COTS software includes communication protocol applications and linkable software libraries. It is acceptable that the qualified and dedicated COTS software be used in the Software Class Q software products. The SMPM [2.3(1.a)] describes the qualification and dedication of COTS software.

3.9.3 Previously Developed Software

Previously Developed Software (PDS) is software developed for prior projects and not necessarily verified and validated per the requirements outlined in this SQAPM. The IVVT shall independently verify and validate the PDS evaluation report prepared by the Design Team for software intended for use in Class Q software. The SMPM [2.3(1.a)] describes the evaluation of PDS.

3.10 RECORDS COLLECTION, MAINTENANCE, AND RETENTION

Section 6.8, Record Collection and Retention describes the collection, maintenance, and retention of design documentation, design outputs, and quality records, such as audit reports, SSA reports, and test reports.

3.11 TRAINING

Personnel supporting the quality tasks shall be trained, as necessary, to ensure proficiency in applicable quality and technical tasks prior to the assignment of work activities affecting the quality of software products as required by Quality and Technical Training [2.3(2.x)]. The Design Team and the SPE teams shall be trained, either by self-study or classroom, this SQAPM, the SMPM [2.3(1.a)], applicable tools required to support the design and quality tasks, and the referenced EOPs and P&Ps. The training records shall be maintained in the training database.

3.12 RISK MANAGEMENT

Risk Management is the process of identifying, controlling, and eliminating or mitigating unpredictable events that may affect the project.

Risk Management shall be implemented in accordance with Project Risk Management Procedure [2.3(3.a)].

The Task Leads shall prepare a risk management plan to document responsibilities and actions needed to assess, abate, monitor, and control the identified risks. It is acceptable that the risk management plan be included in the task-specific PWP.

4. SOFTWARE SAFETY PLAN

4.1 PURPOSE AND SCOPE

This Software Safety Plan (SSP) establishes the processes and activities 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, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants [2.2.3]. This SSP meets the guidelines specified in Chapter 7 of NUREG 0800 SRP [2.2.1] and the requirements outlined in Section 4.4 of IEEE Std. 1228, "IEEE Standard for Software Safety Plans" [2.4].

Software Safety Analysis (SSA) is performed on the software for Software Class Q and N3 software products.

Safety critical software is defined as any software for Software Class Q and N3 software products.

4.2 SOFTWARE SAFETY MANAGEMENT

4.2.1 Organization and Responsibilities

SQAPM Subsection 3.2.1 describes the organizational responsibilities in supporting the SSA activities. The roles and responsibilities of the Software Safety Team (SST) are described in SQAPM Subsection 3.2.3.4.4.

The SPE Manager and the SST Task Lead have responsibility for the completion of SSA activities:

- Prepare the SSA plan
- Obtain and allocate resources to ensure effective implementation of the SSP including budgeting, qualified personnel, and suitable training or continuing education to keep personnel current
- Coordinate safety task planning with other organizational components or functions, such as development, system safety, software quality assurance, software reliability, software configuration management, V&V, and software testing
- Coordinate software safety tasks within the overall context of the system safety program
- Coordinate technical issues related to software safety with other components of the development and support organization, with the project sponsor, or with the licensee
- Ensure that required records are retained to document the conduct of software safety activities
- Participate in audits of the implementation of the SSP
- Ensure training of safety personnel in methods, tools, and techniques used in software safety analyses
- Ensure that the deviations and discrepancies are identified, documented and dispositioned by the Design Team

4.2.2 Qualifications and Training

Personnel assigned specific responsibilities for SSA shall meet the qualifications and on-going training as defined in SQAPM Subsection 3.2.3.

4.2.3 Software Life Cycle

The software safety process shall be integrated into the software life cycle process defined in SMPM [2.3 (1.a)] Section 5.3, Organization of Software Life Cycle Process.

4.2.4 Documentation Requirements

This Subsection of the SSP specifies the documentation to be prepared and its contents. The list below delineates the requirements for documentation of safety-critical software.

- Software Project Management. Documentation of how the software safety program is implemented, integrated, and managed with the software development activities is discussed in this SQAPM and in the SMPM [2.3(1.a)].
- Software Configuration Management. Information regarding the CM of the design documentation and design outputs (including safety-critical design documents and design outputs for Class Q and N3) is specified in Section 6.0, Software Configuration Management Plan.
- Software Quality Assurance. Information regarding the SQA of Software Class Q and N3 design documentation and design outputs is specified in Section 3.0 of this SQAPM.
- Software Safety Requirements. Specification of safety-critical requirements to be implemented by the software to avoid or control system hazards are documented in the requirements documentation as specified in the SMPM [2.3(1.a)], Section 5.7.
- Software Safety Design. The design descriptions for safety-critical elements are specified in the SMPM [2.3(1.a)], Section 5.8.
- Software development methodology, standards, practices, metrics, and conventions. Approved and controlled practices that are essential to satisfy system and software safety objectives and requirements are specified in the SMPM [2.3(1.a)] Subsection 5.8.3.3, Software Coding Conventions and Guidelines Document.
- Test Documentation. Test planning, test design, test cases, test procedures, and test reports for the SVT, SFAT, [[ ]] and SAT are specified in Section 7.7, Test Documentation. Tests produced for testing and verification of safety-critical elements do not need to be separate or isolated from other tests and may be included as part of the other tests. Portions of tests related to safety-critical elements shall be identified as such.
- Software IV&V. Information regarding how software safety-critical requirements will be verified and validated is defined in Section 5.0, Software V&V Plan. The software safety analyses are specified in this SSP. The Requirements Traceability Analysis (RTA) (Subsection 5.2.6.2.6) is used to ensure the traceability of requirements to the design specifications, software source code, and software safety test cases.
- Reporting Software IV&V Activities. Information documenting the results of software IV&V activities is specified in Section 5.4, Verification and Validation Reporting.

- Software User Documentation. Information that is significant to the safe installation, use, maintenance, and retirement of the software product is specified in the SMPM [2.3(1.a)] Section 8.0, Software Operations and Maintenance Plan.
- Results of Software Safety Requirements Analysis. The reporting requirements for this activity are specified in Subsection 4.3.1, Software Safety Requirements Analysis.
- Results of Software Safety Design Analysis. The reporting requirements for this activity are specified in Subsection 4.3.2, Software Safety Design Analysis.
- Results of Software Safety Code Evaluation. The reporting requirements for this activity, including software functional testing, are specified in Subsection 4.3.3, Software Safety Code Analysis.
- Results of Software Safety Test Analysis. The reporting requirements for this activity are specified in Subsection 4.3.4, Software Safety Test Analysis.
- Results of Software Safety Change Analysis. The reporting requirements for this activity are specified in Subsection 4.3.6, Software Safety Change Analysis.
- Results of Deviations and Discrepancies. Deviations and discrepancies identified during performance of software safety activities shall be documented and dispositioned prior to proceeding in accordance with Problem Reporting and Corrective Actions described in Subsection 3.6 of this SQAPM.

4.2.5 Software Safety Program Records

Records of software safety program activities shall be generated and maintained in accordance with SQAPM Section 6.8, Records Collection, Maintenance and Retention. Software safety records include the following:

- Results of analyses, including V&V, performed on requirements, design, code, test, and other technical documentation.
- Information on suspected or confirmed safety problems in the pre-release or installed software product
- Results of audits performed on software safety program tasks.
- Results of tests conducted on any safety-critical software modules, components or system.
- A record of training provided to software safety program personnel.
- Results of any certifications performed.
- Results of deviations and discrepancies.

The Software Safety Analysis Report shall be prepared to document the following:

- Name and Description of the Software Evaluated.
- System.
- Software Classification.

- Purpose and Scope.
- Reference Inputs.
- Software Safety Analysis Body of Report.
  - Results of Software Safety Requirements Analysis. The reporting requirements for this activity are specified in Subsection 4.3.2, Software Safety Requirements Analysis.
  - Results of Software Safety Design Analysis. The reporting requirements for this activity are specified in Subsection 4.3.3, Software Safety Design Analysis.
  - Results of Software Safety Code Evaluation. The reporting requirements for this activity, including software functional testing, are specified in Subsection 4.3.4, Software Safety Code Analysis.
  - Results of Software Safety Test Analysis. The reporting requirements for this activity are specified in Subsection 4.3.5, Software Safety Change Analysis.

Results of Deviations and Discrepancies. Deviations and discrepancies identified during performance of software safety analyses shall be documented and dispositioned in accordance with Problem Reporting and Corrective Actions in Section 3.6 of this SQAPM.

This documentation and disposition shall include:

- Anomalies noted
- Conclusion
- Responsible engineer
- Approving authority

The report shall be placed under the configuration control as defined in Section 6.0, Software Configuration Management Plan.

The Requirements Traceability Matrix (RTM) shall be utilized as the tracking system to ensure that hazards, their responsibility assignment, and their status can be tracked throughout the software life cycle through retirement.

4.2.6 Software Configuration Management Activities

Software Configuration Management for safety-critical software shall be in force during all phases of the software life cycle and shall be accomplished in accordance with SQAPM Section 6.0, Software Configuration Management Plan. Configuration Management includes control of safety-critical element related design documentation, source code, object code, data, development tools, environments (both hardware and software), and test documentation.

Applicability of Configuration Management provisions ensures that additional requirements necessary for safety-critical elements are met for the following:

- Software development tools
- Previously developed software
- Vendor provided software

- Subcontractor-developed software
- V&V and SSA tools

Safety critical software is defined as any software for Software Class Q and N3 software products.

4.2.7 Software Quality Assurance Activities

Software Quality Assurance activities, as described in this SQAPM, shall assure proper performance of software safety program activities. Software Quality Assurance activities shall include, at a minimum:

- The Software Safety Plan is prepared, approved, implemented, changed, and made consistent with the SQAPM in accordance with Section 4.10.
- The technical recommendations resulting from software safety tasks are reviewed, considered by change control authority, and, where appropriate, implemented.
- The reviews and audits shall address software safety concerns, requirements, guidelines, and process certification.
- The conduct of the software safety program shall be monitored.

4.2.8 Software V&V

Software V&V activities are specified in SQAPM Section 5.0, Software Verification and Validation Plan. The results of each life cycle phase will be matched against the system safety requirements and system hazard analysis to ensure:

- System safety requirements have been satisfied within the software life cycle phases
- No additional hazards have been introduced by the work done during the software life cycle activity

4.2.9 Tool Support and Approval

Software tools used in the development and evaluation of Software Class Q and N3 software shall be evaluated for suitability as specified in the SMPM [2.3(1.a)]. Configuration control of software tools is managed in accordance with the requirements of the SCMP (Section 6.0).

