

**US-APWR**  
**Software Program Manual**

Non-Proprietary Version

**May 2011**

**©2011 Mitsubishi Heavy Industries, Ltd.**  
All Rights Reserved

## Revision History

Revision	Date	Page (Section)	Description
0	December 2007	All	Original issued
1	April 2010		The following items are revised based on RAI responses (UAP-HF-09141 and UAP-HF-10063).
		1 (1.1)	“based in” is changed to “which conform to” to follow the response (UAP-HF-10063) to RAI 07-14 BTP-30.
		4 (2.2.2)	Description of the responsibility of DTM is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-41.
		4 (2.2.2)	Description of the responsibility of VTM is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-41.
		14 (3.1.4)	Description of the security of the software development tool is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-35.
		15 (3.1.10)	Section 3.1.10 is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		17 (3.2.4)	Description of the potential risk of application software is revised to follow the response ( ) to RAI 07-14 BTP-9.
		17 (3.2.5)	Description of metrics is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-36.
		17 (3.2.9)	Description of standards is revised to follow the response (UAP-HF-09141) to RAI 07-14 BTP-14.
		18 (3.3.5)	Description of QA activity of Plant Requirement and System Requirement Phase is revised to follow the responses (UAP-HF-09141 and UAP-HF-10063) to RAI 07-14 BTP-2 and RAI 07-14 BTP-33.
		21 (3.3.5)	“and all software classes” is deleted to follow the response (UAP-HF-09141) to RAI 07-14 BTP-3.

Revision	Date	Page (Section)	Description
		21 (3.3.6)	Description of MHI's QA program for safety related documentation is added to follow the response (UAP-HF-09141) to RAI 07-14 BTP-4.
		22 (3.3.7)	Description of reuse of application software is revised to follow the response (UAP-HF-09141) to RAI 07-14 BTP-5.
		22 (3.3.8)	Description of standards is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		23 (3.4.3)	Description of the error rate during integration activities is added to follow the response (UAP-HF-09141) to RAI 07-14 BTP-11.
		24 (3.4.4)	The following sentences are added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-37. <ul style="list-style-type: none"> <li>▪ "After installing ... are being reported.</li> </ul>
		24 (3.4.4)	Description of documented procedures for integration activities is added to follow the response (UAP-HF-09141) to RAI 07-14 BTP-12.
		24 (3.4.6)	Section 3.4.6 is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		26 (3.5.6)	Section 3.5.6 is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		27 (3.6.1)	Description of purpose of SMP is revised to follow the responses (UAP-HF-09141 and UAP-HF-10063) to RAI 07-14 BTP-17 and RAI 07-14 BTP-39.
		27 (3.6.2)	Description of errors is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-39.
		28 (3.6.6)	Description of troubleshooting is added to follow the response (UAP-HF-09141) to RAI 07-14 BTP-19.
		28 (3.6.6)	Description of implementation of error corrections is added to follow the response (UAP-HF-09141) to RAI 07-14 BTP-18.
		28 (3.6.7)	Description of tools is added to follow the response (UAP-HF-09141) to RAI 07-14 BTP-20.

Revision	Date	Page (Section)	Description
		26 (3.6.8)	Section 3.6.8 is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		26 (3.7.6)	Section 3.7.6 is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		34 (3.9.2)	Description of Organization/Responsibilities for SSP is added to follow the responses (UAP-HF-09141 and UAP-HF-10063) to RAI 07-14 BTP-21 and RAI 07-14 BTP-41.
		35 (3.9.4)	Description of metrics is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-36.
		41 (3.10.8)	Description of standards is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		42 (3.11.1)	Description of the purpose of the SCMP is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-32.
		44 (3.11.3.2)	Editorial correction “ <b>Managemen<del>t</del></b> ” → “ <b>Management</b> ”
		45 (3.11.6)	Description of the procedures of configuration identification management is added to follow the response (UAP-HF-10063) to RAI 07-14 BTP-45.
		47 (3.11.6.6)	“Software safety analysis” is added to Step 1 to follow the response (UAP-HF-09141) to RAI 07-14 BTP-27.
		48 (3.11.9)	Description of standards is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		49 (3.12.1)	“module testing, unit testing” is changed to “component testing (e.g., module testing, unit testing)” to follow the response (UAP-HF-09141) to RAI 07-14 BTP-29.
		49 (3.12.2)	Description of organization/responsibilities of STP is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-31.
		49 (3.12.3)	Description of the prevention of a possible virus is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-35.

Revision	Date	Page (Section)	Description
		49 (3.12.4)	Description of metrics is revised to follow the response (UAP-HF-09141) to RAI 07-14 BTP-36.
		52 (3.12.8)	Description of standards is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
		53 (4.0)	Editorial correction Description of Item 9 in Table 4.0-1 “results” → “Results”
		54 (4.0)	Note1 is added.
		55 (5.0)	Description of references is revised to follow the response (UAP-HF-10063) to RAI 07-14 BTP-38.
2	September 2010	All	Following items are revised to reflect feedback received from the NRC at the public meeting held on August 18 and 19, 2010 and commitments made in the letter (UAP-HF-10237).
		General	Methods to use the acronyms and words are corrected.
		General	Descriptions of Unit Testing are revised or deleted.
		xvii (List of Acronym)	The acronyms are revised.
		1 (1.2)	Description is moved from Section 2.0 and revised.
		1 (1.2)	“and operation” is added.
		1 (1.2)	“Assumptions in a specific project are described as follows” is added.
		2 (2.1)	Description is moved to Section 1.2 and revised.
		4 (2.2.1)	Figure 2.2-1 and related description are revised.
		4 (2.2.2)	Description of the roles and responsibilities of PM is added.
		5 (2.2.2)	Description of the roles and responsibilities of DTM is added.
		5 (2.3.1)	Description of Overview of Lifecycle is added.
		5 (2.3.1)	Description of Plant requirements phase is revised.

Revision	Date	Page (Section)	Description
		6 (2.3.1)	Description of Hardware/software requirements phase is revised.
		6-12 (2.3.1)	Table 2.3-1 and related description are added.
		14 (3.0)	Figure 3.0-1 is corrected.
		15 (3.0)	Description of overview of lifecycle is added.
		16 (3.1.1)	Table 3.1-1 and related description are deleted.
		17 (3.1.2)	"Software management activities should be periodically reported to PM" is added.
		17 (3.1.2)	Description of subcontractors and suppliers is added.
		18 (3.1.4)	"Detailed discussion is described in Section 3 of Appendix C." is added.
		18 (3.1.6)	"and to improve the process progress" is added.
		18 (3.1.6)	Editorial correction "remedial" → "corrective"
		19 (3.1.8)	"During each project phase," is added.
		19 (3.1.8)	Editorial correction "Section 3.2" → "Section 3.1.5"
		19 (3.1.10)	"Conformance to above standard is shown in Appendix B." is added.
		20 (3.2.3)	Description of software quality factors is added.
		21 (3.2.4)	Description of conformance to IEEE Std 7-4.3.2-2003 is added.
		21 (3.2.6)	Description of Procedure of SDP is revised.
		21 (3.2.7)	Description of Schedule of SDP is revised.
		21 (3.2.8)	Description of generation of logic diagram is revised.
		22 (3.2.8)	Description of reuse of software is added.
		22 (3.2.8)	Description of document control is added.
		22 (3.2.9)	"and IEEE Std 830-1993 (Reference 7) endorsed by RG 1.172 (Reference 21)." is added.

Revision	Date	Page (Section)	Description
		22 (3.2.9)	“Conformance to above standards is shown in Appendix B.” is added.
		23 (3.3.1)	Description of conformance to IEEE Std 7-4.3.2-2003 is added.
		23 (3.3.2)	Description of audit results is added.
		23 (3.3.2)	Description of conformance to IEEE Std 7-4.3.2-2003 is added.
		23 (3.3.5)	Description of software quality factors is added.
		24 (3.3.5)	Description of traceability of SQAP activities is added.
		25 (3.3.5)	Description of conformance to IEEE Std 7-4.3.2-2003 is added.
		26 (3.3.5)	Item 6 “Operation Phase” is added.
		26 (3.3.5)	“These technical reviews...IEEE std 1028-1997 (Reference 9).” is added.
		28 (3.3.8)	“Conformance to above standards is shown in Appendix B.” is added.
		30 (3.4.4)	“For these integration activities...and used” is revised.
		30 (3.4.6)	“Conformance to above standards is shown in Appendix B.” is added.
		31 (3.5.1)	Description of testing environment of PSMS functions is revised.
		32 (3.5.6)	“Conformance to above standard is shown in Appendix B.” is added.
		33 (3.6.5)	Description of Measurement of SMaintP is revised.
		34 (3.6.7)	Description of Resource of SMaintP is revised.
		35 (3.6.8)	“Conformance to above standard is shown in Appendix B.” is added.
		36 (3.7.2)	Descriptions of Organization/Responsibilities of STrngP are revised.
		36 (3.7.3)	Descriptions of Measurement of STrngP are revised.
		37 (3.7.6)	“Conformance to above standard is shown in Appendix B.” is added.
		38 (3.8.2)	3.8.2 Organization → Organization/Responsibilities

Revision	Date	Page (Section)	Description
		38 (3.8.2)	Description of the responsibility of SOP is revised.
		39 (3.8.3)	"Contingency plan shall ensure response to penetration." is added.
		39 (3.8.4)	Description of Measurement of SOP is revised.
		39 (3.8.5)	Descriptions are added.
		39 (3.8.6)	Description of providing manual is added.
		40 (3.9.1)	Description of Purpose of SSP is revised.
		40 (3.9.1)	Description of conformance to IEEE Std 1074-1195 is added.
		40 (3.9.2)	Descriptions of Organization/Responsibilities of SSP are revised.
		40 (3.9.3)	Description of Risks of SSP is revised.
		41 (3.9.4)	"by the V&V Team" → "by the Design Team"
		41 (3.9.5)	Description of Procedures of SSP is revised.
		41 (3.9.6)	Descriptions of Methods/tools are revised.
		41 (3.9.7)	"Conformance to above standards is shown in Appendix B." is added.
		42 (3.10.1)	Description of conformance to IEEE Std 7-4.3.2-2003 is added
		42 (3.10.2)	Descriptions of Organization/Responsibilities are revised.
		43 (3.10.4)	Descriptions of the potential risk and contingency program are added.
		43 (3.10.5)	Descriptions of Measurement of SVVP are revised.
		43-44 (3.10.6)	Descriptions of Procedures of SVVP are revised.
		45 (3.10.6)	Figure 3.10-1 is added.
		46 (3.10.6.1)	Description of V&V Team outputs is revised.
		47 (3.10.6.2)	Descriptions of V&V Team outputs are revised.

Revision	Date	Page (Section)	Description
		47 (3.10.6.3)	Descriptions of V&V Team outputs are revised.
		48 (3.10.6.4.1)	Descriptions of V&V Team outputs are revised.
		49 (3.10.6.5)	Descriptions of Verification Basis are revised.
		49 (3.10.6.5)	Descriptions of V&V Team Tasks are revised.
		49 (3.10.6.5)	Descriptions of V&V Team outputs are revised.
		49-50 (3.10.7)	Descriptions of Methods/tools of SVVP are revised.
		50 (3.10.8)	"Conformance to above standards is shown in Appendix B." is added.
		51 (3.11.1)	Description of conformance to IEEE Std 7-4.3.2-2003, IEEE 828-1990 and IEEE Std 1042-1987 is added.
		52 (3.11.2)	Item 1 of configuration management is revised.
		53 (3.11.3.2)	Description of Configuration Control Management is revised.
		54 (3.11.5)	"In each phase...of each SCM activity" is added.
		54 (3.11.6)	Description of reference sections of SCM activities is added.
		56 (3.11.6.6)	"and organization" is added.
		57 (3.11.7)	Description of backup copies is revised.
		57 (3.11.8)	Description of item 2 is revised.
		57 (3.11.9)	"Conformance to above standards is shown in Appendix B." is added.
		58 (3.12.1)	Descriptions of Purpose of STP are revised.
		58 (3.12.2)	Descriptions of Organization/Responsibilities are revised.
		58 (3.12.4)	Descriptions of Measurement are revised.
		58 (3.12.5)	Item 1 and 2 are added to contents of test specifications.

Revision	Date	Page (Section)	Description
		59 (3.12.5)	Descriptions of Procedures of STP are revised.
		59 (3.12.5)	Descriptions of FAT – First System are revised.
		60 (3.12.5)	Description of Installation Test is revised.
		60 (3.12.5)	“Test documents listed in Table 4.0-1 are prepared in accordance with IEEE std 829-1983 (Reference 15).” is added.
		61 (3.12.7)	Description of Methods/tools is revised.
		61 (3.12.8)	“Conformance to above standards is shown in Appendix B.” is added.
		64-65 (5.0)	References 23 to 25 are added.
		A-1 (Appendix A)	Appendix A is added.
		B-1 (Appendix B)	Appendix B is added.
		C-1 (Appendix C)	Appendix C is added.
3	January 2011	All	Following items are revised to reflect feedback received from the NRC at the public meeting held on December 10, 2010 and RAI 07.01-24. Most of the contents of revision 2 were revised; therefore the revision bar is omitted.
		1.0-1 – 1.0-2 (1.2)	Scope and responsibilities between the PSMS application software and the MELTAC platform basic software are added.
		1.0-2 – 1.0-3 (1.3)	Applicable documents section is added as 1.3.
		All pages of Section 2.0	Organization and responsibilities are revised to clearly identify the independence between the DT and the VVT. The activities tables for each section are moved to Section 3.2 “SDP”.
		All pages of Section 3.0	Summary description of each plan is identified and the overview figure is revised.
		All pages of Section 3.1	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.2	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.3	Completely revised based on the comments and RAI 07.01-24 from the NRC.