To lessen the possibility of inadvertent introduction of software hazards by software tools, the following areas shall be addressed in the SMPM [2.3(1.a)]:

- Tool approval for use on the project
- Installation of upgrades to previously approved tools
- Withdrawal of a previously approved tool
- Identification of limitation that may be imposed on tool use

The SST shall confirm that the Software Support Tool Documentation Package addresses tool approval, upgrade installation to an approved tool, approved tool withdrawal and identification of limitation on tool use.

4.2.10 Previously Developed or Purchased Software

Previously developed software (PDS) or commercial off-the-shelf (COTS) software that 1) can be qualified, 2) presents acceptable risk, or 3) remains safe in the context of its planned use shall be used in safety-critical software products. The inability to determine the level of risk present or the consequence of failure shall be sufficient justification for rejecting the use of the PDS or COTS software.

The SST shall evaluate the PDS or COTS Software Evaluation Report to:

- Verify the interfaces to and functionality of the PDS or COTS software that will be used in safety-critical systems
- Confirm the relevant documents that are available and determine their status
- Verify the PDS or COTS software to published specifications
- Verify the capabilities and limitations of the PDS or COTS software with respect to the project requirements are identified
- Verify the safety-critical features of the PDS or COTS software are validated using an appropriate test plan, design, cases and procedures
- Verify that a risk assessment has been conducted in the use of the PDS or COTS software and these will not result in an unacceptable level of risk

The results of this approval process shall be documented in the SSA Report. The inability to determine the level of risk present or the consequence of failure shall be sufficient justification for rejecting the use of PDS or COTS software.

4.2.11 Subcontract Management

Management of subcontractors for safety-related software shall be carried out in accordance with Vendor Control (Subsection 3.9.1). Design activities performed by a subcontractor shall be performed either in accordance with the SMPM or an alternate plan approved by GEH before the performance of the activity.

The Responsible System Engineer (RSE) shall be responsible for ensuring that hazards impacting or identified by the subcontractor are communicated to the affected organizations.

4.2.12 Process Certification

Process certification, performed to certify that the software product is produced in accordance with the SSP, is achieved through baseline reviews. Baseline reviews are described in the SVVP (SQAPM 5.2.6.2.5).

4.3 SOFTWARE SAFETY ANALYSES

The Software Safety Analysis (SSA) is performed to ensure that:

- The system safety requirements have been correctly addressed
- No additional hazards have been introduced by the work done
- Software elements that can affect safety are identified

- There is evidence that other software and system elements do not affect safety
- Safety problems and resolutions identified in these analyses are documented

4.3.1 Software Safety Preparation Analysis

Software safety analysis preparation is performed by the SST during the Planning Phase of the software life cycle to: [[

]]

4.3.2 Software Safety Requirements Analysis

Software safety requirements analysis is performed during the Requirements Phase of the software life cycle to evaluate potential errors and deficiencies in the requirements that may contribute to a hazard.

4.3.2.1 SSA Inputs, Tasks and Outputs

SSA Inputs: [[

]]

Table 4.3.2.1-1 Software Safety Requirements Analysis Tasks and Outputs

SSA Tasks	SSA Outputs
1. [[	
2.	
3.	
4.	

SSA Tasks	SSA Outputs
5.	
6.	
	]]

4.3.3 Software Safety Design Analysis

Software safety design analysis is performed during the Design Phase of the software life cycle to confirm that the safety-critical portion of the software design correctly implements the safety-critical software functional requirements identified during the Requirements Phase, and the software design introduces no new hazards.

4.3.3.1 SSA Inputs, Tasks and Outputs

SSA Inputs: [[

]]

Table 4.3.3.1-1 Software Safety Design Analysis Tasks and Outputs

SSA Tasks	SSA Outputs
1. [[	
2.	
3.	

SSA Tasks	SSA Outputs
4.	
5.	
6.	

SSA Tasks	SSA Outputs
7.	
8.	

SSA Tasks	SSA Outputs
9.	
	]]

4.3.4 Software Safety Code Analysis

Software safety code analysis is performed during the Implementation Phase of the software life cycle to confirm that the safety-critical portions of the software design are correctly implemented in the software code, and the software coding introduces no new hazards.

4.3.4.1 SSA Inputs, Tasks and Outputs

SSA Inputs: [[

]]

Table 4.3.4.1-1 Software Safety Code Analysis Tasks and Outputs

SSA Tasks	SSA Outputs
1. [[	
2.	
3.	
4.	

SSA Tasks	SSA Outputs
5.	
6.	
7.	
8.	

SSA Tasks	SSA Outputs
9.	
10.	
	]]

4.3.5 Software Safety Test Analysis

Software safety test analysis is performed to confirm that the safety-critical portions of the software design are correctly implemented in the software code, and the software coding introduces no new hazards.

4.3.5.1 SSA Inputs, Tasks and Outputs

SSA Inputs: [[

]]

Table 4.3.5.1-1 Software Safety Test Analysis Tasks and Outputs

SSA Tasks	SSA Outputs
1. [[	

SSA Tasks	SSA Outputs
2.	
3.	

SSA Tasks	SSA Outputs
4.	

SSA Tasks	SSA Outputs
5.	

SSA Tasks	SSA Outputs
6.	

SSA Tasks	SSA Outputs
7.	

SSA Tasks	SSA Outputs
8.	
9.	

SSA Tasks	SSA Outputs
10.	]]

4.3.6 Software Safety Installation Analysis

Software safety installation analysis is performed during the Installation Phase of the software life cycle to confirm safety-critical requirements have been correctly implemented and the software functions safely within its specified environment.

4.3.6.1 SSA Inputs, Tasks and Outputs

SSA Inputs: [[

]]

Table 4.3.6.1-1 Software Safety Test Analysis Tasks and Outputs

SSA Tasks	SSA Outputs
1. [[	
2.	
3.	
4.	

SSA Tasks	SSA Outputs
5.	
	]]

4.3.7 Software Safety Change Analysis

Software safety change analysis is performed as part of Baseline Change Assessment during the Operations and Maintenance (O&M) Phase of the software life cycle to identify the safety-critical design elements that are affected directly or indirectly by the change request.

4.3.7.1 SSA Inputs, Tasks and Outputs

SSA Inputs: [[

]]

Table 4.3.7.1-1 Software Safety Change Analysis Tasks and Outputs

SSA Tasks	SSA Outputs
1. [[	

SSA Tasks	SSA Outputs
2.	

SSA Tasks	SSA Outputs
3.	
4.	]]

4.4 POST DEVELOPMENT

The section of the SSP defines the requirements for training, deployment, monitoring, maintenance, and retirement of safety-critical software that are necessary to ensure the continued safety of the system after its deployment and until its orderly retirement.

4.5 TRAINING

Training shall be provided in accordance with the systematic approach to training to assure safe operation of the software product. The Software Training Plan (STrngP) is described in Section 9.0 of the SMPM [2.3(1.a)].

4.6 DEPLOYMENT

4.6.1 Installation

Installation safety analysis tasks are described in Subsection 4.3.6. Compliance with these referenced sections assures installation of the software safety product consistent with the results of the software safety analyses.

4.6.2 Startup and Transition

Prior to starting up the newly installed safety-critical software product, the anomaly report shall be reviewed and evaluated, pre-operational tests shall be conducted to demonstrate the installed software product operates as intended; and, if applicable, the required set points (e.g., trip and alarm) will be established. The pre-operational test shall be conducted in accordance with an approved Licensee test plan and procedure.

The pre-operational test is outside the scope of this SQAPM as it is usually the Licensee's responsibility. It shall be supported by qualified engineers who are knowledgeable in the installed software product and plant operation shall support it.

The Installation Plan shall address the requirements for safely starting the new software product and, if an old software product is to be replaced, for making a safe transition from the old software product to the new software product. At a minimum, the following shall be assessed for applicability and where applicable implemented:

- Fallback modes for the new software product
- Startup of backup components and subsystems
- Startup of the new software product
- Parallel operation with backups
- Parallel operation of the old software product and the new software product
- Subsystem vs. full system operation
- Switchover to full system operation
- Validation of results from the new software product
- Cross validation of results between the old software product and the new software product
- Fallback in the case of failure of the new software product, including fallback to an old software product if one exists

4.6.3 Operations Support

The Operation and Maintenance (O&M) Manual shall be provided for the software product. The O&M Manual is described in Section 8.0 of the SMPM [2.3(1.a)].

4.7 MONITORING

The Licensee is responsible for monitoring the operation of the software product. Safety concerns that are detected during operation shall be documented and reported with the plant's problem-reporting procedures.

If GEH identifies a condition that could have potential safety implications for the software product, the Licensee shall be notified in accordance with applicable procedures.

4.8 MAINTENANCE

Software maintenance is discussed in Subsection 5.12.3 of the SMPM [2.3(1.a)].

4.9 RETIREMENT AND NOTIFICATION

Retirement and notification are described in Section 5.13 of the SMPM [2.3(1.a)].

4.10 PLAN APPROVAL

The Software Safety Plan is approved as part of this SQAPM in accordance with Section 3.0.

5. SOFTWARE VERIFICATION AND VALIDATION PLAN

This Software Verification and Validation Plan (SVVP) establishes the V&V tasks for the design and development of the software products. This SVVP satisfies the requirements of RG 1.168 [2.2.3], except where specified in Appendix A. RG 1.168 endorses IEEE Std. 1012, IEEE Standard for Verification and Validation Plans [2.2.4] and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits [2.2.4].

5.1 PURPOSE AND SCOPE

5.1.1 Purpose

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

- The 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 industry and regulatory standards, and licensing commitments
- The final software product is correct, complete, accurate, and traceable to requirements specified in the design documents and outputs

The goal of this SVVP is to assure that 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.

5.1.2 Scope

This SVVP outlines the formal set of standards and processes necessary to comprehensively verify and validate Class Q, N3, and N2 software products during all phases of the software life cycle.

V&V activity is limited to software designed and developed by GEH and GEH vendors. The list of selected software to undergo V&V shall be delineated in the PWP for the software project. Qualification of COTS software is performed by the Design Team as described in Subsection 5.8.3.6 of the SMPM [2.3(1.a)].

5.2 V&V OVERVIEW

5.2.1 Organization

Section 3.2, Management Organization, describes the organization efforts in supporting the Verification and Validation (V&V) activities.

5.2.2 V&V Schedule

The V&V schedule and contingency planning to identify risks shall be documented in the IV&V Tasks PWP (Software Class Q) and the project PWP (Software Class N3 and N2).

5.2.3 Software Integrity Level Scheme

The software integrity level scheme approach is described in Section 1.5, Software Classification.

5.2.4 Resources Summary

Subsection 3.2.3.4.2, Independent Verification and Validation Team (IVVT), describes the personnel required to support IV&V activities for Software Class Q software. The Design Team is responsible for the Software Class N3 and N2 V&V activities.

Subsection 3.2.3.4.3, Baseline Review Team (BRT), describes the personnel required to support the baseline review activities.

Subsection 5.2.6, Tools, Techniques, and Methods, addresses the tools, techniques, and methods used to support the V&V activities.