Revision	Date	Page (Section)	Description
		All pages of Section 3.4	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.5	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.6	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.7	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.8	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.9	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.10	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.11	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 3.12	Completely revised based on the comments and RAI 07.01-24 from the NRC.
		All pages of Section 4.0	All outputs documents of each PSMS application software life cycle process are described.
		All pages of Section 5.0	Necessitate references RG, NUREG, IEEE and related documents are added.
		All pages of Appendix A	Definitions are revised to follow the definitions in accordance with IEEE Std 610.12-1990.
		All pages of Appendix B	Detail compliance matrix of BTP 7-14 is deleted, and compliance matrices for all IEEE which are endorsed by RG are added.
		All pages of Appendix C	All descriptions are revised to consistent with the all revised description of other sections.
4	May 2011	All	Editorial corrections have been made.
		1.1	Purpose of this Technical Report has been revised to clarify that this document encompass not only for the application software but also basic software. (Action item at the public meeting.)
		1.2	Scope of this Technical Report has been revised to clarify that this document encompass not only for the application software but also basic software. (Action item at the public meeting.)

Revision	Date	Page (Section)	Description
		1.2	Applicability of the augmented quality systems has been added. (Action item at the public meeting.)
		2.2.2	Explanation of V&V resources from Design Team is added. (Action item at the public meeting.)
		3.1.10	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.2.6.1.2	DCD Tier 1 has been added as an output of Plant Requirement Phase. (Action item at the public meeting.)
		3.2.9	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.3.8	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.4.6	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.5.6	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.6.4	References to “cyber security” have been changed as appropriate “secure development / operational environment.” (Response to RAI 710-5493)
		3.6.8	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.7.1	Customer training plan for MELTAC Platform has been added. (Response to RAI 732-5627)
		3.7.2	Customer training plan for MELTAC Platform has been added. (Response to RAI 732-5627)

Revision	Date	Page (Section)	Description
		3.7.4.1	Customer training plan for MELTAC Platform has been added. (Response to RAI 732-5627)
		3.7.5	Customer training plan for MELTAC Platform has been added. (Response to RAI 732-5627)
		3.7.6	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.8.3	References to “cyber security” have been changed as appropriate “secure development / operational environment.” (Response to RAI 710-5493)
		3.8.7	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.9.7.12	Description of the subcontractor management has been revised or added. (Response to RAI 733-5650)
		3.9.8.1	Description of the Plant Requirement Phase SSA is revised. (Response to RAI 734-5659)
		3.9.9	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.10.2.2	Explanation of V&V resources from Design Team is added. (Action item at the public meeting.)
		3.10.6.3.2.1	DCD Tier 1 has been added as an output of Plant Requirement Phase. (Action item at the public meeting.)
		3.11.3.6	Description of the subcontractor management has been revised or added. (Response to RAI 733-5650)
		Figure 3.10-2	DCD Tier 1 has been added as an output of Plant Requirement Phase. (Action item at the public meeting.)

Revision	Date	Page (Section)	Description
		3.10.8	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.11.7	References to “cyber security” have been changed as appropriate “secure development / operational environment.” (Response to RAI 710-5493)
		3.11.12	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		3.12.3	References to “cyber security” have been changed as appropriate “secure development / operational environment.” (Response to RAI 710-5493)
		3.12.8	Conformance or exception statements for BTP 7-14 and IEEE Standards have been added. (Action item at the public meeting.)
		Appendix B	Appendix B has been deleted. (Action item at the public meeting.)
		Appendix C	References to “cyber security” have been changed as appropriate “secure development / operational environment.” (Response to RAI 710-5493)
		Appendix D	Applicability of the augmented quality systems has been added. (Action item at the public meeting.)

© 2011  
**MITSUBISHI HEAVY INDUSTRIES, LTD.**  
All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with the U.S. Nuclear Regulatory Commission ("NRC") licensing review of MHI's US-APWR nuclear power plant design. None of the information in this document, may be disclosed, used or copied without written permission of MHI, other than by the NRC and its contractors in support of the licensing review of the US-APWR.

This document contains technological information and intellectual property relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Heavy Industries, Ltd.  
16-5, Konan 2-chome, Minato-ku  
Tokyo 108-8215 Japan

## **Abstract**

This Software Program Manual (SPM) describes the processes, which ensure the reliability and design quality of the US-APWR Protection and Safety Monitoring System (PSMS) software throughout its entire life cycle. By following this SPM, the digital safety I&C system software achieves high functionality and high quality as shown below.

- Software for the PSMS achieves a quality level expected for nuclear plant safety functions.
- Application software provides the required safety functions.
- The processes and procedures described in this SPM are based on established technical and document control requirements, practices, rules and industrial standards.

## Table of Contents

List of Tables  
List of Figures  
List of Acronyms

1. INTRODUCTION	1-1
1.1 Purpose	1-1
1.2 Scope	1-1
1.3 Applicable Documents	1-2
1.3.1 Regulatory Documents and Codes	1-2
1.3.2 Standards	1-3
1.3.3 Other Standards	1-3
1.3.4 Supplemental Documents	1-4
1.4 Definitions	1-4
2. SOFTWARE LIFE CYCLE PROCESS CONTROL	2-1
2.1 Purpose	2-1
2.2 Organization and Responsibilities	2-3
2.2.1 Organization	2-3
2.2.2 Responsibilities	2-3
2.3 General Requirements	2-4
2.3.1 Overview of Life Cycle	2-4
2.3.2 Classification of Software	2-6
2.3.3 Documentation	2-6
3. SOFTWARE LIFE CYCLE PLANS	3-1
3.1 Software Management Plan	3.1-1
3.1.1 Purpose	3.1-1
3.1.2 Organization/Responsibilities	3.1-2
3.1.3 Oversight	3.1-3
3.1.4 Security	3.1-4
3.1.5 Measurement	3.1-5
3.1.6 Procedures	3.1-5
3.1.7 Budget	3.1-7
3.1.8 Methods/Tools	3.1.7
3.1.9 Personnel	3.1.9
3.1.10 Standards	3.1.9
3.2 Software Development Plan	3.2-1
3.2.1 Purpose	3.2-1
3.2.2 Organization	3.2-1
3.2.3 Oversight	3.2-2
3.2.4 Risks	3.2-2
3.2.5 Measurement	3.2-2
3.2.6 Procedures	3.2-2
3.2.7 Schedule	3.2-7
3.2.8 Methods/Tools	3.2-7
3.2.9 Standards	3.2-10

---

3.3 Software Quality Assurance Plan	3.3-1
3.3.1 Purpose	3.3-1
3.3.2 Organization/Responsibilities	3.3-1
3.3.3 Security	3.3-2
3.3.4 Measurement	3.3-3
3.3.5 Procedures	3.3-3
3.3.6 Record Keeping	3.3-8
3.3.7 Methods/Tools	3.3-9
3.3.8 Standards	3.3-10
3.4 Software Integration Plan	3.4-1
3.4.1 Purpose	3.4-1
3.4.2 Organization/Responsibilities	3.4-1
3.4.3 Measurement	3.4-1
3.4.4 Procedures	3.4-2
3.4.5 Methods/Tools	3.4-2
3.4.6 Standards	3.4-2
3.5 Software Installation Plan	3.5-1
3.5.1 Purpose	3.5-1
3.5.2 Organization/Responsibilities	3.5-1
3.5.3 Measurement	3.5-1
3.5.4 Procedures	3.5-2
3.5.5 Methods/Tools	3.5-3
3.5.6 Standards	3.5-3
3.6 Software Maintenance Plan	3.6-1
3.6.1 Purpose	3.6-1
3.6.2 Organization/Responsibilities	3.6-1
3.6.3 Risks	3.6-2
3.6.4 Security	3.6-2
3.6.5 Measurement	3.6-2
3.6.6 Procedures	3.6-2
3.6.7 Methods/Tools	3.6-4
3.6.8 Standards	3.6-4
3.7 Software Training Plan	3.7-1
3.7.1 Purpose	3.7-1
3.7.2 Organization/Responsibilities	3.7-1
3.7.3 Measurement	3.7-1
3.7.4 Procedures	3.7-2
3.7.5 Resources	3.7-4
3.7.6 Standards	3.7-4
3.8 Software Operations Plan	3.8-1
3.8.1 Purpose	3.8-1
3.8.2 Organization/Responsibilities	3.8-1
3.8.3 Security	3.8-1
3.8.4 Measurement	3.8-1
3.8.5 Procedures	3.8-1
3.8.6 Methods/Tools	3.8-2

---

3.8.7 Standards	3.8-2
3.9 Software Safety Plan	3.9-1
3.9.1 Purpose	3.9-1
3.9.2 Organization/Responsibilities	3.9-2
3.9.3 Risks	3.9-3
3.9.4 Measurement	3.9-5
3.9.5 Procedures	3.9-5
3.9.6 Methods/Tools	3.9-6
3.9.7 Software Safety Management (SSM)	3.9-6
3.9.8 Software Safety Analysis (SSA)	3.9-9
3.9.9 Standards	3.9-20
3.10 Software Verification and Validation Plan	3.10-1
3.10.1 Purpose	3.10-1
3.10.2 Organization/Responsibilities	3.10-2
3.10.3 Management and Oversight of V&V Activities	3.10-5
3.10.4 Risks	3.10-5
3.10.5 Measurement	3.10-6
3.10.6 Procedures	3.10-6
3.10.7 Methods/Tools	3.10-35
3.10.8 Standards	3.10-35
3.11 Software Configuration Management Plan	3.11-1
3.11.1 Purpose, Scope and Applicability	3.11-1
3.11.2 SCM Management	3.11-4
3.11.3 SCM Activities	3.11-6
3.11.4 SCM Schedules	3.11-10
3.11.5 SCMP Resources	3.11-10
3.11.6 SCMP Maintenance	3.11-10
3.11.7 Security	3.11-10
3.11.8 Measurement	3.11-10
3.11.9 Procedures	3.11-10
3.11.10 Record Keeping	3.11-12
3.11.11 Methods/Tools	3.11-12
3.11.12 Standards	3.11-13
3.12 Software Test Plan	3.12-1
3.12.1 Purpose	3.12-1
3.12.2 Organization/Responsibilities	3.12-1
3.12.3 Security	3.12-1
3.12.4 Measurement	3.12-1
3.12.5 Procedures	3.12-1
3.12.6 Record Keeping	3.12-7
3.12.7 Methods/Tools	3.12-7
3.12.8 Standards	3.12-7
4. OUTPUT DOCUMENTS	4-1
5. REFERENCES	5-1

Appendix A Definitions

Appendix B Deleted

Appendix C PSMS Application Software Security Features

Appendix D Software Program Manual for Augmented Quality Systems

## List of Tables

Table 2.1-1	Correspondence to BTP 7-14	2-2
Table 3.2-1	Project Department Activities	3.2-11
Table 3.2-2	Design Team Activities	3.2-13
Table 3.2-3	V&V Team Activities	3.2-22
Table 3.2-4	QA Department Activities	3.2-30
Table 3.2-5	Map of MHI Software Life Cycle Activities to IEEE Std 1074-1995 endorsed by RG 1.173	3.2-31
Table 3.2-6	Minimum Contents of SysRS	3.2-35
Table 3.2-7	Required SysRS Functional Characteristics	3.2-37
Table 3.2-8	Required SysRS Process Characteristics	3.2-38
Table 3.10-1	Software Integrity Level (SIL)	3.10-7
Table 3.11-1	IEEE Std 828-1990 vs. SCMP Section	3.11-1
Table 3.11-2	Matrix of SCM Responsibilities	3.11-5
Table 3.12-1	Alignment with IEEE Std 1012-1998 Testing Activities	3.12-2
Table 3.12-2	Alignment with IEEE Std 829-1983 Test Documents	3.12-4
Table 4-1	Output Documents of Project Department	4-1
Table 4-2	Output Documents of Design Team	4-2
Table 4-3	Output Documents of V&V Team	4-4
Table 4-4	Output Documents of QA Department	4-7

## List of Figures

Figure 1.2-1	Scope of Application and Basic Software	1-2
Figure 2.2-1	Organizational Structure to Manage the Software Life Cycle Process	2-3
Figure 3-1	Overview of Software Life Cycle Plan	3-5
Figure 3.2-1	Overview of Application Software Life Cycle Process	3.2-39
Figure 3.2-2	Development Process of the Application Software	3.2-41
Figure 3.10-1	V&V Activity Flow	3.10-4
Figure 3.10-2	Overview of Application Software V&V Activities, Tasks and Outputs	3.10-9
Figure 3.10-3	Implementation V&V	3.10-23

## List of Acronyms

A/D	Analog/Digital
AOO	Anticipated Operational Occurrences
BTP	Branch Technical Position
CAD	Computer Aided Design
CAR	Corrective Action Report
CCB	Configuration Control Board
CCF	Common Cause Failure
CDF	Core Demerge Frequency
CFR	Code of Federal Regulations
CI	Configuration Item
CM	Configuration Management
COL	Combined License
COTS	Commercial-Off-The-Shelf
CRC	Cyclic Redundancy Check
DAS	Diverse Actuation System
DC	Design Certification
DCD	Design Control Document
DT	Design Team
DTE	Design Team Engineer
DTM	Design Team Manager
ESF	Engineered Safety Features
ESFAS	Engineered Safety Feature Actuations System
FAT	Factory Acceptance Test
FBD	Function Block Diagram
FD	Function Diagram
FMEA	Failure Modes and Effects Analysis
FPGA	Field-Programmable Gate Array
F-ROM	Flash Read Only Memory
FSAR	Final Safety Analysis Report
GBD	Graphic Block Diagram
GM	General Manager
HSI	Human System Interface
I&C	Instrumentation and Control
IDD	Interface Design Document
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IRS	Interface Requirements Specification
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
LAN	Local Area Network
LERF	Large Early Release Frequency

---

MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries, Ltd.
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
PCMS	Plant Control and Monitoring System
PJM	Project Manager
PMT	Project Management Team
POL	Problem Oriented Language
PRA	Probabilistic Risk Assessment
PSMS	Protection and Safety Monitoring System
QA	Quality Assurance
QAE	Quality Assurance Engineer
QAM	Quality Assurance Manager
QAP	Quality Assurance Plan
RFP	Request for Proposal
RG	Regulatory Guide
ROM	Read Only Memory
RPS	Reactor Protection System
RTM	Requirement Traceability Matrix
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCR	Software Change Request
SDD	Software Design Description
SDP	Software Development Plan
SER	Safety Evaluation Report
SIL	Software Integrity Level
SInstP	Software Installation Plan
SIntP	Software Integration Plan
SLC	Safety Logic System
SMaintP	Software Maintenance Plan
SMP	Software Management Plan
SOP	Software Operations Plan
SPDS	Safety Parameter Display System
SPM	Software Program Manual
SQAP	Software Quality Assurance Plan
SRP	Standard Review Plan
SRS	Software Requirement Specification
SSA	Software Safety Analysis
SSE	Software Safety Analysis Engineer
SSM	Software Safety Management
SSP	Software Safety Plan
STP	Software Test Plan
STrngP	Software Training Plan
SVVP	Software Verification and Validation Plan

SVVR	Software Verification and Validation Report
SysDD	System Design Description
SysRS	System Requirements Specification
VDU	Visual Display Unit
V&V	Verification and Validation
VVT	V&V Team
VVTE	V&V Team Engineer
VVTM	V&V Team Manager

## 1. INTRODUCTION

### 1.1 Purpose

This Software Program Manual (SPM) describes the software quality assurance requirements which govern the software life cycle for the Protection and Safety Monitoring System (PSMS) of the US-APWR. This SPM provides the software program plans which conform to the Chapter 7 of NUREG 0800 "Standard Review Plan" and the guidance of Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" (Reference 1).

### 1.2 Scope

This SPM shall be applied to the design, production, maintenance and operation of software of the PSMS. The software life cycle shall be implemented, operated and maintained based on the program plans of this SPM. During the operation of the PSMS, the responsibility of the software life cycle may become the responsibility of the nuclear plant maintenance or engineering organization. The nuclear plant organization shall maintain the software in accordance with this SPM, and in accordance with their Quality Assurance (QA) manual.

The plans provided in this SPM are applicable to all US-APWR projects. Project specific plan is provided as a Project Plan.

Organization and responsibilities is described in Section 2.2.

The PSMS consists of the application software (project specific) and MELTAC platform. The MELTAC platform includes hardware and basic software for the digital I&C system, and is common to all US-APWR projects. This SPM describes both the application and basic software lifecycle of the PSMS. However, the MELTAC platform, including the life cycle process for the basic software, is described in MUAP-07005 (Reference 2) and is addressed in this SPM to ensure that the as-built basic software is developed and controlled by MELTAC Platform Basic Software Program Manual (Reference 24). The scope of application and basic software is described in Figure 1.2-1. The method of controlling the basic software is described in Sections 3.9.7.12 and 3.11.3.6.

This SPM is also applied to the application software of the augmented quality systems, including following functions as described in Table 7.1-5 of the DCD.

- Safety functions controlled by O-VDU
- Safety Parameter Display System (SPDS)
- Alarms for Credited Manual Operator Actions
- Signal Selection Algorithm
- Risk-significant non-safety I&C systems

Applicability of this SPM for the augmented quality systems is described in Appendix D.



**Figure 1.2-1 Scope of Application and Basic Software**

### **1.3 Applicable Documents**

Applicable documents are identified for the software life cycle activities.

#### **1.3.1 Regulatory Documents and Codes**

- (1) NUREG-0800, BTP7-14 Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control System", March 2007.
- (2) 10 CFR 50 Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.
- (3) Regulatory Guide 1.152 Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", January 2006.
- (4) Regulatory Guide 1.153 Revision 1, "Criteria for Safety Systems", June 1996.
- (5) Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", February 2004.
- (6) Regulatory Guide 1.169 Revision 0, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
- (7) Regulatory Guide 1.170 Revision 0, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
- (8) Regulatory Guide 1.171 Revision 0, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.

- (9) Regulatory Guide 1.172 Revision 0 "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
- (10) Regulatory Guide 1.173 Revision 0 "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.

### 1.3.2 Standards

The following standards are endorsed by Regulatory Guide.

- (1) IEEE Std 603-1991, "IEEE Standard Criteria for Safety System for Nuclear Power Generating Stations".
- (2) IEEE Std 828-1990, "IEEE Standard for Configuration Management Plans".
- (3) IEEE Std 829-1983, "IEEE Standard for Software Test Documentation".
- (4) IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications".
- (5) IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing".
- (6) IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation".
- (7) IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits".
- (8) IEEE Std 1042-1987, "IEEE Guide for Software Configuration Management".
- (9) IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes".
- (10) IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

### 1.3.3 Other Standards

The other standards are applicable to the software life cycle activities, but not endorsed by Regulatory Guide.

- (1) IEEE Std 730-1989, "IEEE Standard for Software Quality Assurance Plans".
- (2) IEEE Std 1058-1988, "IEEE Standard for Software Project Management Plans".
- (3) IEEE Std 1061-1998, "IEEE Standard for a Software Quality Metrics Methodology".
- (4) IEEE Std 1228-1994, "IEEE Standard for Software Safety Plans".
- (5) IEEE/EIA 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207:1995".
- (6) ISO 9001-2008, "Quality management and quality assurance standards".

- 
- (7) NUREG/CR-6101, 1993, "Software Reliability and Safety in Nuclear Reactor Protection System".

#### 1.3.4 Supplemental Documents

The following supplemental documents are applicable to the software life cycle activities

- (1) DCD MUAP-DC007 R3, "US-APWR Chapter7 Instrumentation and Controls". |
- (2) Topical Report MUAP-07004 R7, "Safety I&C Description and Design Process". |
- (3) Topical Report MUAP-07005 R7, "Safety System Digital Platform – MELTAC –". |
- (4) Technical Report JEXU-1012-1132 R3, "MELTAC Platform Basic Software Program Manual". |

#### 1.4 Definitions

The definitions of terminology in this SPM are described in Appendix A.

## 2. SOFTWARE LIFE CYCLE PROCESS CONTROL

### 2.1 Purpose

This SPM describes overall management plans for the PSMS software life cycle process, including design, safety management, manufacturing, integration, Verification and Validation (V&V), training, installation, operation, maintenance, and configuration management.

Table 2.1-1 shows the PSMS application software life cycle plans described in this SPM and their correlation to the plans described in BTP 7-14 (Reference 1).

As defined in various plans described in Section 3, instructions and procedures for each US-APWR project shall be prepared in accordance with the requirements specified in this SPM.

**Table 2.1-1 Correspondence to BTP 7-14**

Plan proposed by BTP 7-14	Section in this SPM discussing the plan
Software Management Plan (SMP)	3.1
Software Development Plan (SDP)	3.2
Software Quality Assurance Plan (SQAP)	3.3
Software Integration Plan (SIntP)	3.4
Software Installation Plan (SInstP)	3.5
Software Maintenance Plan (SMaintP)	3.6
Software Training Plan (STrngP)	3.7
Software Operations Plan (SOP)	3.8
Software Safety Plan (SSP)	3.9
Software Verification and Validation Plan (SVVP)	3.10
Software Configuration Management Plan (SCMP)	3.11
Software Test Plan (STP)	3.12

## 2.2 Organization and Responsibilities

### 2.2.1 Organization

The organizational structure to manage the PSMS application software life cycle process is shown in Figure 2.2-1.

The QA Department, the Design Team (DT), the V&V Team (VVT) and the Project Department are independent of each other. The VVT shall be technically independent, managerially independent, and financially independent from the DT and the Project Department as defined in Annex C of IEEE Std 1012-1998 (Reference 11).



**Figure 2.2-1 Organizational Structure to Manage the Software Life Cycle Process**

### 2.2.2 Responsibilities

The roles and responsibilities for each organization are described as follows;

(1) Quality Assurance Manager (QAM) and Engineer (QAE)

The QAM is responsible for activities that can affect the quality of items and services used in the US-APWR including the PSMS application software. The QAM assigns the QA Engineer (QAE) resources for reviewing Anomaly Reports for adverse trends, and performing QA audits in accordance with IEEE Std 1028-1997 (Reference 9).

The QAM plans and schedules for QA audits.

(2) Project Manager (PJM) and Project Management Team (PMT)

The PJM oversees project activities of the design and manufacturing departments, as well as the interfaces between the design and manufacturing departments and the VVT.

The PJM has no authority to control plans, schedules, budgets or any other V&V activities.

(3) Design Team Manager (DTM) , Design Team Engineer (DTE) and Software Safety Analysis Engineer (SSE)

The DTM is responsible for ensuring adequate qualified staffing to execute all responsibilities of the team, including the responsibilities for the Software Safety Plan (SSP) as described in Section 3.9. The DTM assigns DTE resources for the PSMS application software design and SSE resources for the software safety analysis. The DT conducts all design activities for hardware and software. The DTM assures that the DTE and the SSE correctly design and analyze for the PSMS application software based on technical requirements and the development process in accordance with the SQAP in Section 3.3.

The DTM has no authority to control plans, schedules, budgets or any other V&V activities.

(4) V&V Team Manager (VVTM) and Engineer (VVTE)

The VVTM is responsible for all independent V&V activities and tasks described in Section 3.10 "SVVP" of this SPM. The VVTM assigns VVTE resources for the PSMS application software verification and validation activities which are described in Section 3.10, including assigned resources from other Design Teams. The VVTM is responsible for all V&V activities and shall report the results of V&V activities to the responsible General Manager (GM), QAM and PJM to assure oversight of any necessary corrective actions.

The VVTM has authority to control plans, schedules, budgets or any other V&V activities.

## 2.3 General Requirements

### 2.3.1 Overview of Life Cycle

The development of the PSMS application software is conducted according to a formally defined life cycle process. The formally defined life cycle consists of seven (7) phases, Plant Requirements Phase, System Requirements Phase, Design Phase, Implementation Phase, Test Phase, Installation Phase, and Operation and Maintenance phase.

MHI applies the PSMS application software life cycle process for US-APWR projects described in this SPM based on these experiences, and this PSMS application software life cycle process conforms to BTP7-14 (Reference 1) as shown in Appendix B.

An overview of software life cycle process is described below.

(1) Plant Requirements Phase

This phase defines the requirements and the key design aspects for PSMS that are critical to the plant's design basis for safety, performance and maintainability. This phase determines the industry regulations and standards that apply to the I&C systems and the

---

design process for those systems. The concept phase and requirement phase are combined into one phase as Plant requirements phase in this SPM.

(2) System Requirements Phase

This phase defines the requirements for the PSMS. The system requirement specifications are provided for the PSMS application software in this phase. These specifications explain the performance requirements, functional and Human System Interface (HSI) requirements, and system interfaces requirements. All of these requirements are integrated and documented in the system requirements specification.

(3) Design Phase

This phase defines the specifications for hardware and software. The system design description for the PSMS application software is designed and documented in accordance with the system requirements specification in this phase.

(4) Implementation Phase

During this phase, hardware and basic software for the PSMS are manufactured and configured in the PSMS target system with all power and signal wiring. The PSMS application software is also created for all PSMS controllers and HSI devices. During this phase, the PSMS application and basic software are integrated with the platform hardware for each sub-system of the PSMS.

(5) Test Phase

A series of tests validates the design of the PSMS application software, first at the system level and then at the level of I&C systems integration.

(6) Installation Phase

Activities in this phase include application software installation (or confirmation of software installation), inspection of the software/hardware configuration, and acceptance of the installed configuration through acceptance testing. Acceptance tests are conducted to ensure all equipment has not been damaged during installation or possible shipping, and that all interconnections are correct. Additional functional testing may be conducted as required by plant design.

(7) Operation and Maintenance Phase

During this phase, the I&C systems are in operation. Self-diagnostics continuously monitor performance. Calibration and manual tests are conducted periodically to monitor the PSMS application software. A failure of the PSMS can be immediately detected, and the failed component can be required or replaced. Also, software or hardware may be upgraded to accommodate new requirements, correct design errors or manage obsolescence. Retirement of application software is included in this phase.

### 2.3.2 Classification of Software

The PSMS hardware is classified as Class 1E based on the definition of IEEE Std 603-1991 (Reference 4). The PSMS application software and the basic software are classified as software integrity level (level 4) in accordance with Chapter 1 of RG 1.168 Rev.1.

### 2.3.3 Documentation

Each PSMS application software life cycle plan requires output documents. The output documents are defined in Section 4.

### 3. SOFTWARE LIFE CYCLE PLANS

This section describes the key contents of the 12 plans that govern the application software life cycle process.