5.2.5 Roles and Responsibilities

The roles and responsibilities of IVVT members are described in Subsection 3.2.3.4.2, Independent Verification and Validation Team. Subsection 3.2.3.1, SQA Manager, describes Quality Organization support in the V&V activities.

The Design Team is responsible for the Software Class N3 and N2 V&V activities. The roles and responsibilities of the Design Team are described in the SMPM [2.3(1.a)]. For Software Class Q software, the Responsible Technical Project Engineer (RTPE) shall formally notify the IVVT Task Lead via a formal project letter when a design document is ready for IV&V.

The Responsible Technical Project Engineer (RTPE) shall formally notify the BRT Task Lead via a formal project letter when a software life cycle phase is ready for baseline review.

The project letters shall be filed in the project DRF.

Table 9-2 lists the V&V tasks and the individual or group responsible for performing these tasks.

5.2.6 Tools, Techniques, and Methods

5.2.6.1 V&V Tools

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

[[

]]

5.2.6.2 Techniques and Methods

5.2.6.2.1 Verification

Verification is performed to determine whether or not the design documentation and design outputs for a given software life cycle phase fulfilled (i.e., is traceable to) the requirements established in the previous phase. This is also performed to determine if the design documentation is complete, consistent, and correct, and will support the next phase.

[[

]]

5.2.6.2.2 Code Review

Code reviews are performed to verify that the software source code implements the specified design and does so in a manner that is compliant with the guidelines outlined in the applicable Software Coding Conventions and Guidelines Document. Code review shall be performed by a qualified software engineer other than the individual who performed the code implementation.

[[

]]

5.2.6.2.3 Software Functional Test

The software functional test includes the software module test and the software integration test.

[[

]]

5.2.6.2.4 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 specified in the System Design Specification (SDS), Hardware/Software Specification (HSS), and System Requirements Specification (SyRS).

[[

]]

5.2.6.2.5 Baseline Reviews

Baseline Reviews are formal, independent evaluations of the software design and development activities performed at the completion of each software life cycle phase.

[[

]]

5.2.6.2.6 Requirements Traceability Analysis

Requirements Traceability Analysis (RTA) is performed for Software Class Q, N3 and N2 software requirements.

[[

]]

5.2.6.2.7 Audit Support

Subsection 3.5.2.3 describes the In-Process Audits.

[[

]]

5.2.6.2.8 Walk-Through

Design walk-through is a static analysis technique used during the design and development of the software product, which is used to:

- Identify possible design errors
- Identify violation of design requirements, codes, and standards
- Evaluate alternative implementation approaches

[[

]]

5.3 V&V ACTIVITIES AND TASKS

The following sections describe the V&V activities and tasks to be performed for each Software Life Cycle Phase.

[[

]]

5.3.1 Management of V&V Activities

[[

]]

- Continuous reviews of the V&V effort
- Revision of the PWP as necessary based upon updated project schedules and development status
- Coordination of the V&V tasks with the Design Team, the SST, the BRT, and the SQA Manager

The following subsection describes the Management of V&V tasks:

5.3.1.1 SVVP Generation

An SVVP is generated as a stand-alone document or incorporated it as part of the PWP for the software project in order to meet codes and standards, and in order to identify milestones, schedules and tasks for the software project. SVVP Generation Activities and Outputs are defined in Table 5.3.1.1-1.

V&V Inputs: [[

]]

Table 5.3.1.1-1 SVVP Generation V&V Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.1.2 Baseline Change Assessment

Baseline changes assessment is described in Subsection 5.5.2, Baseline Change Assessment and Task Iteration Policy.

5.3.1.3 V&V Management Review

A management review of V&V is performed to ensure:

- Correct and timely implementation of the SVVP
- Effectiveness of the V&V effort in preventing and mitigating problems

- Compliance of the V&V effort with the requirements in the SVVP
- Basis of V&V
- Acceptance and certification of the software product

V&V Management Review Activities and Outputs are defined in Table 5.3.1.3-1.

V&V Inputs: [[

]]

Table 5.3.1.3-1 V&V Management Review Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.1.4 Management and Technical Review Support

The IVVT shall provide support for management and technical reviews, including attendance at the design review and verification of timely completion of each V&V task in accordance with the schedule in the SVVP or PWP.. Management Technical Review Support Activities and Outputs are defined in Table 5.3.1.4-1.

Review Inputs: [[

]]

Table 5.3.1.4-1 Management and Technical Review Support Activities and Outputs

Activities	Outputs
1. [[ ]]	

5.3.1.5 Organizational Interfaces & Supporting Processes

The IVVT Lead shall provide organizational interfacing and support for coordination of V&V tasks with the SST, and to support SQA audits of the supplier. Organizational Interfaces and Supporting Processes Activities and Outputs are defined in Table 5.3.1.5-1.

V&V Inputs: [[ ]]

Table 5.3.1.5-1 Organizational Interfaces & Supporting Processes Activities and Outputs

Activities	Outputs
1. [[ ]]	

5.3.1.6 Acquisition Support V&V Activities (Acquisition Process)

The IVVT Task Lead shall provide IV&V support for the scoping, interface planning and requirements review of acquired software. Acquisition Support V&V Activities and Outputs are defined in Table 5.3.1.6-1.

V&V Inputs: [[ ]]

Table 5.3.1.6-1 Acquisition Support V&V Activities (Acquisition Process) and Outputs

Activities	Outputs
[[	
1.	
2.	

Activities	Outputs
3.	
	]]

5.3.2 Planning Phase V&V Activities

The following subsections describe the V&V tasks to be conducted during the Planning Phase. The organizations responsible for these tasks are specified in Table 9-2.

5.3.2.1 Concept Documentation Evaluation

Concept documentation and system requirements are evaluated in the Planning Phase for the software project. Concept Documentation Evaluation Activities and Outputs are defined in Table 5.3.2.1-1.

Evaluation Inputs: [[

]]

Table 5.3.2.1-1 Concept Documentation Evaluation Activities and Outputs

Activities	Outputs
1. [[	
2.	
3.	
	]]

5.3.2.2 Software Plans Evaluation

The software plans to be used to control the software project are evaluated in the Planning Phase to ensure that codes, standards and regulatory guidance are appropriately captured and dispositioned. Software Plans Evaluation Activities and Outputs are defined in Table 5.3.2.1-1.

Evaluation Inputs: [[

]]

Table 5.3.2.2-1 Software Plans Evaluation Activities and Outputs

Activities	Outputs
1. [[	
2.	]]

5.3.2.3 Criticality Analysis

Subsection 4.3.1.1 describes the tasks necessary to establish the classification and hazard analysis results within the Planning Phase. Review and update of the existing classification and hazard analysis results (criticality analysis) from any prior Criticality Task Report may cause previously assigned software integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired software integrity consequences are introduced by reviewing the revised software integrity levels.

5.3.2.4 Hardware, Software and User Requirements Allocation Analysis

The allocation of the hardware, software and user requirements specified in the SDS are analyzed in the Planning Phase for correctness, accuracy and completeness. Hardware, software and user requirements allocation analysis activities and outputs are defined in Table 5.3.2.4-1.

Hardware, Software and User Requirements Allocation Analysis Inputs: [[

]]

Table 5.3.2.4-1 Hardware, Software and User Requirements Allocation Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.2.5 Traceability Analysis

Requirements Traceability Analysis (RTA) is initiated in the Planning Phase to identify the system requirements (contained in the SDS and Logic Diagrams) that will be implemented

completely or partially by software, and that these requirements are traceable to the contract. The RTA results will be placed into a requirements traceability matrix (RTM) and summarized in a RTM report. RTA activities and outputs are defined in Table 5.3.2.5-1.

RTA Inputs: [[

]]

Table 5.3.2.5-1 Traceability Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.2.6 [[ ]] *and SAT Plan Generation and Evaluation*

[[ ]] and SAT Plan shall be generated to describe the test scope, approach, resources, schedules, and risks requiring contingency planning of the testing activities to ensure the software correctly implements system and software requirements in an operational environment. The test plan shall be generated in accordance with the test document purpose, format, and content specified in Section 7.0. [[ ]] and SAT Plan verification activities and outputs are defined in Table 5.3.2.6-1.

V&V Inputs: [[

]]

Table 5.3.2.6-1 [[ ]] and SAT Plan Generation Evaluation Activities and Outputs

Activities	Outputs
1. [[ ]]	

5.3.2.7 Hazard Analysis

Hazard analysis is performed on the concept documents to identify the potential hazards to and from the conceptual system. Hazard analysis activities and outputs are defined in Table 5.3.2.7-1.

Hazard Analysis Inputs: [[ ]]

Table 5.3.2.7-1 Hazard Analysis Activities and Outputs

Activities	Outputs
1. [[ ]]	

5.3.2.8 Risk Analysis

Review the hazard analysis report, contract and PWP to assess the technical and management risks and provide recommendations to eliminate, reduce, or mitigate the risks. Risk analysis activities and outputs are defined in Table 5.3.2.8-1.

Risk Analysis Inputs: [[

]]

Table 5.3.2.8-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.2.9 Acquisition V&V Activities

The acquisition V&V activities during the Planning Phase addresses the initiation, preparation of response, contract, planning, execution and control, review and evaluation, and delivery and completion activities. Acquisition V&V activities for the Planning Phase and outputs are defined in Table 5.3.2.9-1.

Table 5.3.2.9-1 Acquisition V&V Activities and Outputs

Activities	Outputs
1. [[	

Activities	Outputs
2.	]]

5.3.2.10 Configuration Management Assessment

The Configuration Management Assessment activities during the Planning Phase address baseline review of the scope of the software product, the verified design outputs, nuclear safety, technical and contractual requirements, and the placement of the SQA process. Configuration Management Assessment activities and outputs are defined in Table 5.3.2.10-1.

Configuration Management Assessment Inputs: [[

]]

Table 5.3.2.10-1 Configuration Management Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.3 Requirements Phase V&V Activities

The following subsections describe the Activities to be conducted during the Requirements Phase. The organizations responsible for these tasks are specified in Table 9-2.

5.3.3.1 Traceability Analysis

Requirements Traceability Analysis (RTA) traces the software requirements [contained in the SRS, SyRS, Data Communication Protocol Specification (DCPS), and User Interface Specification (UIS)] to system requirements (contained in the SDS and HSS), and system requirements to the software requirements. The RTA analyzes the identified relationships for correctness, consistency, completeness, and accuracy. The RTA results will be placed into a requirements traceability matrix (RTM) and summarized in a RTM report. RTA activities and outputs are defined in Table 5.3.3.1-1.

RTA Inputs: [[

]]

Table 5.3.3.1-1 Requirements Traceability Analysis Activities and Outputs

Activities	Outputs
1. [[	]]
2.	
3.	