(1) Software Management Plan (SPM)

- a. Basic strategy and process for managing the PSMS application software life cycle
- b. Method for monitoring progress against a US-APWR Project Plan
- c. Method for identifying any deviations from a US-APWR Project Plan, or deviations from this SPM
- d. Procedure for managing the PSMS application software

(2) Software Development Plan (SDP)

- a. Technical aspects for the design and development activities of the PSMS application software
- b. Phase activities in the application software life cycle for a US-APWR project
- c. Inputs to and outputs from each activity.

(3) Software Quality Assurance Plan (SQAP)

- a. Organizational responsibilities, security, quality assurance requirements, procedure and methodology for application software
- b. Metrics used to measure the specific quality
- c. Reviews and audits in accordance with IEEE Std 1028-1997
- d. Problem reporting and corrective action

(4) Software Integration Plan (SIntP)

- a. Procedures for software integration
  - 1) Integrate application software units together to form Application Execution Module
  - 2) Integrate the result of 1) with the target CPU hardware modules
  - 3) Test the resulting integrated product

(5) Software Installation Plan (SInstP)

- a. Procedures for software installation

- 1) Plan installation
- 2) Distribute software
- 3) Install software
- 4) Accept software in operational environment

(6) Software Maintenance Plan (SMaintP)

- a. Processes for correcting faults and errors of the PSMS application software during plant operation
- b. Activities for the maintenance of the PSMS application and basic software
  - 1) Failure reporting
  - 2) Fault correction
  - 3) Re-release software
  - 4) Configuration management system

(7) Software Training Plan (STrngP)

- a. Metrics for the effectiveness of the training
- b. Procedures for software training
  - 1) Training activities
  - 2) Software training manual and material
- c. Specification of effective and sufficient training resources

(8) Software Operations Plan (SOP)

Operation of the PSMS application software during the Operation and Maintenance phase

(9) Software Safety Plan (SSP)

- a. Methodologies for software safety for all life cycle process of PSMS application software
- b. Definition of technical requirements and organizational responsibilities for specific software safety activities
- c. Software Safety Management (SSM) in accordance with IEEE Std 1228-1994 (Reference 10)

- d. Software Safety Analysis (SSA)
  - 1) Plant requirement phase SSA
  - 2) System requirement phase SSA
  - 3) Design and implementation phase SSA
  - 4) Test phase SSA
- (10) Software Verification and Validation Plan (SVVP)
  - a. V&V activities during the PSMS application software life cycle phases
  - b. Procedures and methodologies for each V&V activity in accordance with IEEE Std 1012-1998
    - 1) System requirement phase V&V
    - 2) Design phase V&V
    - 3) Implementation phase V&V
    - 4) Test phase V&V
    - 5) Installation V&V
    - 6) Maintenance and operation V&V
  - c. V&V reporting requirements and V&V anomaly reporting and resolution
- (11) Software Configuration Management Plan (SCMP)
  - a. Methods required for maintaining the project specific US-APWR PSMS application software configuration items (CIs) in a controlled configuration
  - b. The six classes of information required by IEEE Std 828-1990 (Reference 13)
    - 1) Introduction
    - 2) SCM management
    - 3) SCM Activities
    - 4) SCM Schedules
    - 5) SCM Resources
    - 6) SMC Maintenance
  - c. Procedure in each phase

(12) Software Test Plan (STP)

a. Methods for the following V&V test activities

1) Component V&V Test

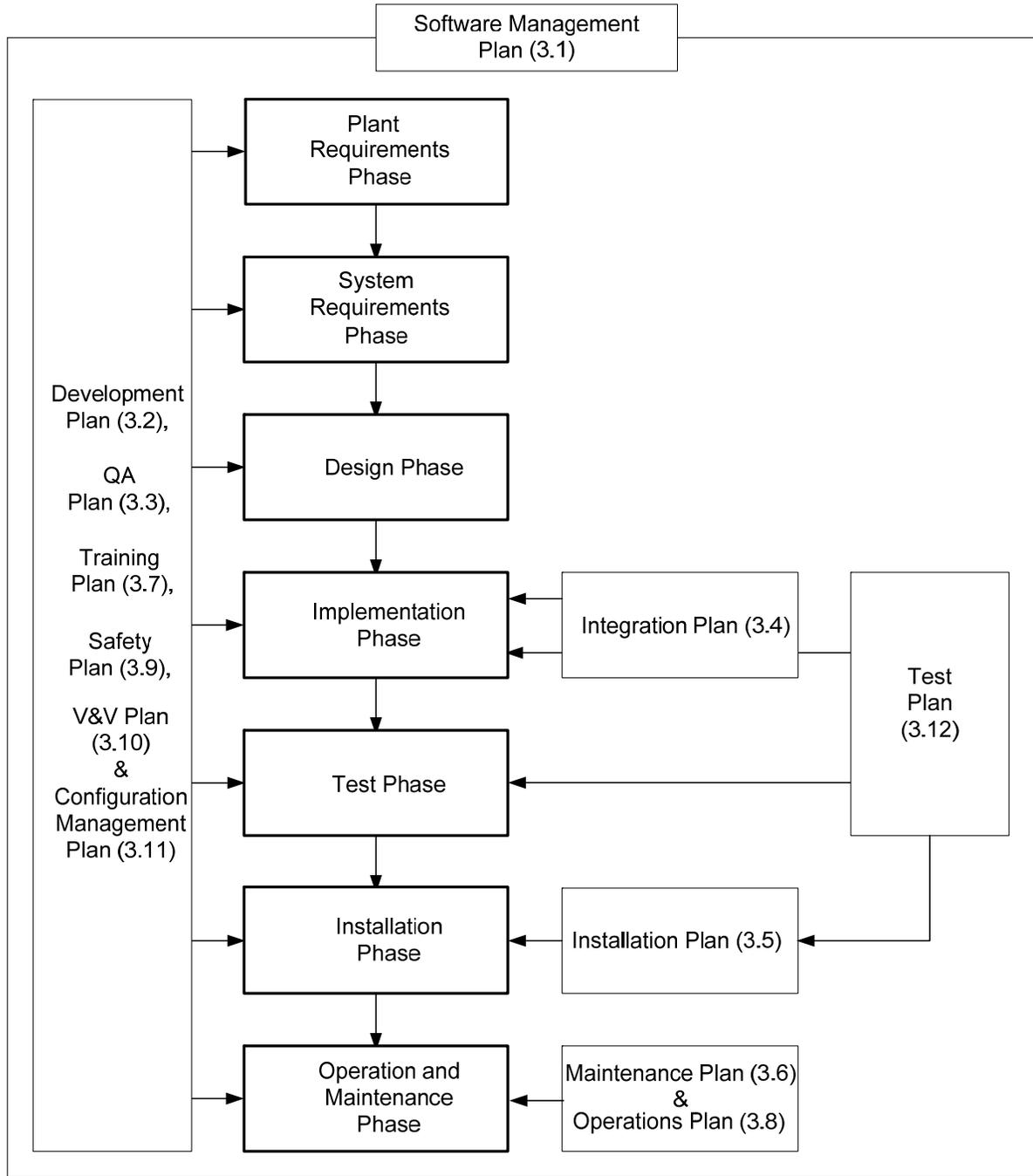
2) Integration V&V Test

3) System V&V Test

4) Acceptance V&V Test

b. Test documents in accordance with IEEE Std 829-1983 (Reference 15)

The relationship of the software life cycle plans to each phase of the software life cycle is shown in Figure 3-1.



(\*.\*) means the section in this SPM.

**Figure 3-1 Overview of Software Life Cycle Plan**

### 3.1 Software Management Plan (SMP)

#### 3.1.1 Purpose

This Software Management Plan (SMP) describes the overall management process for the PSMS application software life cycle. An overview and a description of the general requirements for the PSMS application software life cycle process and a US-APWR project are provided in Section 2.3 “General Requirements” of this SPM.

This SMP describes the basic strategy and process for managing the PSMS application software life cycle process. It also describes the method for monitoring progress against the US-APWR Project Plan, and the method for identifying any deviations from a US-APWR Project Plan, or deviations from this SPM. Project oversight, control, reporting, review, and assessment activities are all described within this SMP.

This SMP complies with the guidance and standards identified in Section 3.1.10.

This SMP describes the general functions of the PSMS application software which are expected to be delivered by a Project, and how each of these functions shall be traceable to the requirements identified in the Plant Requirements Phase output documents. In addition, this SMP describes the following items:

- An overview of the PSMS where the application software will reside.
- General overview of a US-APWR application software project.

##### 3.1.1.1 Functions

The PSMS application software governed by this SMP implements the functions of the PSMS, which includes the Reactor Protection System (RPS), Engineered Safety Features Actuation System (ESFAS), Safety Logic System (SLS) and Safety related Human System Interface System (HSIS) for each US-APWR project. The PSMS application software is integrated with the MELTAC platform that is provided with the basic software. The basic software is controlled and maintained under the MELTAC Platform Basic Software Program Manual (JEXU-1012-1132) (Reference 24).

The key functions of the PSMS application software are:

- Process input process signals and manual system level actuation signals for the reactor protection functions and the Engineered Safety Features (ESF) actuation functions.
- Process signals such as analog to digital (A/D) conversion, input signal and setpoint comparison, trip/actuation algorithm calculations, and a 2-out-of-4 logic.
- Initiate reactor trip signal and engineered safety features actuation signals.
- Process input process signals for post accident monitoring and safe shutdown instrumentations.

- Provide manual components level controls for credited operator actions for accident mitigation and for achieving and maintaining safe shutdown.
- Initiate operating bypasses, maintenance bypasses, system level reset of automatic safety actuation signals and periodic surveillance testing.
- Provide safety related HSI for the Main Control Room and Remote Shutdown Room to monitor, control and test safety functions.

### 3.1.1.2 Overview

To implement the PSMS application software functions listed in Section 3.1.1.1 with the necessary performance and reliability, the PSMS application software has the following configuration and features:

- The PSMS is built on the MELTAC platform as described in Technical Report MUAP-07004 “Safety I&C System Description and Design Process” (Reference 3).
- The MELTAC platform (i.e., hardware and basic software) is qualified and suitable for Class 1E applications, as described in Technical Report MUAP-07005 “Safety System Digital Platform –MELTAC-” (Reference 2).
- The PSMS application software is fully qualified by Independent V&V activities as described in Section 3.10 “SVVP” of this SPM.
- The PSMS is designed with four fully redundant and independent divisions (four trains) with a 2-out-of-4 trip/actuation logic to satisfy the reliability goals of the US-APWR.
- The PSMS application software is distributed among multiple MELTAC controllers within each PSMS division (train).
- The Safety Visual Display Unit (S-VDUs) provides the HSIS monitoring of all safety related plant instrumentations and controls for all safety related components that interface with the PSMS.
- Communication independence between redundant PSMS divisions (trains) and between the PSMS and the Plant Control and Monitoring System (PCMS).

### 3.1.2 Organization/Responsibilities

All organizations involved in the PSMS application software life cycle process described in this SPM shall follow internal procedures that implement the requirements of this SPM and all other sections of this SPM. Internal procedures shall be controlled in accordance with Section 1 “Organization” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27).

The Project Plan for each US-APWR project shall include the following information, as a minimum:

- Project Purpose

- References to the latest applicable versions of the output documents from the Plant Requirements Phase (for compliance with applicable regulations, codes and standards)
- Responsible organizations
- Project-specific customer requirements
- Project schedule
- Project budget

Each US-APWR Project Plan is developed by a Project Management Team (PMT) under the direction of a Project Manager (PJM). The PJM is responsible for reviewing and approving the Project Plan.

Section 2.2 of this SPM describes the software project organizational structure, describes the interfaces and boundaries between the US-APWR project organization and other MHI organizations, and describes the management reporting channels.

The organizational structure and independence between the organizations, as defined in Section 2.2, shall be maintained for each phase of the software life cycle process. The division of responsibility between companies for fulfilling a particular organizational role for a specific life cycle phase, or for fulfilling all organizational roles for a specific life cycle phase, shall be defined in each US-APWR Project Plan.

Section 2.2 of this SPM describes the roles and responsibilities for personnel assigned to activities described in this SPM. Section 2.2 of this SPM also provides a policy statement that the primary responsibility for assuring the quality of the PSMS application software is assigned to the personnel responsible for application software development.

Section 2.2 of this SPM also describes the criteria and responsibilities for assuring independence of the QA organization (QAM and QAE) and the V&V organization (VVTM and VVTE) from the PSMS application software design organization (DTM, DTE and SSE). In particular, Section 2.2 requires VVT independence in accordance with Annex C of IEEE 1012-1998 (Reference 11).

The organizational roles and responsibilities for the PSMS application software described in Section 2.2 of this SPM satisfy the requirements in Section B.3.1.1 of BTP 7-14 (Reference 1) and Section 3.1.1 of NUREG/CR-6101 (Reference 26).

### **3.1.3 Oversight**

#### **3.1.3.1 Basic Strategy**

In managing the PSMS application software life cycle process, the following basic management strategies shall be implemented to achieve high reliability and design quality of the PSMS application software.

- Ensure independence between the life cycle management organizations as described in Section 2.2 of this SPM.

- Ensure the PSMS application software life cycle activities are conducted in accordance with this SPM.
- Ensure that if any deviations from the SPM are detected and reported, corrective actions shall be initiated in accordance with Section 16 “Corrective Action” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27).
- Ensure that the Design Team (DT) who produces each PSMS application software design related output has the primary responsibility for quality of these outputs.
- Ensure that the DT understands that the V&V and QA activities are truly independent of the design activities and can only confirm that the design outputs products are of high quality.