5.3.3.2 Software Requirements Evaluation

Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, data definitions, installation, and acceptance) of the HSS, SRS, SyRS and DCPS for correctness, consistency, completeness, accuracy, readability, and testability. Requirements related to human

factors, user documentation, user operation, and user maintenance are evaluated separately, see Subsection 5.3.4.3. User Interface Specification Evaluation. Software Requirements Evaluation activities and outputs are defined in Table 5.3.3.2-1.

Software Requirements Evaluation Inputs: [[

]]

[[

]]

Table 5.3.3.2-1 Software Requirements Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

Activities	Outputs

Activities	Outputs

5.3.3.3 User Interface Specification Evaluation

Evaluate the requirements (e.g., human factors, user documentation, user operation, and user maintenance) of the User Interface Specification (UIS) for correctness, consistency, completeness, accuracy, readability, and testability. UIS Evaluation activities and outputs are defined in Table 5.3.3.3-1.

UIS Evaluation Inputs: [[

]]

Table 5.3.3.3-1 UIS Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

Activities	Outputs

Activities	Outputs

5.3.3.4 Interface Analysis

Verify and validate that the requirements for software interfaces with hardware, user, operator, and other systems are correct, consistent, complete, accurate, and testable. Interface Analysis activities and outputs are defined in Table 5.3.3.4-1.

Interface Analysis Inputs: [[

]]

Table 5.3.3.4-1 Interface Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

Activities	Outputs

5.3.3.5 Analysis Tasks and Documents

Subsection 4.3.2.1 describes the criticality analysis and the hazards analysis tasks for the Requirements Phase.

5.3.3.6 Risk Analysis

Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks. Requirements Risk Analysis Report is file with the Management Review Report. Risk analysis activities and outputs are defined in Table 5.3.3.6-1.

Analysis Inputs: [[

]]

Table 5.3.3.6-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.3.7 Configuration Management Assessment

A configuration management assessment is performed to confirm that the Configuration Management process is complete and adequate. Configuration management assessment activities and outputs are defined in Table 5.3.3.7-1.

Configuration management assessment Inputs: [[

]]

Table 5.3.3.7-1 Configuration Management Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.4 Design Phase V&V Activities

The following subsections describe the V&V tasks to be conducted during the Design Phase. Organizations responsible for these tasks are specified in Table 9-2.

5.3.4.1 Traceability Analysis

Trace design elements (SDD, SVT Design, SVT Cases, SVT Procedures, SFAT Design, SFAT Cases, SFAT Procedures, and SFAT Specifications) to requirements [SyRS, SRS, DCPS, UIS,

Intra-System Communication Protocol Specification (ISCPS)], and requirements to design elements. Analyze relationships for correctness, consistency, and completeness. Design traceability analysis activities and outputs are defined in Table 5.3.4.1-1.

Design Traceability Analysis Inputs: [[

]]

Table 5.3.4.1-1 Traceability Analysis Activities and Outputs

Activities	Outputs
1. [[	]]
2.	

Activities	Outputs
3.	
4.	

5.3.4.2 Software Design Evaluation

Evaluate the software design evaluation inputs for correctness, consistency, completeness, accuracy, readability, and testability. Software design evaluation activities and outputs are defined in Table 5.3.4.2-1.

Software Design Evaluation Inputs: [[

]]

Table 5.3.4.2-1 Software Design Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

Activities	Outputs

5.3.4.3 Test Plans Generation and Verification

Plan component V&V testing to validate that the software components (e.g., units, source code modules) correctly implement component requirements. The task criteria are 1) compliance with design requirements; 2) assessment of timing, sizing, and accuracy; 3) performance at boundaries and interfaces and under stress and error conditions; and 4) measures of requirements test coverage and software reliability and maintainability. Test Plans Generation and Verification activities and outputs are defined in Table 5.3.4.3-1.

Test Plans Generation and Verification Inputs: [[

]]

Table 5.3.4.3-1 Test Plans Generation and Verification Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.4.4 Interface Analysis

Verify and validate that the software design interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability. Interface analysis activities and outputs are defined in Table 5.3.4.4-1.

Interface Analysis Inputs: [[

]]

Table 5.3.4.4-1 Interface Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.4.5 Criticality Analysis

Subsection 4.3.3.1 describes the tasks necessary to confirm the classification and hazard analysis results from the Requirements Phase for the Design Phase. Review and update the existing classification and hazard analysis results (criticality analysis) results from the prior Criticality

Task Report using the SDD. Implementation methods and interfacing technologies may cause previously assigned software integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired software integrity consequences are introduced by reviewing the revised software integrity levels.

5.3.4.6 Risk Analysis

Review and update risk analysis using prior task reports. Risk analysis activities and outputs are defined in Table 5.3.4.6-1.

Risk analysis Inputs: [[

]]

Table 5.3.4.6-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.4.7 Configuration Management Assessment

The configuration management assessment is an audit of the software development process to ensure that the software development plans are being followed. The configuration management assessment is performed integral with the baseline review. The Configuration Management Assessment activities and outputs are defined in Table 5.3.4.7-1.

Configuration Management Assessment Inputs: [[

]]

Table 5.3.4.7-1 Configuration Management Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.5 Implementation Phase V&V Activities

The following subsections describe the V&V tasks to be conducted during the Implementation Phase. The organizations responsible for these tasks are specified in Table 9-2.

5.3.5.1 Traceability Analysis

Requirements Traceability Analysis (RTA) maps the source code components to corresponding design specifications [contained in the SDS and ISCPS]. The RTA analyzes the identified relationships for correctness, consistency and completeness. The RTA results will be placed into a requirements traceability matrix (RTM) and summarized in a RTM report. RTA activities and outputs are defined in Table 5.3.5.1-1.

RTA Inputs: [[

]]

Table 5.3.5.1-1 Traceability Analysis Activities and Outputs

Activities	Outputs
1. [[	
	]]
2.	
3.	

5.3.5.2 Source Code Components Evaluation

Evaluate the source code components (Source Code Documentation) for correctness, consistency, completeness, accuracy, readability, and testability. The Source Code and Source Code Documentation Evaluation activities and outputs are defined in Table 5.3.5.2-1.

Evaluation Inputs: [[

]]

Table 5.3.5.2-1 Source Code and Source Code Documentation Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]
2.	

Activities	Outputs
3.	
4.	

Activities	Outputs
5.	
6.	

5.3.5.3 Interface Analysis

Verify and validate the correctness, consistency, completeness, accuracy, and testability of the interfaces of the software source code with hardware, user, operator, software, and other systems. The interface analysis activities and outputs are defined in Table 5.3.5.3-1.

Interface Analysis Inputs: [[

]]

Table 5.3.5.3-1 Interface Analysis Activities and Outputs

Activities	Outputs
1. [[	]]
2.	

Activities	Outputs
3.	

5.3.5.4 Criticality Analysis

Subsection 4.3.3.1 describes the tasks necessary to confirm the classification and hazard analysis results from the Design Phase for the Implementation Phase. Review and update the existing classification and hazard analysis results (criticality analysis) results from the prior Criticality Task Report using the source code. Implementation methods and interfacing technologies may cause previously assigned software integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired software integrity consequences are introduced during software implementation by reviewing the revised software classification level.

5.3.5.5 Software Functional Test Execution

Perform software functional testing, analyze test results to validate that software correctly implements the design. Document the results as required by the Test Execution Guidelines described in SMPM [2.3(1.a)], Subsection 6.11.1.3. Software functional test activities and outputs are defined in Table 5.3.5.5-1.

SFT Inputs: [[

]]

Table 5.3.5.5-1 Software Functional Test Execution and Verification Activities and Outputs

Activities	Outputs
1. [[	

Activities	Outputs
2.	

Activities	Outputs
3.	
4.	

Activities	Outputs
5.	]]

5.3.5.6 Software Functional Test Report Verification

The Software Functional Test Report shall be verified to assure the software function test is complete, correct, accurate, and test results are traceable to the requirements and design documents. The Software Functional Test Report Verification Activities and Outputs are defined in Table 5.3.5.6-1.

V&V Inputs: [[

]]

Table 5.3.5.6-1 Software Functional Test Report Verification Activities and Outputs

Activities	Outputs
1. [[	]]

Activities	Outputs

5.3.5.7 Software Build Description Evaluation

The evaluation of the Software Build Description in the Implementation Phase assures that the software can be reproduced from modules and libraries without ambiguity. The Software Build Description Evaluation activities and outputs are defined in Table 5.3.5.7-1.

Evaluation Inputs: [[

]]

Table 5.3.5.7-1 Software Build Description Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.5.8 Software Validation and SFAT Test Design, Test Cases and Test Procedure Specifications Evaluation

The Software Validation and SFAT Test Design, Test Cases and Test Procedure Specifications shall be verified to assure these test documents are complete, correct, accurate and traceable to the system requirements. The evaluation activities and outputs are defined in Table 5.3.5.8-1.

Evaluation Inputs: [[

]]

Table 5.3.5.8-1 Software Validation and SFAT Test Design, Test Cases and Test Procedure Specifications Evaluation Activities and Outputs

Activities	Outputs
1. [[	

Activities	Outputs
	]]

5.3.5.9 Risk Analysis

Review and update risk analysis using prior task reports. Risk analysis activities and outputs are defined in Table 5.3.5.9-1.

Risk analysis Inputs: [[

]]

Table 5.3.5.9-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.5.10 Configuration Management Assessment

The configuration management assessment is an audit of the software development process to ensure that the software development plans are being followed. The configuration management assessment is performed integral with the baseline review. Configuration Management Assessment Activities and Outputs are defined in Table 5.3.5.10-1.

Configuration Management Assessment Inputs: [[

]]

Table 5.3.5.10-1 Configuration Management Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.6 Test Phase V&V Activities

The following subsections describe the V&V activities to be conducted during the Test Phase. The organizations responsible for these tasks are specified in Table 9-2.

5.3.6.1 Traceability Analysis

Trace [[ ]] test cases and procedures to requirements (SDS and Logic Diagrams), and requirements to [[ ]]. Trace Site Acceptance Test (SAT) test cases and procedures to requirements (SDS, Logic Diagrams and Contract), and requirements to SAT test cases and procedures. Analyze relationships for correctness, consistency, and completeness. Traceability analysis activities and outputs are defined in Table 5.3.6.1-1.

Traceability Analysis Inputs: [[

]]

Table 5.3.6.1-1 Traceability Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.6.2 Software Validation Test Execution

Perform Software Validation Test (SVT) using an approved test procedure to validate that the software is operational and conforms to the functional and performance requirements specified by the HSS, SyRS, SRS, UIS and DCPS. SVT activities and outputs are defined in Table 5.3.6.2-1.

Test Inputs: [[

]]

Table 5.3.6.2-1 Software Validation Test Execution Activities and Outputs

Activities	Outputs
1. [[	

Activities	Outputs
2.	]]

5.3.6.3 Software Validation Test Report Evaluation

The Software Validation Test Report shall be verified to assure the software validation test is complete, correct, accurate, and test results are traceable to the requirements documents. SVT Test Report evaluation activities and outputs are defined in Table 5.3.6.3-1.