### 3.1.3.2 Other Considerations

- The DTM defines and controls precise milestones for design activities of the PSMS application software life cycle process in the project schedule defined in the Project Plan, and develops each PSMS application software product in the order required by the schedule.
- Progress of the design activities shall be confirmed by regular DT meetings to check the design activity status and deviations.
- Any design activities that deviate from the project schedule are investigated for the reason for the deviation, and corrective actions shall be identified promptly.
- The VVT independently defines and controls milestones for each V&V activity of the PSMS application software life cycle, and performs the required V&V activities in the order required by the V&V schedule.
- Progress and effectiveness of V&V activities shall be confirmed by regular VVT meetings to check the V&V activity status and deviations.

### 3.1.4 Security

Security controls shall be implemented in the application software environment throughout each phase of the PSMS application software life cycle process as follows:

- There shall be no connection between the PSMS application software development tools and the business Local Area Network (LAN) or the Internet.
- The application software development tools shall be checked regularly to ensure they are free from “Trojan horses” computer viruses, worms and any other malicious codes.

In addition to the general security requirements described above, additional security measures for specific PSMS application software life cycle process are described in the other life cycle plans described within this SPM.

Above security requirements of the SMP shall be conducted in accordance with RG 1.152 Rev2 (Reference 17).

A conformance evaluation and security assessments are described in Appendix C of this SPM.

### 3.1.5 Measurement

The following measures shall be used to monitor and control the progress of the PSMS application software life cycle process.

Data for these measures shall be collected and analyzed to review to what extent the PSMS application software is efficiently managed and implemented by this SMP in accordance with Clause 4.5.3.6 of IEEE Std 1058-1998 "Metrics collection plan" (Reference 28).

- Progress status of documents in comparison to the project schedule. This may be expressed as a percentage (progress rate).
- The number of open items on the Problem List as described in Section 3.1.8.2 "SMP" of this SPM.
- The number and severity level of V&V Anomaly Reports as described in Section 3.10 "SVVP" of this SPM.
- The number of design changes.

### 3.1.6 Procedures

#### 3.1.6.1 Objective and Priorities

The PSMS application software projects are authorized and initiated by the PJM.

The DTM shall describe the objectives and priorities for management activities and specify the preliminary schedule, requirements, scope and budget for the PSMS application software development, and provide this information to the PJM for incorporation into the Project Plan. The DTM shall include any necessary assumptions, dependencies and constraints in the information provided to the PJM.

- assumption: degree of risk
- dependency: relationship between activities, or activity and milestone
- constraints: options regarding scope, staffing and schedule

The VVTM has the authority to approve the release of the design outputs of the PSMS application software.

#### 3.1.6.2 Risk Management

Risk management shall be performed in the PSMS application software life cycle process. The

Project Manager shall evaluate potential risk areas and determine if any risks should be periodically assessed in the course of the project.

Identified risks shall be placed on a Risk Matrix that describes each risk and the methods to be used for assessing and mitigating them as described in Section 3.1.8.2. The Design Team Manager (DTM) shall initiate and maintain the Risk Matrix, including updates to account for new risk items identified through periodic review methods described in the SQAP (Section 3.3 of this SPM).

The Project Manager shall employ the following risk mitigation strategies for risks identified on the Risk Matrix:

- Analyze identified risks to determine their relative rank and priority.
- Develop contingency plans for high priority or safety significant risks.
- Immediately initiate corrective actions if an identified risk becomes an actual problem.
- Maintain a working environment that supports effective communication of emerging risks and problems.

### **3.1.6.3 Monitoring and Controlling**

Application software life cycle activities shall be executed and controlled by procedures that implement each of the plans in this SPM (Sections 3.1 "SMP" through 3.12 "STP").

- The Managers identified in Section 2.2 shall be responsible for the activities described Sections 3.2 to 3.12 of this SPM.
- Meetings shall be held periodically to review and confirm the status of project activities to identify any issues to be addressed, and to initiate corrective actions if needed.
- The PMT shall monitor, review and periodically report project progress and the Problem List to the PJM.

Each organization involved in the PSMS application software life cycle process shall develop internal procedures for their areas of the PSMS application software life cycle process. The specific procedures used to implement the requirements of this SPM shall be specified in the Project Plan for each US-APWR project. Should the division of responsibility for the PSMS application software life cycle process change or the procedures change, each US-APWR Project Plan shall be revised to invoke the appropriate procedures.

Implementing procedures shall be controlled as described in Section 6 "Document Control" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27).

The PJM is responsible for coordination of communications and information transfer between the following entities to ensure that organizational interfaces on the PSMS application software project are effective:

- The DT and the customer
- The DT and the QA Department

- The DT and the Verification and Validation Team (VVT)

#### **3.1.6.4 Staffing Plan**

The DTM and the VVTM shall specify the number of personnel required to conduct the design activities and the V&V activities of each US-APWR project and develop staffing plans in accordance with the US-APWR project schedule. However, the V&V activities shall be controlled solely by the VVTM, and shall not be influenced by the DTM or the PJM.

#### **3.1.6.5 Document Plan**

All outputs described in this SPM, including software configuration items and documents, are listed in Section 4.0 of this SPM. The responsible organization for each output is included in Section 4.0 of this SPM.

#### **3.1.6.6 Change Plan**

A means of managing externally or internally driven changes to any of the PSMS application software and related documents is described in the SCMP (Section 3.11 of this SPM).

The organizations responsible for assessing potential changes to any of the PSMS application software and related documents in this SPM (Section 3.1 through 3.12) are described in the SCMP.

#### **3.1.7 Budget**

Sufficient resources shall be made available, such as financing, human resources and tools for each organization that is assigned activities described in this SPM.

The QAM/QAE and the VVTM/VVT shall be provided budgets that are independent from the DT budget. Before proceeding beyond the initiation of a project, the required resources shall be identified. Resource utilization reports shall be periodically prepared and assessed by each responsible manager to ensure adequate resources are available throughout the PSMS application software life cycle process.

In addition, budget reports for each department shall be periodically prepared and assessed by each manager to ensure availability of resources when needed for executing the requirements of this SPM.

#### **3.1.8 Methods/Tools**

##### **3.1.8.1 Methods**

During each project phase, project management shall be executed in accordance with the basic process described in Section 3.1.6.

##### **3.1.8.2 Tools**

The following tools shall be used for the PSMS application software project management, as a minimum:

### (1) Project Plan

A Project Plan shall be initiated and maintained by the Project Manager for each development or change activity that produces or affects an application software configuration item, with the exception of editorial changes to documents that do not affect any functional, performance, safety or quality characteristics of the application software (such document changes may be the result of a management review, design review, or QA Audit, and shall be controlled as described in the SQAP).

The following information shall be included in the Project Plan, as a minimum:

- a. Scope Description
- b. Summary Description of Systems, Components or configuration items to be produced or affected
- c. List of Nonconformances or Corrective Action Reports to be resolved by the project (if any)
- d. Results of Configuration Control Board (CCB) activities (if required), as described in the SCMP (Section 3.11 of this SPM)
- e. Project Schedule (with periodic updates for progress and schedule changes), including milestones, hold points and review schedules

### (2) Risk Matrix

The Project Manager shall evaluate potential risk areas and determine if any risks should be periodically assessed in the course of the project. Identified risks shall be placed on a Risk Matrix that describes each risk and the methods to be used for assessing and mitigating them. The DTM shall initiate and maintain the Risk Matrix, including updates to account for new risk items identified through periodic reviews as described in the SQAP (Section 3.3 of this SPM).

The following risk areas shall be considered for inclusion on the Risk Matrix:

- Previous project experience and lessons learned
- Industry operating experience
- US-APWR operating experience
- Complexity of the proposed change, including impact on multiple configuration items
- Internal and external organizational interfaces
- Schedule pressure
- Insufficient resources
- Need for specialized resources
- Results of previous QA Audits and Corrective Action Reports
- Previous V&V Anomaly Reports

- Previous Nonconformance Reports

### (3) Problem List

Items on the Risk Matrix that become actual issues, or any other issues that occur such as technical problems, significant design review comments, organizational conflicts, facility and environment problems, and resource problems in the course of a project shall be identified and reported on a Problem List.

The Problem List shall be maintained and updated by the Project Manager as problems are identified, changed, and closed. Activities to mitigate and close each identified problem shall be described in the Problem List.

Problems that can impact a critical safety function as described in the SSP (Section 3.9 of this SPM) require the initiation of a Nonconformance Report as described in the SQAP.

#### 3.1.9 Personnel

DTE, including individuals assigned to perform the software safety analyses activities described in the SSP (Section 3.9 of this SPM) shall be trained and qualified prior to performing any of the activities assigned to the DT as described in this SPM. The DTM is responsible for assuring that DTE are trained and qualified for their assigned activities.

The VVTE, including individuals assigned to perform V&V of the software safety analyses outputs from the DT, shall be trained and qualified prior to performing any of the V&V activities assigned to the VVT as described in the SVVP and STP (Sections 3.10 and 3.12 of this SPM, respectively). The VVTM is responsible for assuring that the VVTE are trained and qualified for their assigned activities.

Training and qualification of the DTE and VVTE shall include technical competencies, software engineering competencies, and the PSMS application software life cycle process knowledge as determined by the DTM and the VVTM, respectively.

#### 3.1.10 Standards

This SMP complies with the following guidance and standards.

- Clause 3 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22)
- Section 3.1.1 of NUREG/CR-6101 (Reference 26)

## 3.2 Software Development Plan (SDP)

### 3.2.1 Purpose

This Software Development Plan (SDP) describes the design and development activities of the PSMS application software.

The purpose of this SDP is to:

- Describe the phase activities in the application software life cycle for a US-APWR project
- Describe the inputs to and outputs from each activity.

This SDP complies with the guidance and standards identified in Section 3.2.9.

### 3.2.2 Organization

#### 3.2.2.1 Application Software Life Cycle Process

As described in Section 2.3.1, the PSMS application software life cycle process consists of the following seven phases. Figure 3.2-1 illustrates the application software life cycle.

1. Plant Requirements
2. System Requirements
3. Design
4. Implementation
5. Test
6. Installation
7. Operation and Maintenance

The activities illustrated in Figure 3.2-1 shall be performed by the Project Department, the Design Team (DT), the Verification and Validation Team (VVT) and the Quality Assurance Departments described in Section 2.2 of this SPM. Figure 3.2-1 also provides the organizational interfaces and boundaries.

The activities required of each organization are listed in Tables 3.2-1 to 3.2-4, including the phase-specific activity inputs and outputs.

#### 3.2.2.2 Comparison of Application Software Life Cycle Activities to IEEE Std 1074-1995

The relationship of the application software life cycle to IEEE Std 1074-1995 is mapped in Table 3.2-5, where it demonstrates that all mandatory activities are accounted for in the PSMS application software life cycle process.

### 3.2.3 Oversight

Project oversight activities and measures are described in Section 3.1 “SMP” of this SPM (Section 3.1.3).

### 3.2.4 Risks

Risk management activities and measures are described in Section 3.1 “SMP” of this SPM (Section 3.1.6).

### 3.2.5 Measurement

Measurements used to monitor and control the technical and quality aspects of the application software development process shall be performed as described in Section 3.3 “SQAP” of this SPM (Section 3.3.4).

### 3.2.6 Procedures

This section describes the inputs, the activities and the outputs of each application software life cycle phase. An accompanying illustration is provided in Figure 3.2-1 (in this SDP).

The body of this SDP annotates specific activities in parentheses, such as “(P-2),” for cross-reference to Figure 3.2-1. The first digit means the type of activity, such as “P” for “Project” and the second digit means the application software life cycle phase where it is performed as listed in Section 3.2.2.1. For example, “(P-2)” means a Project Management activity, as listed in Table 3.2-1, in the System Requirements Phase (Item 2 in the list provided in Section 3.2.2.1).

Software safety analyses shall be performed as described in Section 3.9 “SSP” of this SPM.

#### 3.2.6.1 Plant Requirements Phase

The Plant Requirements Phase is defined as the activities that are conducted in the course of US-APWR Design Certification (DC) and COL Applications. This phase defines the key design aspects for the PSMS. The Plant Requirements Phase consists of the following activities.

1. Develop/Maintain Platform (B-1)
2. Develop/Maintain Plant Requirements (D-1)

##### 3.2.6.1.1 Develop/Maintain Platform



### 3.2.6.1.2 Develop/Maintain Plant Requirements



### 3.2.6.2 System Requirements Phase

The System Requirements Phase defines the requirements for the PSMS. These requirements include performance, functional and Human System Interface (HSI) requirements, and system interface requirements.

The System Requirements Phase consists of the following activities:

1. Develop System Requirements (D-2)
2. System Requirements Phase V&V (V-2)

#### 3.2.6.2.1 Develop System Requirements



### 3.2.6.2.2 System Requirements Phase V&V Activity

### 3.2.6.3 Design Phase

The Design Phase transforms the system requirements into the system design description. The Design Phase consists of the following activities:

1. Develop System Design (D-3)
2. Design Phase V&V (V-3)

#### 3.2.6.3.1 Develop System Design

### 3.2.6.3.2 Design Phase V&V

### 3.2.6.4 Implementation Phase

The Implementation Phase consists of the following activities.