Evaluation Inputs: [[

]]

Table 5.3.6.3-1 Software Validation Test Report Evaluation Activities and Outputs

Activities	Outputs
1. [[	

Activities	Outputs
	]]

5.3.6.4 [[ ]] *and SAT Test Design, Case and Procedure Specifications Evaluation*

Evaluate [[ ]] and SAT test documentation for correctness and completeness. The evaluation activities and outputs are defined in Table 5.3.6.4-1.

Evaluation Inputs: [[

]]

Table 5.3.6.4-1 [[ ]] and SAT Test Design, Case and Procedure Specifications Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.6.5 Hazard Analysis

Subsection 5.7.9 in SMPM [2.3(1.a)] described qualification of software support tool to ensure tool used to support testing will not inadvertently introduce new hazards. Hazard analysis shall be performed on test tool used to support testing of Class Q software. Hazard analysis activities and outputs are defined in Table 5.3.6.5-1.

Hazard Analysis Inputs: [[

]]

Table 5.3.6.5-1 Hazard Analysis Activities and Outputs

Activities	Outputs
1. [[	
2.	]]

5.3.6.6 Risk Analysis

Review and update risk analysis using prior task reports. Risk analysis activities and outputs are defined in Table 5.3.6.6-1.

Risk analysis Inputs: [[

]]

Table 5.3.6.6-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.6.7 Configuration Management Assessment

The configuration management assessment is an audit of the software development process to ensure that the software development plans are being followed. The configuration management assessment is performed integral with the baseline review. The configuration management assessment activities and outputs are defined in Table 5.3.6.7-1.

Configuration Management Assessment Inputs: [[

]]

Table 5.3.6.7-1 Configuration Management Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.6.8 Software O&M and Software Training Manual Evaluation

Evaluate Software O&M Manual and Software Training Manual for correctness, accuracy, completeness and readability. The evaluation activities and outputs are defined in Table 5.3.6.8-1.

Evaluation Inputs: [[

]]

Table 5.3.6.8-1 Software O&M and Software Training Manual Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7 Installation Phase V&V Activities

The following subsections describe the V&V tasks to be conducted during the Installation Phase. The organizations responsible for these tasks are specified in Table 9-2.

5.3.7.1 System Factory Acceptance Test Execution

Perform System Factory Acceptance Test (SFAT) using an approved test procedure to validate that the software product is operational, conformed to the functional and performance requirements specified by the SFAT Plan and performed as intended. SFAT activities and outputs are defined in Table 5.3.7.1-1.

SFAT Inputs: [[

]]

Table 5.3.7.1-1 System Factory Acceptance Test Execution Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.2 System Factory Acceptance Test Report Evaluation

The SFAT Report shall be verified to assure the software factory acceptance test is complete, correct, accurate, and test results are traceable to the requirements documents. SFAT Report evaluation activities and outputs are defined in Table 5.3.7.2-1.

Evaluation Inputs: [[

]]

Table 5.3.7.2-1 System Factory Acceptance Test Report Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.3 [[ ]] *and Site Acceptance Test Execution*

[[

]]

[[ ]] and SAT Inputs: [[

]]

Table 5.3.7.3-1 [[ ]] and Site Acceptance Test Execution Activities and Outputs

Activities	Outputs
1. [[	

]]

5.3.7.4 [[ ]] *and Site Acceptance Test Report Evaluation*

[[

]]

Evaluation Inputs: [[

]]

Table 5.3.7.4-1 [[ ]] and Site Acceptance Report Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.5 Installation Configuration Audit

Verify that the software products required to correctly install and operate the software are present in the installation package. Validated that all site dependent parameters or conditions to verify supplied values are correct. Installation configuration audit activities and outputs are defined in Table 5.3.7.5-1.

Installation Configuration Audit Inputs: [[

]]

Table 5.3.7.5-1 Installation Configuration Audit Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.6 Installation Configuration Table Generation and Evaluation

Evaluate the Installation Configuration Table for completeness, correctness, consistency, accuracy and traceability. Evaluation activities and outputs are defined in Table 5.3.7.6-1.

Evaluation Inputs: [[

]]

Table 5.3.7.6-1 Installation Configuration Table Generation and Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.7 Installation Checkout

Verify that the software and software products have been correctly installed and operate in the target environment. Installation checkout activities and outputs are defined in Table 5.3.7.7-1.

Installation Checkout Inputs: [[

]]

Table 5.3.7.7-1 Installation Checkout Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.8 Hazard Analysis and Risk Analysis

Review and update risk analysis using prior task reports. Risk analysis activities and outputs are defined in Table 5.3.7.8-1.

Risk Analysis Inputs: [[

]]

Table 5.3.7.8-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.9 Configuration Management Assessment

The configuration management assessment is an audit of the software development process to ensure that the software development plans are being followed. The configuration management assessment is performed integral with the baseline review. Configuration Management Assessment activities and outputs are defined in Table 5.3.7.9-1.

Configuration Management Assessment Inputs: [[

]]

Table 5.3.7.9-1 Configuration Management Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.7.10 V&V Final Report Generation

V&V activities and results shall be assessed at the end of the Installation Phase or at the conclusion of the V&V effort. Assessment activities and outputs are defined in Table 5.3.7.10-1.

V&V Inputs: [[

]]

Table 5.3.7.10-1 V&V Final Report Generation Activities and Outputs

Activities	Outputs
1. [[	]]
2.	

5.3.8 Operations and Maintenance Phase V&V Activities

The following subsections describe the V&V tasks to be conducted during the Operations and Maintenance Phase. The organizations responsible for these tasks are specified in Table 9-2.

5.3.8.1 Evaluation of New Constraints

New Constraints evaluation is performed as part of Baseline Change Assessment. Baseline Change Assessment is described in Subsection 5.5.2. New constraints evaluation activities and outputs are defined in Table 5.3.8.1-1.

Evaluation Inputs: [[

]]

Table 5.3.8.1-1 Evaluation of New Constraints Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.8.2 Proposed Change Assessment

Proposed change assessment is performed as part of Baseline Change Assessment. Baseline Change Assessment is described in Subsection 5.5.2. Proposed change assessment activities and outputs are defined in Table 5.3.8.2-1.

Proposed Change Assessment Inputs: [[

]]

Table 5.3.8.2-1 Proposed Change Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.8.3 SVVP Revision

Revise SVVP to incorporate new requirements needed to modify software product. SVVP revision activities and outputs are defined in Table 5.3.8.3-1.

SVVP Revision Inputs: [[

]]

Table 5.3.8.3-1 SVVP Revision Activities and Outputs

Activities	Outputs
1. [[	
2.	
3.	
4.	]]

5.3.8.4 Anomaly Evaluation

Anomalies identified during the operation of the software product are documented within the Baseline Change Assessment. Baseline Change Assessment is described in Subsection 5.5.2. Proposed change assessment activities and outputs are defined in Table 5.3.8.4-1.

Anomaly Evaluation Inputs: [[

]]

Table 5.3.8.4-1 Anomaly Evaluation Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.8.5 Regression Analysis

Regression analysis is performed to identify the extent to which the regression test is to be performed as a consequence of modifications. Regression analysis activities and outputs are defined in Table 5.3.8.5-1.

Regression Analysis Inputs: [[

]]

Table 5.3.8.5-1 Regression Analysis Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.8.6 Migration Assessment

Assess the software requirements and implementation to ensure the following topics are addressed:

- Migration requirements
- Migration tools
- Conversion of software products and data
- Security requirements
- Software archiving
- Support for the prior environment
- User notification

Migration assessment activities and outputs are defined in Table 5.3.8.6-1.

Migration Analysis Inputs: [[

]]

Table 5.3.8.6-1 Migration Assessment Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.8.7 Retirement Assessment

Assess the installation package to ensure the following topics are addressed: [[

]]

Retirement assessment activities and outputs are defined in Table 5.3.8.7-1.

Retirement Analysis Inputs: [[

]]

Table 5.3.8.7-1 Retirement Assessment Activities and Outputs

Activities	Outputs
1. [[ ]]	

5.3.8.8 Hazard Analysis and Risk Analysis

Subsection 4.3.6 describes the safety change analysis for the Operations and Maintenance (O&M) Phase.

Review and update risk analysis using prior task reports. Risk analysis activities and outputs are defined in Table 5.3.8.8-1.

Subsection 4.3.4.1 addresses the tasks necessary to verify that no inconsistent or unintentional functions are introduced during coding and that no new hazards are introduced.

Risk analysis Inputs: [[

]]

Table 5.3.8.8-1 Risk Analysis Activities and Outputs

Activities	Outputs
1. [[ ]]	

5.3.8.9 Task Iteration

Perform the V&V tasks identify during SVVP revision (see Subsection 5.3.8.3) to ensure:

- The planned changes are implemented correctly

- Documentation is complete and current
- Changes do not cause unacceptable or unintended system behaviors (see Subsection 5.3.8.5)

Iterated V&V activities and outputs are defined in Table 5.3.8.9-1.

V&V Inputs: [[

]]

Table 5.3.8.9-1 Task Iteration Activities and Outputs

Activities	Outputs
1. [[	]]

5.3.9 Acquired Software and Vendor V&V Tasks

Acquired software refers to:

- Support software tools used to support the software development and V&V activities.
- COTS software.
- Previously developed software (PDS).

5.3.9.1 Software Support Tools

[[

]]

5.3.9.2 Commercial Off The Shelf Software

COTS software is software that is commercially available to the public. It is acceptable that COTS software be used in a Software Class Q application if it is qualified and dedicated in accordance with EPRI TR-106439, Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications [2.3(4)]. Dedication of Commercial Grade Items [2.3(2.u)] provides additional guidance in dedicating commercial grade items procured for use in safety-related applications.

[[

]]

5.3.9.3 Previously Developed Software

[[

]]

5.3.9.4 Vendor Software

[[

]]

5.4 V&V REPORTING

V&V report shall be prepared at the conclusion of each V&V task to capture the V&V results and status. The control of the V&V report is described in the SCMP (Section 6.0, Software Configuration Management Plan). The following Subsections describe the V&V reports that are required by this V&V process.

5.4.1 Independent Verification Package

[[

]]

5.4.2 Design Review Report

[[

]]

5.4.3 Test Report

The test report is described in Subsection 7.7.3.

5.4.4 Anomaly Report

[[

]]

5.4.5 Baseline Review Record

[[

]]

5.4.6 Managerial Review Report

[[

]]

5.4.7 V&V Final Report

[[

]]

5.5 V&V ADMINISTRATIVE REQUIREMENTS

The Verification and Validation Administrative Requirements used in conjunction with the V&V activities are outlined in the following subsections.

5.5.1 Anomaly Resolution and Reporting

[[

]]

5.5.2 Baseline Change Assessment and Task Iteration Policy

[[

]]

5.5.3 Deviation Policy

[[

]]

5.5.4 Control Procedures

The V&V activities records are configured, protected, and maintained in accordance with the procedures described in Section 6.0, Software Configuration Management Plan.

5.5.5 Standards, Practices, and Conventions

The standards, practices, and conventions that govern this SVVP are specified in Section 3.4. Additional standards, practices, and conventions for a project as required by contract shall be stated in the project-specific PWP and documented in the DRF.

5.5.6 Test Documentation Requirements

The purpose, format, and content of the test documents used to support the V&V are specified in Section 7.0, Software Test Plan.

6. SOFTWARE CONFIGURATION MANAGEMENT PLAN

6.1 PURPOSE AND SCOPE

This Software Configuration Management Plan (SCMP) establishes the Software Configuration Management (SCM) activities during the design and development of the software products. This SCMP satisfies the requirements of RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants [2.2.3], except where specified in Appendix A. RG 1.169 endorses IEEE Std. 828, IEEE Standard for SCM Plans [2.2.4]. This SCMP also complies with the planning requirements of IEEE 1042 [2.2.4].

6.1.1 Purpose

The intent of this SCMP is to provide additional guidance and direction necessary to implement the SCM activities required throughout the software product life cycle. This SCMP supplements GEH 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 shall remain in effect throughout the software life cycle.

6.1.2 Scope

The scope of SCMP includes the following:

- Describes the individual with the overall responsibility and authority for the SCM and organizations responsible for supporting the SCM activities.
- Defines the SCM tasks, including methods, timing, and responsibility for the implementation of design control and design change control.
- Identifies the tools, procedures, and individuals needed to execute or support each SCM task.
- Identifies the SCM required schedule and coordination with the design activities and the Quality tasks described in this SQAPM.

6.2 SOFTWARE CONFIGURATION MANAGEMENT

6.2.1 Organization

The hierarchy of responsibility for the Software Configuration Management (SCM) activities is as follows:

- The Configuration Management Manager (CMM) has the overall responsibility and authority for the CMS, including system maintenance and enhancement.
- The BRT Task Lead has the overall responsibility of the baseline review process and the configuration control of software products.
- The Responsible Configuration Control Engineer (RCCE) is responsible for the configuration control of the design documentation and outputs related to the software product, and the maintenance of software library.

- The BRT is responsible for judging adherence to the software development process for the design documentation and/or outputs being baselined. The members of this team are appointed by the BRT Task Lead and must be independent from the design team responsible for the design documentation and/or outputs.
- The Responsible Manager is responsible for the technical scope (design and development) of the software product.
- The Responsible Engineer is responsible for a given technical item (e.g., the design and development of the documentation).

6.2.2 SCM Responsibilities

The primary responsibilities of the Configuration Management Team, under the direction of the CMM, are to support the following:

- Design control throughout the software life cycle to ensure compliance with the applicable safety and performance requirements.
- Design change control to establish the change approval criteria for change requests (as defined in Change Control Board [2.3(2.r)]).
- Engineering document management to control the project records
- Engineering document format and issuance to ensure consistency and standardization of the engineering documentation and issuance process are being used and followed.

The Change Control Board (CCB) is responsible for the evaluation of the proposed high impact modifications to the software product design or product configuration documentation. The CCB also provides recommendations, which include concurrence, rejection, modification, or hold for further investigation.

The requirements and procedures applicable to the operation of the CCB are described in Change Control Board [2.3(2.r)]).

High impact modification is a change that affects one or more of the following factors:

- Safety and licensing
- System or plant performance
- Design interface (internal or external)

A detailed list of high impact changes is described in Engineering Change Control [2.3(2.p)].

The SCM responsibilities of the I&C Design Engineering Manager is to review and approve the initiation or change of design documents for Software Class Q, N3 and N2 software to confirm:

- V&V were performed by technically competent individual(s).
- Scope of review and verification per Independent Design Verification [2.3(2.i)] is complete.
- Comments made by the reviewers were adequately resolved.

The SCM responsibilities of the responsible SQA manager:

- Approve the validated software.
- Participate in Baseline Reviews.

The SCM responsibilities of the TPE are to:

- Identify the reason for the document initiation or change (i.e., error correction, regulatory or Licensee requirement, etc.).
- Determine the timing of baseline review.
- Identify the items to be baselined.
- Authorize the distribution or release of the approved software (i.e., source, object, and executable codes) to RCCE for configuration control.

The SCM responsibilities of the RE are to:

- Initiate or revise engineering controlled documentation and obtain verification in accordance with Independent Design Verification [2.3(2.i)].
- Resolve the non-conformances identified.

The responsibilities of the RCCE are to:

- Ensure the software and associated documentation are entered into the software library after the approval of the BRT.
- Release software source code/application code to the Design Team for revision or the approved software package for production.
- Coordinate software configuration control with Configuration Management Manager.
- Support baseline review as a BRT member.
- Maintain the software library.

The BRT chairperson is appointed by the BRT Task Lead. The responsibilities of the BRT chairperson are to:

- Appoint members of the BRT.
- Establish the BRT by assigning review responsibilities.
- Initiate baseline reviews.
- Chair the baseline reviews.
- Document the baseline review meeting, BRT members, and attendees. This information shall be stored in the appropriate DRF.
- Track open baseline items.

The BRT members shall have sufficient skill and experience to effectively judge the adequacy of the V&V of the CIs being baselined. The BRT Members shall be knowledgeable in the Baseline Review process. They shall be independent from the design and development of the CIs under review.

The BRT may include individuals from the Quality Organization, the Configuration Management Team, or the Design Team, who are independent of the design and development of the CI subject to baseline. The responsibilities of the BRT are to:

- Ensure that the CIs are properly identified, verified, and controlled.
- Ensure compliance with the SMP, SCMP, SVVP, and SSP.
- Review and approve the resolved nonconformance comments from baseline reviews.

The project manager is responsible for coordinating the release of design documentation to the vendor supporting the project, including the coordination of review and approval by the RE of vendor submittals, the design interface review, and control of project correspondence. Vendor Control is described in Subsection 3.9.1.

6.2.3 Applicable Policies, Procedures, and Directives

The P&Ps, EOPs, and directives applicable to the SCM activities, are specified in Section 2.3. These policies and procedures are used to supplement the process specified in this SCMP. If any external constraints are placed on the software product per contract requirements, such constraints and its impact and effect on the SCMP shall be documented in the project-specific PWP.

6.2.4 SCM Schedule

The SCM schedule that establishes the sequence and SCM tasks shall be specified in the PWP by the individuals responsible (Subsection 6.2.1) for the SCM tasks. Subsection 3.2.5 describes the scheduling and planning for the Quality tasks, including the tasks related to SCM.

6.3 SOFTWARE CONFIGURATION MANAGEMENT RESOURCES

6.3.1 SCM Tools

The following are the SCM Tools used to support the design of software products:

- Product Data Management System (PDMS) is the GEH official CMS. It is used for the creation, control, approval, storage, and retrieval of documents or data in electronic media. PDMS is described in Subsection 3.7.1.4, Product Data Management System.
- Design Record File (DRF) is a formal controlled information record under the GEH procedures for in-progress and completed engineering work which is retained and from which work can be retrieved. DRF is described in Subsection 3.7.1.5, Design Record File
- Human Factors Engineering Issue Tracking System (MMIS/HFE IP [2.1]) is a web-based database used to track:
  - Software problems, defects, or anomalies discovered during design and development (not part of V&V activities)
  - Baseline review open items
- Commitment Tracking System (Subsection 3.7.1.1) is used to track:

- Requirement violations, deviations, repeat procedural violations, and non-conformances
- Post delivery software and documentation errors and discrepancies
- Issues identified that are outside the scope of the Design Review, as defined in Design Review [2.3(2.e)]

- Discrepancy Tracking System (Subsection 3.7.1.6) is used to track anomalies identified during SFAT, [[ ]] and applicable SAT.

6.3.2 SCM Techniques

Section 6.4 identifies the SCM Tasks, the techniques and procedures used to accomplish each task, the individuals responsible for each task, and applicable tools used to support each task.

6.4 SCM TASKS

6.4.1 Configuration Identification

The CIs subject to this plan include:

- Engineering documents prepared to document the design, to communicate system requirements for software products and material, and to support the implementation and manufacturing of the software products. Engineering documents are typically issued documents. They shall be assigned a unique document identification number, revision status, quality classification, and pagination, including the total number of pages in the document.

  Document Initiation or Change by Engineering Review Memorandum/Engineering Change Notice [2.3(2.k)] establishes the requirements for the initiation or change of engineering documents by use of the Engineering Review Memorandum/Engineering Change Notice (ERM/ECN).

- Quality records such as V&V reports (Subsection 5.4), Test Reports (Subsection 7.7.8), Audit Reports (Subsection 3.5.2) and SSA Reports (Subsection 4.2.5) are prepared to document evidence of the quality of CI and/or execution of Quality tasks. These records shall be filed in the project-specific Design Record File (DRF). A DRF is the formal controlled information record used to document design activities and retain/protect completed engineering work.

  Each DRF shall be assigned a unique identification number. Design Record File [2.3(2.g)] defines the procedures to establish and maintain a DRF.

- Acquired software such as support software and software tools, COTS software, and PDS, shall be assigned a unique identification and revision number in accordance with the format described in project level documentation.

- Software, such as source code listings, objects, and executable files shall be assigned a unique file name and revision number.

  Each software module source files shall contain a header comment section, which as a minimum, shall include the quality classification and a revision status.

Upon completion of software validation testing, the RCCE or individual assigned this responsibility shall place the validated software package (such as source code, object code, executable code, and associated data files for each released revision) under configuration control in the assigned software library. The software library shall serve as the final control point and repository for the released computer-based software configuration items. Different software libraries or project-specific software libraries may be used to control the computer-based configuration items as the software products may be implemented using other control product lines or other computer platforms. Procedures shall be established to describe the retrieval and reproduction process of the controlled computer-based software CIs from library storage.

The software library structures shall have a consistent naming convention and an appropriate level of security control (e.g., password control). The security measures implemented shall provide assurance that the integrity of the baselined CI is maintained. Read and write control access to the software library accounts shall be granted to the RCCE. Personnel participating in the design and development of the software product shall only have read access to the software library. Changes to the software libraries can only be made by the RCCE.

Figure 5 shows an example of the naming convention.

- Vendor submittals shall be assigned a unique identification and revision number.

  Supplier Supporting Document Review [2.3(2.m)] defines the responsibilities and the procedural requirements for review and acceptance of design documents submitted by vendors.

  CIs shall be placed under configuration control and stored in the PDMS (Subsection 3.7.1.4). Table 9-4 contains a list of CIs, their structures, retention medium, and life cycle control points.