1. Manufacture Hardware
2. Develop Application Software (D-4A)
3. Integrate Software with Hardware (D-4B)
4. Implementation Phase V&V (V-4A)

#### 3.2.6.4.1 Manufacture Hardware

#### 3.2.6.4.2 Develop Application Software

#### 3.2.6.4.3 Integrate Software with Hardware

---

[ ]

#### 3.2.6.4.4 Implementation Phase V&V

[ ]

#### 3.2.6.5 Test Phase

The Test Phase consists of the following activities:

1. Integration V&V Test (V-5A)
2. System V&V Test (V-5B)

##### 3.2.6.5.1 Integration V&V Test

[ ]

##### 3.2.6.5.2 System V&V Test

[ ]

#### 3.2.6.6 Installation Phase

The Installation Phase consists of the following activities.

1. Install System (D-6)
2. Installation Phase V&V (V-6A)
3. Acceptance V&V Test (V-6B)

##### 3.2.6.6.1 Install System

[ ]

##### 3.2.6.6.2 Installation Phase V&V

[ ]

##### 3.2.6.6.3 Acceptance V&V Test

[ ]

### 3.2.6.7 Operation and Maintenance Phase

The Operation and Maintenance Phase consists of the following activities.

1. Operations and Maintenance Support (D-7)
2. Maintenance Phase V&V (V-7)

#### 3.2.6.7.1 Operations and Maintenance Support

[ ]

#### 3.2.6.7.2 Maintenance Phase V&V

[ ]

### 3.2.7 Schedule

The software development schedule including milestones, hold points and coordination with the QA Department is provided in the Project Plan, as described in the SMP (Section 3.1 of this SPM).

### 3.2.8 Methods/Tools

The following methods and techniques are used to develop the software.

#### 3.2.8.1 Methods

##### 3.2.8.1.1 Design Verification

The DT shall perform the design verification for all design outputs described in 3.2.6, prior to the distribution of them, as described in the SQAP (Section 3.3 of this SPM). The DTM shall confirm that the qualification and independence criteria are met for the personnel selected for DT:

- A verifier should be a person different from the person who prepared the document or configuration item.
- A verifier should have digital control system and US-APWR knowledge and experience equal to or greater than the person who prepared the document or configuration item.

##### 3.2.8.1.2 Software quality Metrics

The DT shall develop and maintain the software quality metrics as described in Section 3.3 "SQAP" of this SPM (Section 3.3.5.1).

### **3.2.8.1.3 Equipment Qualification**

The DT shall assure the qualification of the MELTAC Platform is maintained as described in Technical Report "Safety System Platform – MELTAC-" (MUAP-07005), to be in compliance with Clause 5.4.2 of IEEE Std 7-4.3.2-2003 (Reference 5), as endorsed by RG 1.152 (Reference 17).

### **3.2.8.4 Software Review and QA Audit**

Software Review and QA Audits are described in Section 3.3 "SQAP" of this SPM (Section 3.3.5.2).

### **3.2.8.5 Software Training**

Software Training is described in Section 3.7 "STrngP" of this SPM.

### **3.2.8.6 Software Safety Analysis**

Software safety analysis is described in Section 3.9 "SSP" of this SPM.

### **3.2.8.1.7 Verification and Validation (V&V)**

Independent V&V is described in Section 3.10 "SVVP" of this SPM.

### **3.2.8.1.8 Software Configuration Management**

Software Configuration Management is described in Section 3.11 "SCMP" of this SPM.

## **3.2.8.2 Tools**

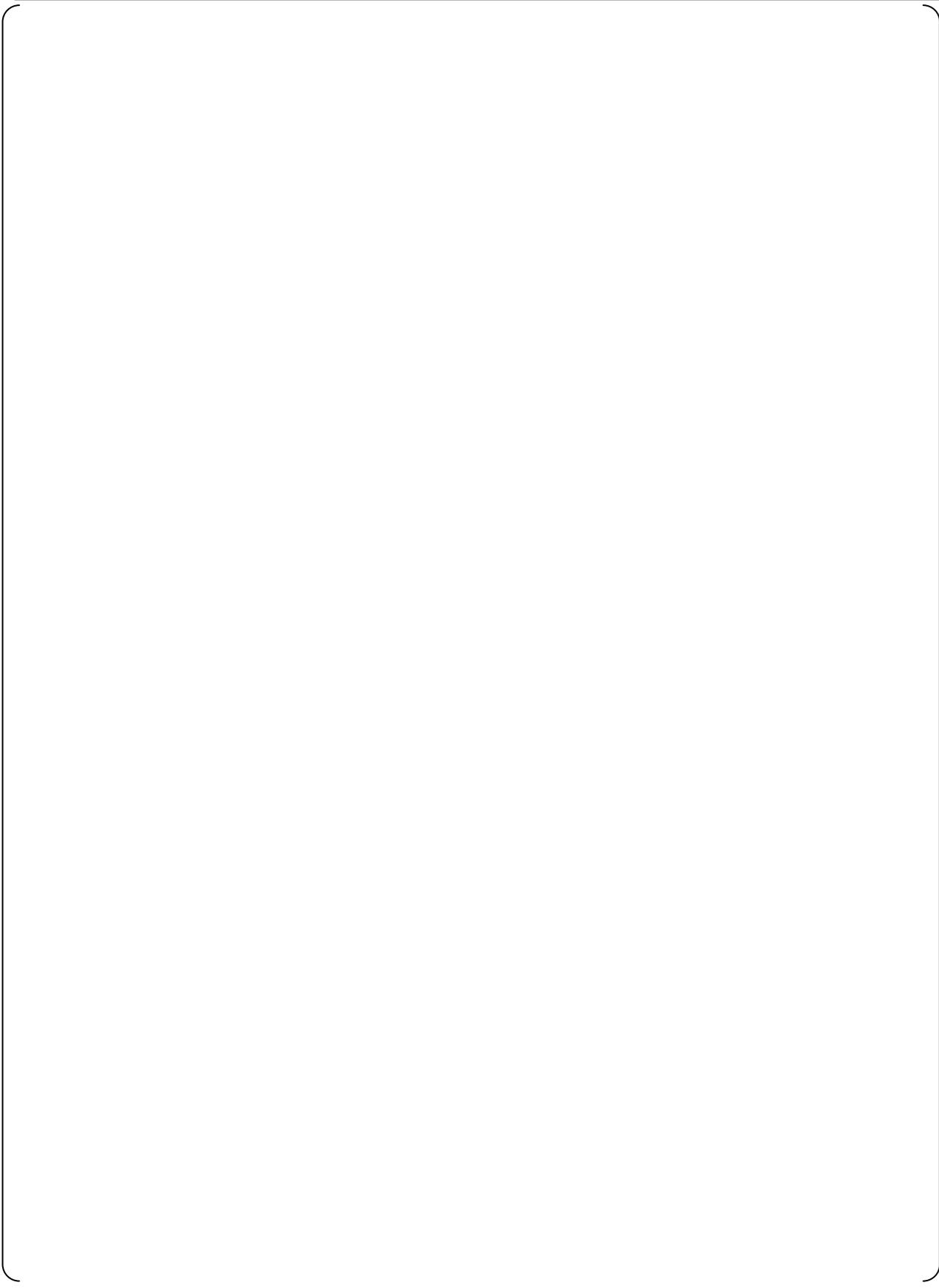
### **3.2.8.2.1 Documented Checklists**

Checklist shall be used to verify the design outputs. Documented Checklist is described in Section 3.3 "SQAP" of this SPM (Section 3.3.7).

### **3.2.8.2.2 Requirements Traceability Matrix**

Traceability of documents between phases shall be identified and documented using Requirements Traceability Matrix (RTM) for verifying the design outputs. The RTM is described in Section 3.10 "SVVP" of this SPM.

### **3.2.8.2.3 Application Software Development Tool**



### 3.2.9 Standards

This SDP complies with the following guidance and standards.

- Clause 5.3 and 5.9 of IEEE Std 603-1991 (Reference 4) which are endorsed by RG 1.153 (Reference 30)
- Clause 5 of IEEE Std 7-4.3.2-2003 (Reference 5) which is endorsed by RG1.152 (Reference 17)
- IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22)
- IEEE Std 830-1993 (Reference 7) endorsed by RG 1.172 (Reference 21),  
with the following exception:  
Clause 4.6 is not applicable to this SDP. The lifecycle activities for the PSMS application software are organized in a waterfall model.
- NUREG/CR-6101 (Reference 26)

Table 3.2-1 Project Department Activities (1/2)



Table 3.2-1 Project Department Activities (2/2)



Table 3.2-2 Design Team Activities (1/9)

Table 3.2-2 Design Team Activities (2/9)

Table 3.2-2 Design Team Activities (3/9)

Table 3.2-2 Design Team Activities (4/9)

Table 3.2-2 Design Team Activities (5/9)

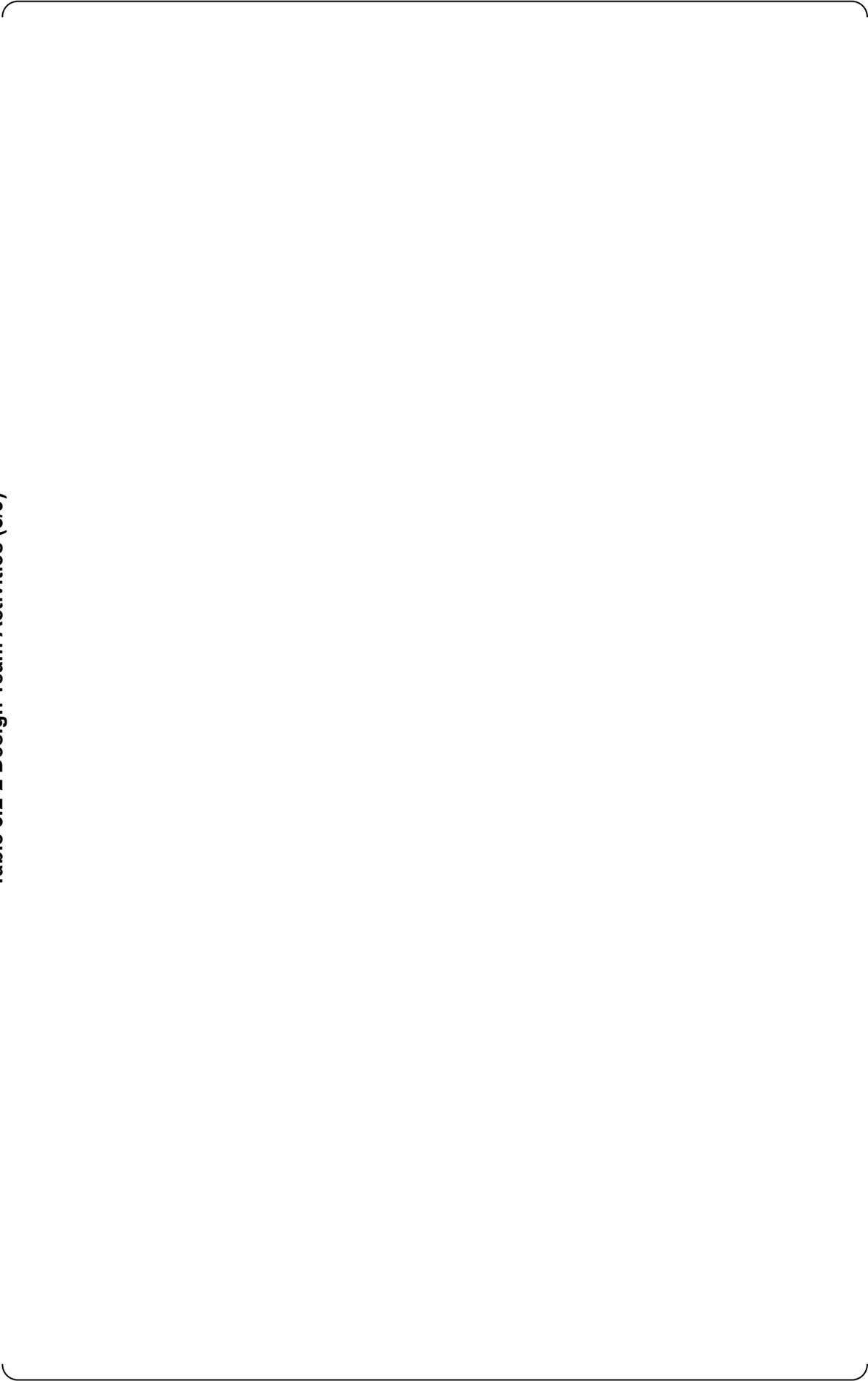


Table 3.2-2 Design Team Activities (6/9)

Table 3.2-2 Design Team Activities (7/9)

Table 3.2-2 Design Team Activities (8/9)

Table 3.2-2 Design Team Activities (9/9)

Table 3.2-3 V&V Team Activities (1/8)

Table 3.2-3 V&V Team Activities (2/8)

Table 3.2-3 V&V Team Activities (3/8)

Table 3.2-3 V&V Team Activities (4/8)

Table 3.2-3 V&V Team Activities (5/8)

Table 3.2-3 V&V Team Activities (6/8)

Table 3.2-3 V&V Team Activities (7/8)

Table 3.2-3 V&V Team Activities (8/8)

Table 3.2-4 QA Department Activities (1/1)