6.4.2 Configuration Control

6.4.2.1 Design Control

Design control measures for the software product are established to achieve the following:

- Definition of design requirements and performance of design activities in a planned, controlled, and orderly manner.
- Specification of appropriate quality requirements and standards in design documents.
- Selection of appropriate V&V methods and implementation by individuals or groups not directly responsible for the original design.

The design process performed shall be composed of the activities defined by software life cycle. The design process activities include analyses, preparation of specifications and drawings, testing, generation of test reports, and the technical support (i.e., installation and training) required to complete the design, implementation, installation, operation, and maintenance of the software products.

The design process and required design documentation are described in the SMPM [2.3(1.a)] and Design Process [2.3(2.f)]. Document Initiation or Change by Engineering Review Memorandum/Engineering Change Notice [2.3(2.k)] describes the configuration control process for initiating new or revised design documentation. The Product Data Management System (PDMS) [2.3(2.b)] is used for this purpose. PDMS is described in Subsection 3.7.1.4. V&V shall be performed for the design activities. Section 5.0 of the SVVP describes the required V&V tasks to be performed. V&V task outputs shall be retained within the project documentation in each project-specific DRF.

6.4.2.2 Design Change Control

The Design Change Control process includes change initiation, review, approval, implementation, disposition, status reporting, document updating, and distribution of I&C software. The purpose of this process is to:

- Ensure that the impact, risks and hazards are considered before a change is approved
- Ensure that the documents are identified and revised after a change is approved
- Provide authority for a change
- Identify pertinent interfaces and organizations responsible for these interfaces
- Provide accurate and traceable records of change
- Ensure a schedule for implementation of approved design changes is established

A change request may be initiated by the Licensee for product enhancement or by anyone observing a problem or error with a software product, as described below. Reasons for a proposed change are categorized in Table 6.4.2.2-1.

Table 6.4.2.2-1 Reasons for Change Request

Life Cycle Phase	Reasons
Requirements, Design, Implementation	• Design requirements • Change in regulatory requirement or codes and standards requirement • Change request from Vendor (Subsection 3.9.1 Vendor Control)
Tests	• Anomaly or error correction during V&V and testing, • Change request from Vendor (Subsection 3.9.1 Vendor Control)
Installation	• Anomaly or error correction during software product installation

Life Cycle Phase	Reasons
Operation and Maintenance	• Anomaly or error correction during operation and maintenance of the software product, • Licensee contract change request

[[

]]

Table 6.4.2.2-2 Change Process Steps

Responsible Individual	Change Process Steps
[[	]]
[[	]]

Responsible Individual	Change Process Steps
[[	]]
[[	]]
[[	]]
[[	]]

6.4.2.3 Change Request During Requirements, Design, and Implementation Phase

[[

]]

6.4.2.4 Change Request During V&V and Test Phase

Subsection 5.5.1 describes the documentation of discrepancies or errors discovered during V&V and testing process. The discrepancies or errors shall be evaluated and resolved. If the discrepancies or errors impact an issued document or multiple documents, the RMCN process or the Engineering Change Authorization (ECA) process described above shall be followed.

6.4.2.5 Change Request During Installation Phase

Discrepancies or errors discovered in a software product during the Installation Phase shall be processed using the Field Deviation Disposition Request (FDDR) process per Field Deviation Disposition Request [2.3(2.q)].

6.4.2.6 Change Request During Operations and Maintenance Phase

Change requests initiated during the Operations and Maintenance Phase as the result of software errors shall be reported and tracked via an issue tracking tool, for example, the Nuclear Customer Issue Resolution (CIR) Tool [2.3(2.y)]. If an error is found in either Software Class Q or Class N3 software, then Reporting of Defects and Noncompliance under 10 CFR Part 21 [2.3(3.e)] applies.

6.4.2.7 Change Request from Licensee

Proposed changes to a software product design due to contract revision shall be processed in accordance with Baseline Change Assessment and Task Iteration Policy (Subsection 5.5.2).

6.4.2.8 Change Notification

If discrepancies or errors affect software products already turned over to the Licensee, the Project Manager shall:

- Notify the affected plant Licensee of any detected non-conformances
- Supply to the affected plant the upgraded software or Erasable Programmable Read-Only Memory (EPROM)

If an error is found in either Software Class Q or Class N3 software, then Reporting of Defects and Noncompliance under 10 CFR Part 21 [2.3(3.e)] applies.

6.4.2.9 Design Interfaces Control

Engineering design interfaces with vendors or design organizations supporting the design of the software product shall be formally controlled and information formally transmitted. Project correspondence that pertains to the transmission or acceptance of project documents shall be maintained in PDMS.

To ensure interface compatibility, design documents shall be distributed for information and/or review to the affected design organizations to ensure that there is no conflict in the design objectives and to ensure that the product resulting from the interfacing designs function as

planned. The PM is responsible for coordinating the distribution of design documents to appropriate design organizations.

[[

]]

6.4.3 Configuration Status Accounting

Status for design documentation and design outputs can be collected from the PDMS by selecting report module features to obtain the status of the design documentation and design outputs. The responsible TPE shall maintain a record or database used to prepare reports on the status of design documentation and design outputs. The record or database shall include the initial approved version, the status of requested changes, and the implementation status of approved changes for each CI, as well as outstanding engineering documents undergoing engineering change requests that have not yet been resolved. Configuration status reports shall be used as supporting information to the project progress report to ensure timely reporting of project progress and baseline review.

6.4.4 Configuration Audits

Configuration audits shall be performed on the software CIs (including the computer-based items) to ensure the completeness of the software products. There are two types of configuration audits:

- Functional Audit
- Physical Audit

6.4.4.1 Functional Audit

A functional configuration audit is performed during the baseline review. The BRT shall inspect the design documentation, outputs, and associated traceability matrix for completeness (i.e., demonstration of forward and backward direction). Deficiencies shall be documented in the functional configuration audit minutes and maintained as an attachment or part of the BRR. The responsible TPE is responsible for ensuring that the deficiencies are corrected.

6.4.4.2 Physical Audit

A physical configuration audit is performed during the Test Phase baseline review. The BRT shall inspect the Software Build Description of the Software Class Q for completeness, such that a duplicate version of the software package can be recreated. The BRT shall also determine that items identified as being part of the configuration are present in the product baseline. The audit shall establish that the correct version and revision of each part are included in the product baseline and that they correspond to information contained in the baseline's configuration status report. Deficiencies shall be documented in the physical configuration audit minutes and maintained as an attachment or part of the BRR. The responsible TPE is responsible to ensure that the deficiencies are corrected.

6.4.5 Baseline Reviews

The baseline review is conducted at the completion of each software life cycle phase. The following baselines have been designated by the SMPM [2.3(1.a)]:

1. Planning
2. Requirements
3. Design
4. Implementation
5. Test
6. Installation
7. Operation and Maintenance
8. Retirement

The SMPM [2.3(1.a)], in conjunction with the project PWP, specifies the CIs to be baselined during each software life cycle phase.

The purpose of the baseline review is to establish that:

- The design information developed during the software life cycle phase adheres to the software life cycle process outlined in the SMPM
- The V&V tasks and the SSA tasks performed adhere to the procedures outlined in the SVVP and SSP, respectively
- CySA tasks performed adhere to the procedures outlined in the CySPP [2.3(1.b)]

The baseline review is performed as follows:

1. Upon completion of the design activities within the software life cycle phase, including the required V&V tasks, SSA and CySA, the responsible TPE appoints an engineer to prepare the baseline package. The baseline package consists of CIs to be baselined for the specific software life cycle phase.
2. The responsible TPE shall notify the BRT Task Lead that the design activity for the specific software life cycle phase is completed and ready for baseline review. The BRT Task Lead shall schedule the baseline review and convene a BRT.
3. The BRT shall be provided with the copies or the depository location of the configuration items (CIs) to be baselined (including the associated V&V reports) prior to the baseline review meeting.
4. A baseline review is performed to assess the design control and design change control, CySA, SSA, and V&V tasks of a particular software life cycle phase.
5. The BRT has the authority to approve the configuration items (CIs) to be baselined. The non-conformances and assessment shall be documented in the BRR (Subsection 5.4.5). The engineer responsible for the baseline package is responsible for resolving these non-conformances. The final resolution of the identified non-conformances shall be documented in the BRR.

6. A baseline review is not complete until the discrepancies have been resolved. However, if the responsible TPE can justify that the discrepancies discovered do not impact the safety and/or security requirements, exception may be granted at the discretion of the BRT to allow the design team to proceed to the next software life cycle phase. This justification shall be documented in the BRR or as an attachment to the BRR.
7. The BRT task lead shall prepare the BRR. A copy of the BRR shall be forwarded to the responsible TPE to be filed in the software project DRF.

As software design and development is an iterative process, the baseline review shall be repeated as the baselined configuration item (CI) is modified.

6.4.5.1 Baseline Items Approval Process

The configuration items to be baselined shall be reviewed by the BRT to confirm that:

- Adherence to the SMPM, SQAPM and CySPP has been achieved
- The required documents have been completed and verified
- The V&V scope and approach is reasonable
- Comments made during the V&V process have been adequately documented and that the non-conformances noted have been resolved
- The required testing has been completed, the results documented and verified, and the open issues resolved and approved by the BRT

6.4.5.2 Baseline Review Record

The BRT chairperson shall prepare a Baseline Review Record (BRR). Figure 4 provides an acceptable format for the Baseline Review. The BRR is described in Subsection 5.4.5.

6.5 SOFTWARE RELEASE PROCEDURES

The Responsible Configuration Control Engineer (RCCE) has the responsibility and authority to release the approved software package for production. The approved software shall be released in accordance with the procedures outlined in the Software Build Description.

6.6 SOFTWARE PRODUCT RELEASE

The responsible project QCE has the authority for the release of the final software product. The Software product is formally released for shipment upon issuance of a Product Quality Certificate (PQC).

6.7 VENDOR CONTROL

Vendor Control is described in Subsection 3.9.1.

6.7.1 Software Developed by Vendors for the Project

The vendor shall utilize this Software Configuration Management Plan (SCMP) to support the design and development of the software products or prepare an equivalent SCMP in accordance with the requirements outlined in this SCMP and the SMPM [2.3(1.a)].

The equivalent SCMP shall be submitted to GEH for review and approval. Supplier Design Services Document Review [2.3(2.c)] and Supplier Supporting Document Review [2.3(2.m)] define the responsibilities and procedural requirements for review, approval, acceptance, and control of documentation or supporting documents from suppliers required for design services.

6.7.2 Acquired Software

Acquired software is maintained and controlled in accordance with the procedures outlined in Subsection 3.9.2.

6.7.2.1 Acquired Software Configuration Change Control

Acquired software may be modified by the supplier to:

- Correct discrepancies or deficient conditions
- Improve performance

If necessary, the RE shall reapply the evaluation process outlined in the SMPM [2.3(1.a)] to the modified acquired software.

After the required evaluation has been performed and the revised evaluation report and test results have been verified in accordance with the methods outlined in the SVVP, the acquired software, with its associated documentation package, shall be:

- Assigned a new revision number
- Baselined and placed under configuration control

6.8 RECORD COLLECTION AND RETENTION

The baselined configuration items stored on a magnetic or optical medium shall undergo periodic archival backup in accordance with Quality Record Computer Data [2.3(2.s)]. This document prescribes the requirements, procedures, and responsibilities for the control, retention, and retrieval of quality-related computer-based data maintained within the central computing facility of GEH. The configuration items shall contain a direct indication of the item's revision status.

7. SOFTWARE TEST PLAN

7.1 PURPOSE

The purpose of the Software Test Plan (STP) is to prescribe the scope, approach, resources, and schedule of the test activities associated with the software development process. The STP also identifies the items being tested, the features to be tested, the test tasks to be performed, the personnel responsible for each task, and the risks associated with this plan.

7.2 SCOPE

The STP applies to the digital I&C software. Applicability is not restricted by the size, complexity, or criticality of the software. This plan applies to digital I&C software classification levels. This plan applies to the phases of testing from the IV&V Software Validation Test through and including the Site Acceptance Test.

7.2.1 Test Hierarchy

[[

]]

7.2.2 Test Activities

[[

]]

7.2.3 Vendor Test Submittal

Test submittals include test documentation and test items supplied by vendors. These submittals shall be transmitted, received, and approved in accordance with Subsection 3.9.1, Vendor Control.

7.3 SOFTWARE VALIDATION TEST – INDEPENDENT VERIFICATION AND VERIFICATION TEAM (IVVT)

[[

]]

7.4 SYSTEM FACTORY ACCEPTANCE TEST

[[

]]

7.5 [[ ]] TEST

[[

]]

7.6 SITE ACCEPTANCE TEST

[[

]]

7.7 TEST DOCUMENTATION

[[

]]

7.7.1 Test Plans

[[

]]

7.7.2 Test Design Specifications

[[

]]

7.7.3 Test Case Specifications

[[

]]

7.7.4 Test Procedure Specifications

[[

]]

7.7.5 Test Item Transmittal Report

[[

]]

7.7.6 Test Log

[[

]]

7.7.7 Test Incident Reports

[[

]]

7.7.8 Test Summary Reports

[[

]]

8. SQAPM MAINTENANCE

The SPE and SQA Managers are responsible for the maintenance of the SQAPM. The SQAPM shall be assessed during the managerial review to ensure its suitability, adequacy, and effectiveness and revised to incorporate the agreed upon changes as described in Subsection 3.5.2. When improvements or deficiencies are identified, a Corrective Action Request (CAR) should be used to document the condition in accordance with Corrective Action Process[2.3(2.v)].

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 SQAPM. The SQAPM shall be revised in accordance with the Design Change Control process described in Subsection 6.4.2.2. The SPE Manager or his designated delegate shall distribute the revised SQAPM to the organizations described in Section 3.2, Management Organization.

9. TABLES & FIGURES

Table 9-1a

Software Life Cycle Tasks, Responsibilities and Documentation-Planning Phase

System Design Tasks	System Design Task Inputs	System Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks
[[					
					]]

Table 9-1b

Requirements Phase

System Design Tasks	System Design Task Inputs	System Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks
[[					

Table 9-1b

Requirements Phase

System Design Tasks	System Design Task Inputs	System Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks
					]]

Table 9-1c

Design Phase

Software Design Tasks	Software Design Task Inputs	Software Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks
[[					

Table 9-1c

Design Phase

Software Design Tasks	Software Design Task Inputs	Software Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks

Table 9-1c

Design Phase

Software Design Tasks	Software Design Task Inputs	Software Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks

Table 9-1c

Design Phase

Software Design Tasks	Software Design Task Inputs	Software Design Task Outputs	Development Organization	Review Organization	Associated Quality Tasks
					]]

Table 9-1d

Implementation Phase

Implementation Tasks	Implementation Task Inputs	Implementation Task Outputs	Implementation Organization	Review Organization	Associated Quality Tasks
[[					

Table 9-1d

Implementation Phase

Implementation Tasks	Implementation Task Inputs	Implementation Task Outputs	Implementation Organization	Review Organization	Associated Quality Tasks

Table 9-1d

Implementation Phase

Implementation Tasks	Implementation Task Inputs	Implementation Task Outputs	Implementation Organization	Review Organization	Associated Quality Tasks
					]]

Table 9-1e

Test Phase

Test / Design Tasks	Test / Design Inputs	Test / Design Outputs	Design Organization	Test / Review Organization	Associated Quality Tasks
[[					

Table 9-1e

Test Phase

Test / Design Tasks	Test / Design Inputs	Test / Design Outputs	Design Organization	Test / Review Organization	Associated Quality Tasks

Table 9-1e

Test Phase

Test / Design Tasks	Test / Design Inputs	Test / Design Outputs	Design Organization	Test / Review Organization	Associated Quality Tasks
					]]

Table 9-1f

Installation Phase

Test / Design Tasks	Test / Design Inputs	Test / Design Outputs	Design Organization	Test / Review Organization	Associated Quality Tasks
[[					

Table 9-1f

Installation Phase

Test / Design Tasks	Test / Design Inputs	Test / Design Outputs	Design Organization	Test / Review Organization	Associated Quality Tasks

Table 9-1f

Installation Phase

Test / Design Tasks	Test / Design Inputs	Test / Design Outputs	Design Organization	Test / Review Organization	Associated Quality Tasks
					]]

Table 9-1g Operations and Maintenance Phase

Operation & Maintenance Tasks	Operation & Maintenance Task Inputs	Operation & Maintenance Task Outputs	Operation & Maintenance Organization	Review Organization	Associated Quality Tasks
[[					
			]]		

Table 9-2 lists the V&V and SSA tasks to be performed for software class Q, N3, and N2 software during the software life cycle phase. This table also indicates the organization responsible for conducting these tasks. If a V&V or SSA task is not pertinent to a particular software product, the V&V summary report shall contain the phrase, "The (task name) is not applicable to this (software product name)," with an appropriate reason for exclusion. The description of these V&V and SSA tasks are defined in Appendix E, V&V and SSA Tasks Description.

Table 9-2

V&V and SSA Tasks Assigned to Each Software Class

Software Life Cycle Processes	Planning			Requirements			Design			Implementation			Test			Installation			Operations & Maintenance		
Software Classification	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2
[[																					

Table 9-2

V&V and SSA Tasks Assigned to Each Software Class

Software Life Cycle Processes	Planning			Requirements			Design			Implementation			Test			Installation			Operations & Maintenance		
Software Classification	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2

Table 9-2

V&V and SSA Tasks Assigned to Each Software Class

Software Life Cycle Processes	Planning			Requirements			Design			Implementation			Test			Installation			Operations & Maintenance		
Software Classification	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2

Table 9-2

V&V and SSA Tasks Assigned to Each Software Class

Software Life Cycle Processes	Planning			Requirements			Design			Implementation			Test			Installation			Operations & Maintenance		
Software Classification	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2

Table 9-2

V&V and SSA Tasks Assigned to Each Software Class

Software Life Cycle Processes	Planning			Requirements			Design			Implementation			Test			Installation			Operations & Maintenance		
Software Classification	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2

Table 9-2

V&V and SSA Tasks Assigned to Each Software Class

Software Life Cycle Processes	Planning			Requirements			Design			Implementation			Test			Installation			Operations & Maintenance		
Software Classification	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2	Q	N3	N2
																					]]

[[

]]

Table 9-3

Problems and Corrective Action Reporting

Step	Scenario	Identified by	Documentation
[[			

Table 9-3

Problems and Corrective Action Reporting

Step	Scenario	Identified by	Documentation

Table 9-3

Problems and Corrective Action Reporting

Step	Scenario	Dispositioned / Evaluated by	Documentation

Table 9-3

Problems and Corrective Action Reporting

Step	Scenario	Dispositioned / Evaluated by	Documentation

Table 9-3

Problems and Corrective Action Reporting

Step	Scenario	Accepted / Closed by	Documentation

Table 9-3

Problems and Corrective Action Reporting

Step	Scenario	Accepted / Closed by	Documentation
			]]

Table 9-4

Configuration Items

Configuration Items	Format	Retention Medium
Planning Phase		
[[		
		]]
Requirements Phase		
[[		

Table 9-4

Configuration Items

Configuration Items	Format	Retention Medium
		]]
Design Phase		
[[		
		]]
Implementation Phase		
[[		

Table 9-4

Configuration Items

Configuration Items	Format	Retention Medium
		]]
Test Phase		
[[		
		]]
Installation Phase		

Table 9-4

Configuration Items

Configuration Items	Format	Retention Medium
[[		
		]]
Operation and Maintenance Phase		
[[		
		]]
Retirement Phase		
[[		

Table 9-4

Configuration Items

Configuration Items	Format	Retention Medium
		]]

MFN 09-520

Enclosure 3

Affidavit

GE-Hitachi Nuclear Energy Americas LLC

AFFIDAVIT

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

(1) I am Manager, New Units Engineering, GE-Hitachi Nuclear Energy Americas LLC ("GEH") have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.

(2) The information sought to be withheld is contained in Enclosure 1 of GEH letter MFN 09-520, Mr. Richard Kingston to Nuclear Regulatory Commission, *Submittal of ESBWR Licensing Topical Report – ESBWR -Software Quality Assurance Program Manual, Rev. 4, NEDE-33245P* dated July 30, 2009. The proprietary information is enclosed within double square rackets with a dotted underline. [[This sentence is an example. {3}]] Figures and large equation objects are enclosed in double brackets. The superscript notation {3} refers to Paragraph (3) of the enclosed affidavit in Enclosure 1, which provides the basis for the proprietary determination.

(3) In making this application for withholding of proprietary information of which it is the owner or License, GEH relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.790(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).

(4) Some examples of categories of information which fit into the definition of proprietary information are:

a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by GEH's competitors without license from GEH constitutes a competitive economic advantage over other companies;

b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

c. Information which reveals aspects of past, present, or future GEH customer-funded development plans and programs, resulting in potential products to GEH;

d. Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.

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

(5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GEH, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GEH, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.

(6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge, or subject to the terms under which it was licensed to GEH. Access to such documents within GEH is limited on a "need to know" basis.

(7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GEH are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.

(8) The information identified in paragraph (2), above, is classified as proprietary because it contains the details of GEH's design and licensing methodology. The development of the methods used in these analyses, along with the testing, development and approval of the supporting methodology was achieved at a significant cost to GEH.

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

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

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

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

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

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

Executed on this 30th day of July 2009.

David H. Hinds
GE-Hitachi Nuclear Energy Americas LLC