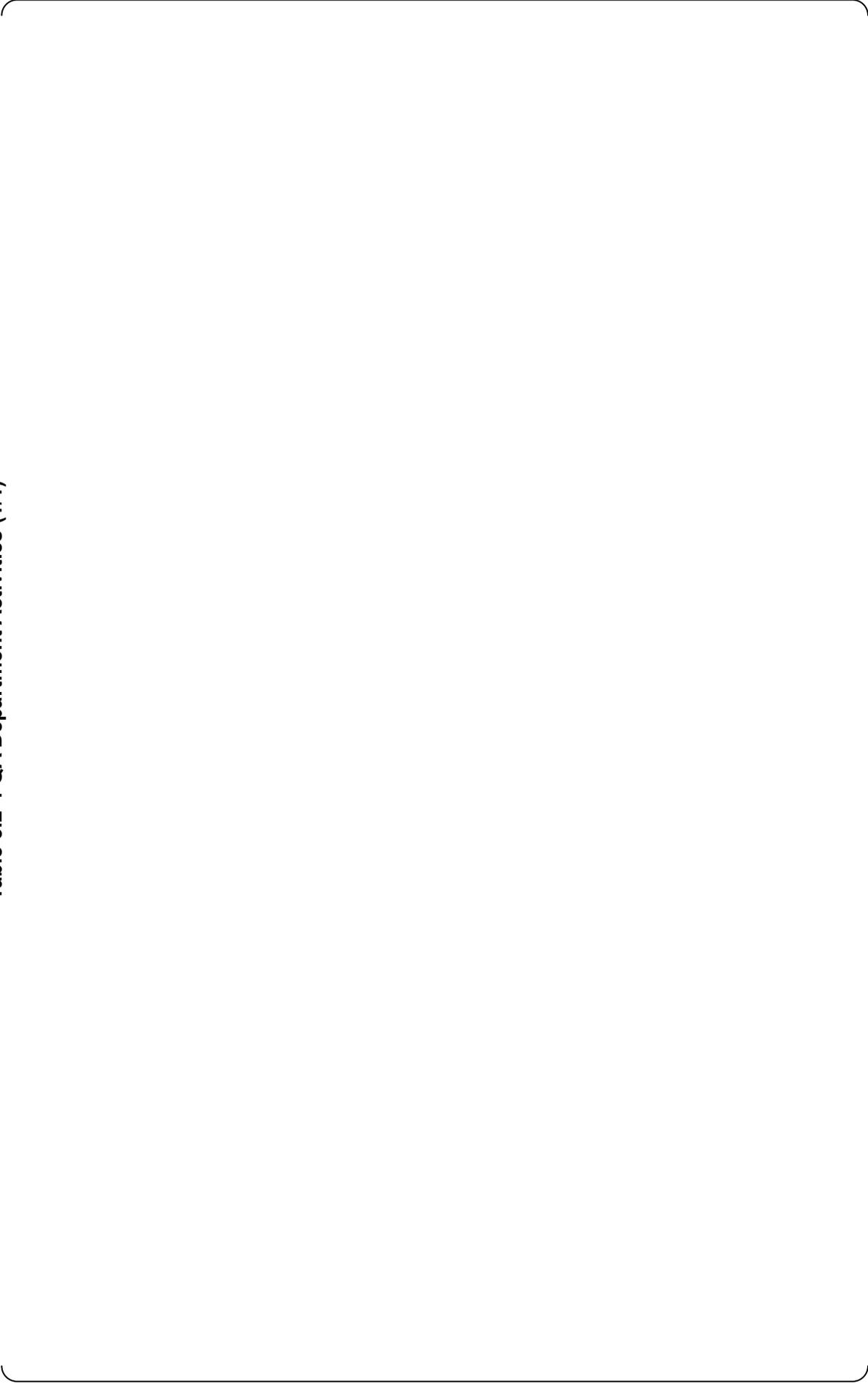


Table 3.2-5 Map of MHI Software Life Cycle Activities to IEEE Std 1074-1995 endorsed by RG 1.173

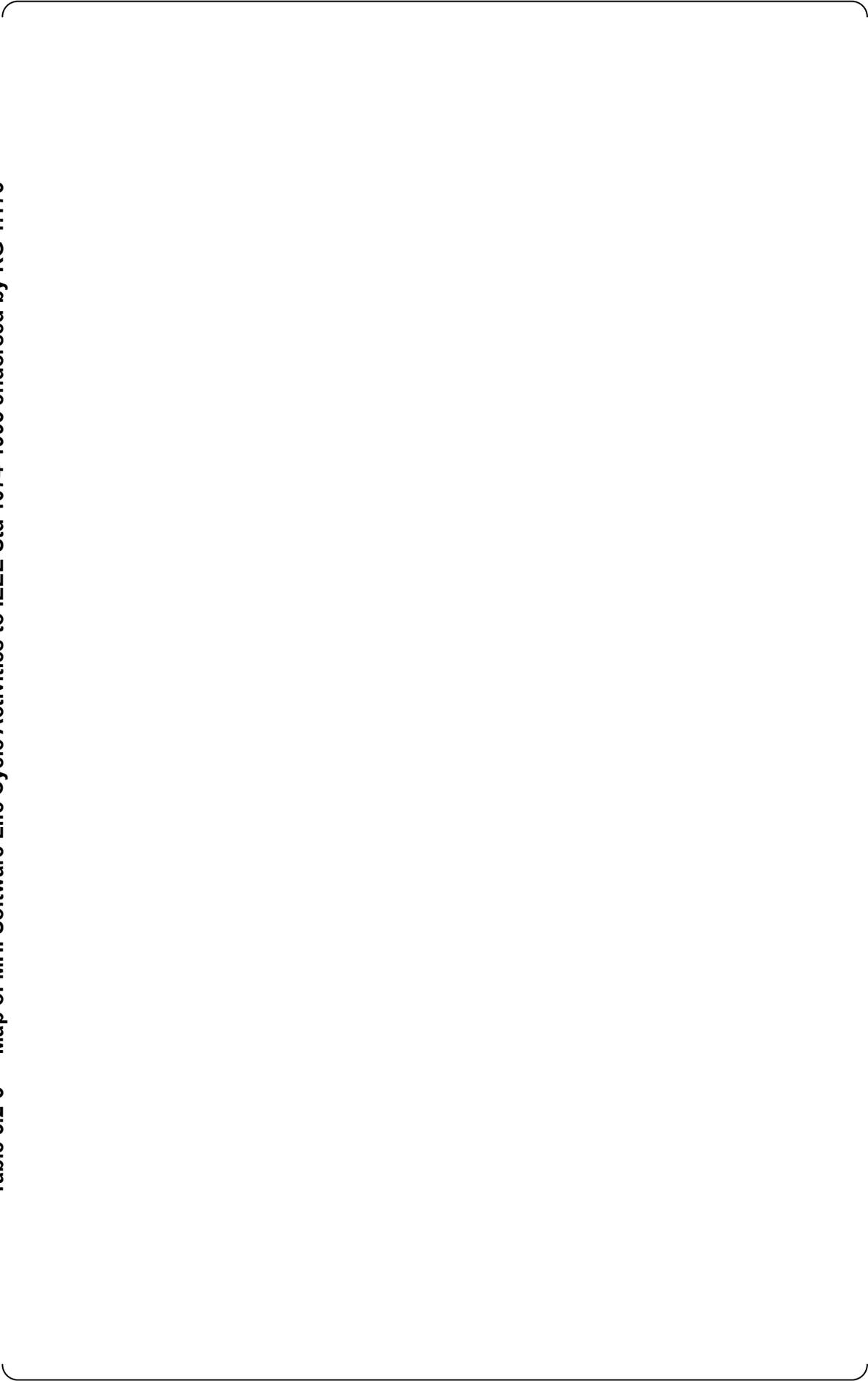


Table 3.2-5 Map of MHI Software Life Cycle Activities to IEEE Std 1074-1995 endorsed by RG 1.173

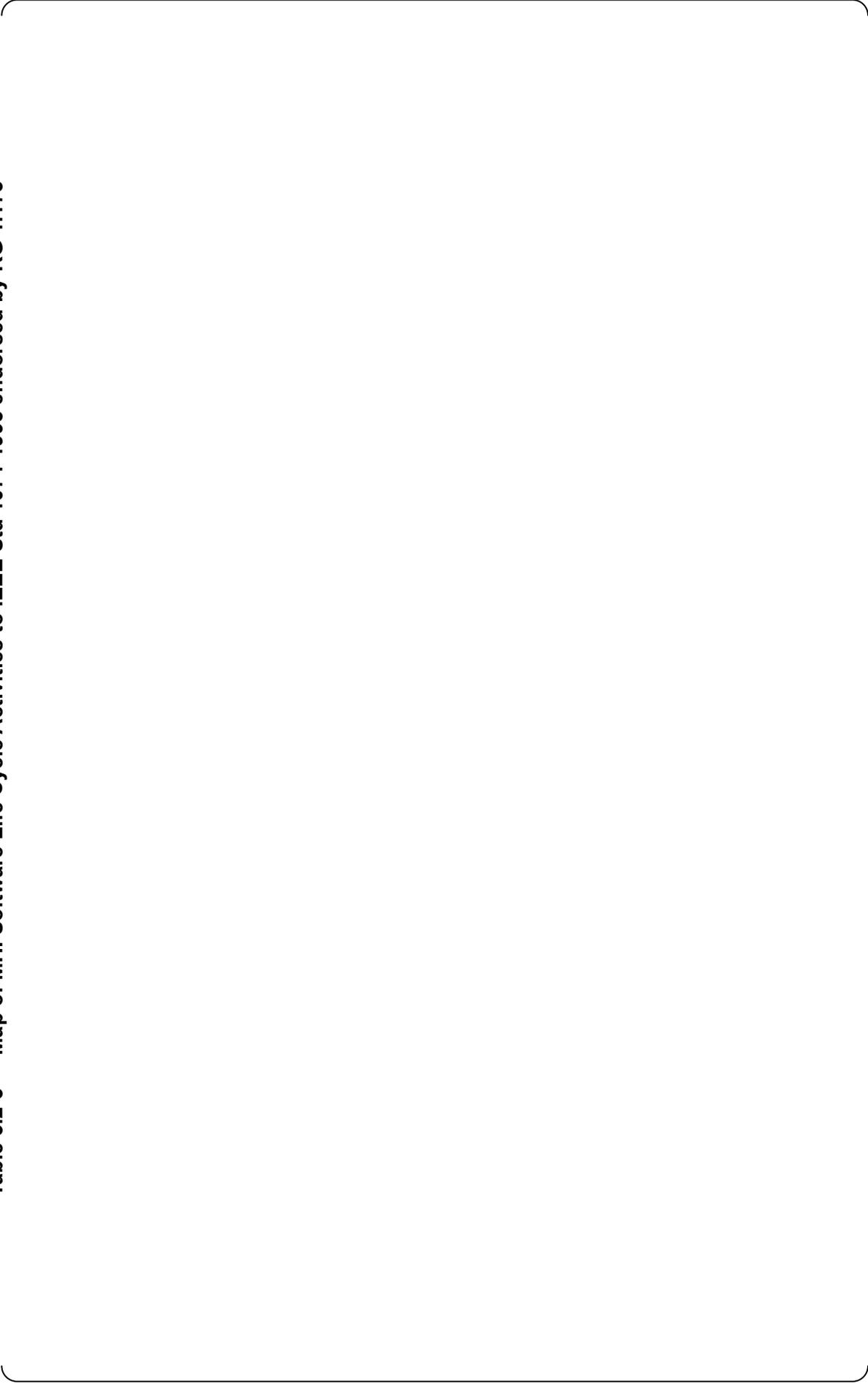


Table 3.2-5 Map of MHI Software Life Cycle Activities to IEEE Std 1074-1995 endorsed by RG 1.173



Table 3.2-5 Map of MHI Software Life Cycle Activities to IEEE Std 1074-1995 endorsed by RG 1.173

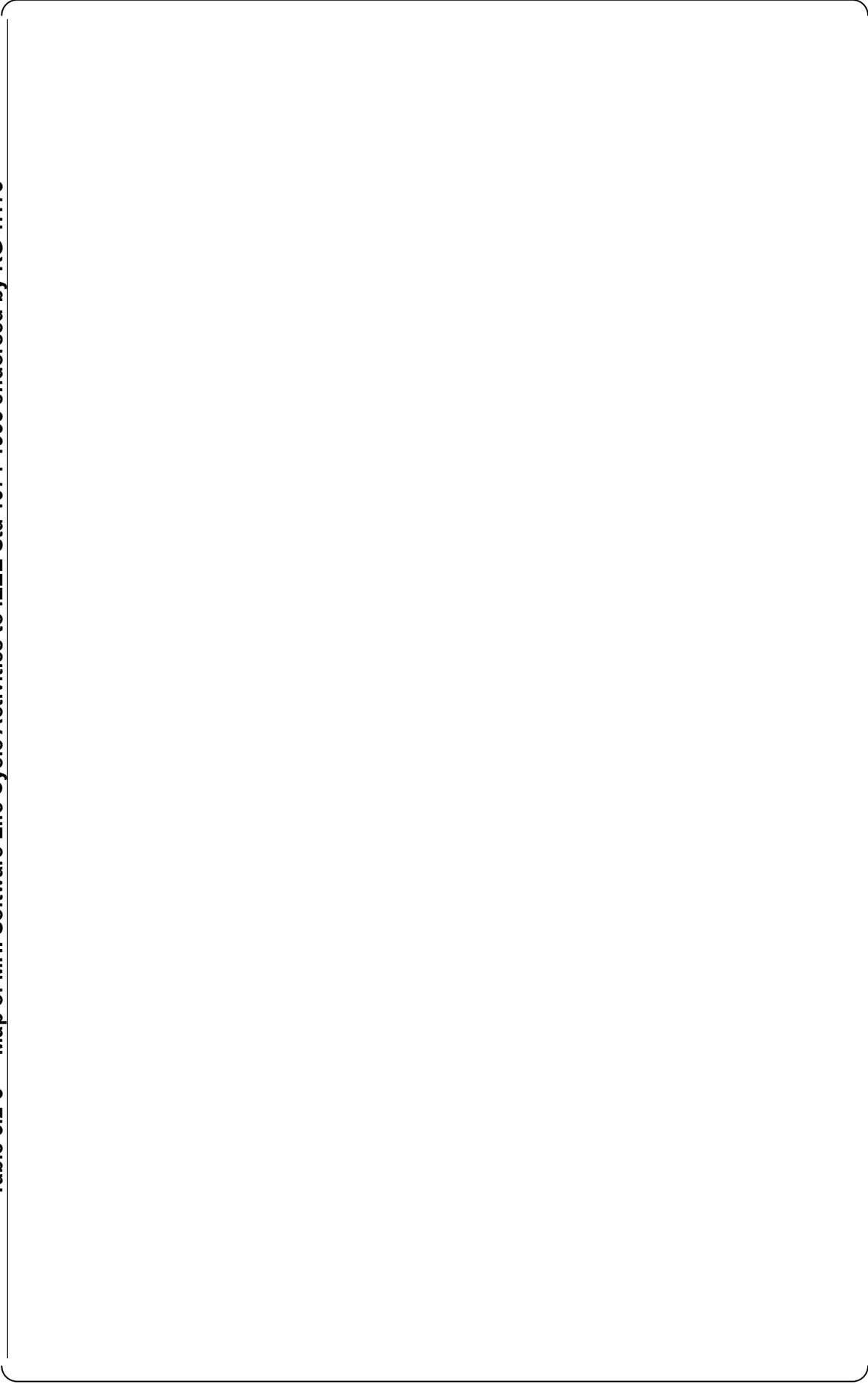


Table 3.2-6 Minimum Contents of SysRS (1/2)

Table 3.2-6 Minimum Contents of SysRS (2/2)

Table 3.2-7 Required SysRS Functional Characteristics

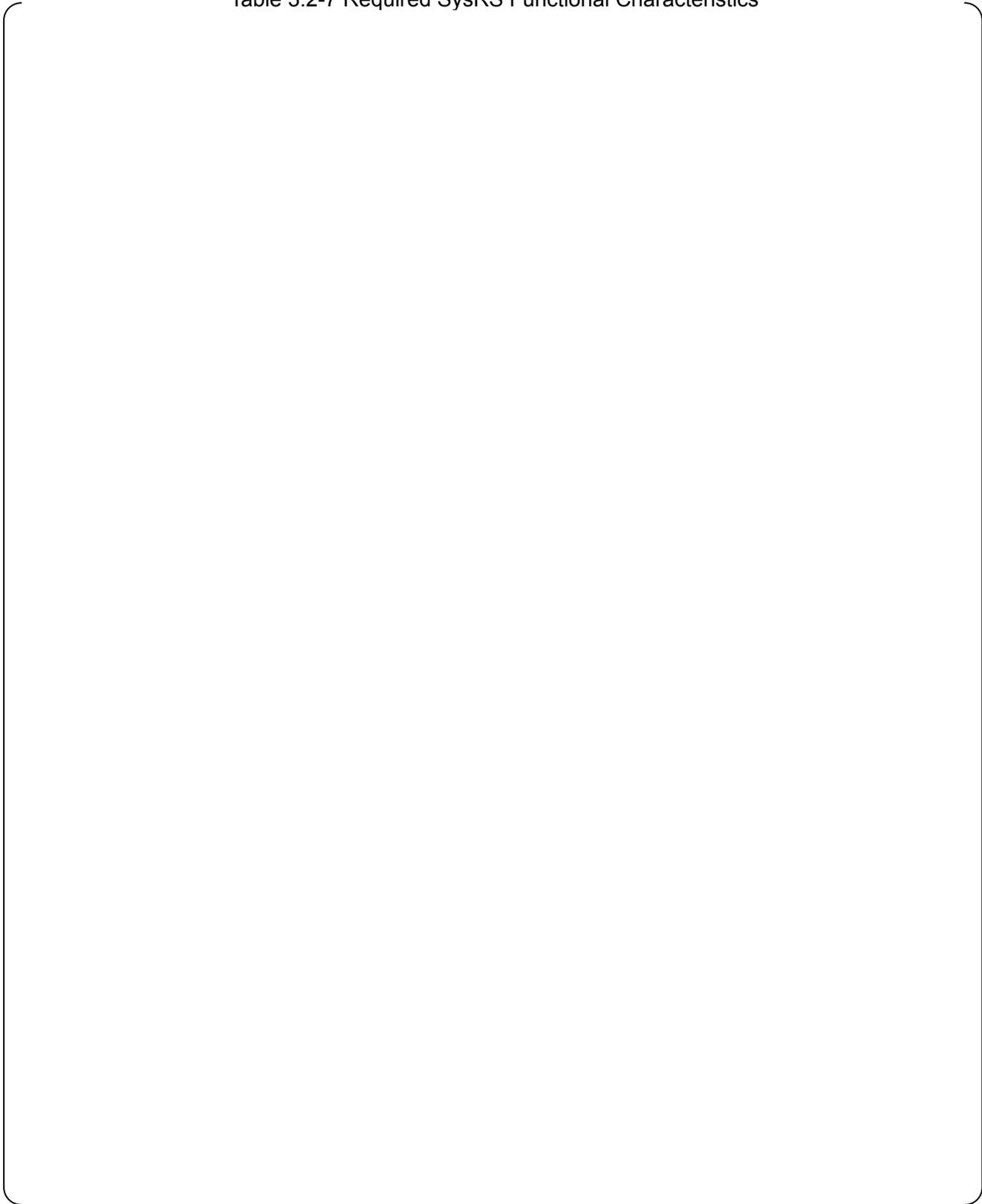


Table 3.2-8 Required SysRS Process Characteristics



Figure 3.2-1 Overview of Application Software Life Cycle Process (1/2)



Figure 3.2-1 Overview of Application Software Life cycle Process (2/2)



Figure 3.2-2 Development Process of the Application Software

### 3.3 Software Quality Assurance Plan (SQAP)

#### 3.3.1 Purpose

This Software Quality Assurance Plan (SQAP) describes the organizational responsibilities, security, quality assurance requirements, techniques, procedures and methodologies for assuring high quality application software for use in the PSMS.

This SQAP is based on the software life cycle process described in the SDP (Section 3.2 of this SPM), and describes the quality methodology to be followed during development and maintenance of the PSMS application software.

This SQAP complies with the guidance and standards identified in Section 3.3.8.

The quality of the following PSMS application software life cycle outputs shall be assured through by applying the QA methods described in this SQAP to activities described in this SPM, with particular emphasis on the following activities and sections:

- (1) The PSMS application software design documents as described in the SDP (Section 3.2 of this SPM)
- (2) The PSMS application software test documents as described in the STP (Section 3.12 of this SPM)
- (3) The V&V documents as described in the SVVP (Section 3.10 of this SPM)
- (4) The PSMS application software configuration items as described in the SCMP (Section 3.11 of this SPM).

#### 3.3.2 Organization/Responsibilities

The following organizations are described in Section 2.2 of this SPM. Their roles and responsibilities for assuring application software quality are described as follows:

- (1) Quality Assurance Manager (QAM)/ Quality Assurance Engineer (QAE)

The QA Department is independent of the Design Team (DT).

The QAM is responsible for assuring that the planned software development and V&V activities are appropriately conducted by the organizations responsible for those activities as described in this SPM, in accordance with implementing procedures as described in Section 1 "Organization" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27).

QA Engineers, assigned by the QAM, confirm that the PSMS application software development process is performed in accordance with this SPM (and implementing procedures) by performing QA audits of the project planning, development, maintenance and V&V activities described in this SPM. The QAE develops the associated QA audit plans and schedules.

The QAE is responsible for documenting the results of QA audits and reporting them to the QAM, DTM and VVTM. If a QA audit results in any findings, they shall be assigned to the organization responsible for the affected activities. Corrective actions related to audit findings shall be promptly developed and initiated by the manager of the responsible organization, and reported back to the QAM, as described in Section 16 "Corrective Action" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27)

The QA audits shall be performed by the QA Department in accordance with IEEE Std 1028-1997 (Reference 9) which is endorsed by RG1.168 (Reference 18).

(2) Design Team Manager (DTM) and Engineer (DTE)

The Design Team Manager (DTM) is responsible for ensuring an adequate number of qualified resources is available for executing the activities assigned to the DT as described in this SPM, including the responsibilities for the software safety analyses activities described in the SSP (Section 3.9 of this SPM).

DTE are responsible for performing the activities assigned to the DT as described within this SPM. The DTE are directly responsible for the quality of the documents and configuration items that they produce, and shall not rely on the QA audits, V&V activities, or any other oversight or review activities for adding or improving quality.

(3) V&V Team Manager (VVTM) and Engineer (VVTE)

The V&V Team Manager (VVTM) is responsible for ensuring an adequate number of qualified resources is available for executing the independent V&V activities described in the SVVP and STP (Section 3.10 and 3.12 of this SPM, respectively).

The VVTM shall confirm that the following qualifications and V&V independence criteria are met for the personnel selected for the V&V Team (VVT):

- a. Technical, managerial and financial independence as defined in Annex C of IEEE Std 1012-1998.
- b. Digital control system and US-APWR knowledge and experience equal to or greater than personnel on the DT.

(4) Project Manager (PJM) and Project Management Team (PMT)

The Project Manager (PJM) oversees project-specific activities of the design and manufacturing departments, as well as the interfaces between the design and manufacturing departments and the VVT or QA Department. The PJM has no authority to plan, schedule, budget, or direct V&V or QA activities.

### 3.3.3 Security

The QA Department shall conduct periodic audits to confirm the security of the PSMS application software development process is controlled in accordance with this SPM.

The security requirements described in this SPM shall be implemented in accordance with RG

1.152 (Reference 17), and the conformance evaluation and security assessment are described in Appendix C of this SPM.

### **3.3.4 Measurement**

General measures of the PSMS application software life cycle process are described in this section. Metrics used to measure the specific quality of the PSMS application software documents and configuration items as they emerge from the PSMS application software life cycle process are described in Section 3.3.5.1.

The number and age of open QA Audit findings reported by the QA Department (QAM/QAE) is recorded as QA data, and is a measure of the quality of the PSMS application software life cycle process and the documents and configuration items that are produced. This measure is an important indicator for observing the extent to which the PSMS application software life cycle processes are performed in accordance with the SPM. Audit findings shall be tracked to closure by the QAM/QAE.

QA Audit findings that detect software hazards (anomalies), not already discovered and documented by either the DT or the VVT (including their independent reviewers), are an indication of a potential weakness in the PSMS application software life cycle process or effectiveness of the overall organization, and merit further investigation.

Other PSMS application software life cycle process measures include the following:

- (1) Number of comments identified by Design Reviews (as described in Section 3.2 “SDP”)
- (2) Number and age of V&V Anomaly Reports (as described in Section 3.10 “SVVP”)
- (3) Number and age of Nonconformance Reports (NCR)
- (4) Number and age of Corrective Action Reports (CAR)

### **3.3.5 Procedures**

#### **3.3.5.1 Metrics**

The metrics described in this Section shall be used to measure the specific quality of the application software documents and configuration items as they emerge from the PSMS application software life cycle process. The metric data described below shall be collected periodically, monitored, and systematically analyzed for emerging trends.

- (1) Correctness / completeness of the Plant Requirements Phase and the System Requirements Phase outputs
- (2) Design Phase output compliance with requirements
- (3) Implementation Phase output compliance with design specifications
- (4) Test Phase output compliance with requirements documents

- (5) Installation (on-site) functional compliance with requirements
- (6) Operations and Maintenance Phase performance history

The DTM shall be responsible for collecting, monitoring and analyzing these metrics, and shall implement improvements to the PSMS application software life cycle process as necessary. Any adverse trends detected shall result in initiation of a Nonconformance Report as described in Section 15 “Nonconforming, Materials, Parts, or Components” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27)

Throughout the PSMS application software life cycle process, the following quality measures of application software configuration items shall also be collected, monitored and analyzed by the DTM. Any adverse trends detected shall result in initiation of a Nonconformance Report.

- (1) Functional and Performance Characteristics
  - a. Accuracy
  - b. Functionality
  - c. Reliability
  - d. Robustness
  - e. Safety
  - f. Security
  - g. Timing
- (2) Application Software Life Cycle Process Document Characteristics
  - a. Completeness
  - b. Consistency
  - c. Correctness
  - d. Style
  - e. Traceability
  - f. Unambiguity
  - g. Verifiability

### **3.3.5.2 Reviews and Audits**

This section describes the reviews and audits required throughout the PSMS application software life cycle process.

The following activities shall be performed using the methods described in IEEE Std 1028-1997 (Reference 9) which is endorsed by RG1.168 (Reference 18):

- (1) Management Reviews
- (2) Design Reviews
- (3) Audits

#### (1) Management Reviews

The objective of the management review is to assess and determine if required activities are making progress, and are being performed in compliance with this SPM and implementing procedures.

Management reviews are a formal activity, held individually and periodically to assess the execution of activities assigned to the DT and VVT. Inputs to the management review include the Project Plan, Risk Matrix, and Problem List described in the SMP (Section 3.1 of this SPM) and the measures described in Section 3.3.5.1. These review inputs shall be examined prior to the review meeting.

- a. The DTM and VVTM shall periodically assess and summarize the activities assigned to their teams to determine if any resource assignment changes are necessary, or to redirect their teams if necessary in order to maintain compliance with this SPM and implementing procedures.
- b. The VVTM shall use the Management Review method to independently determine whether or not to proceed from one phase of the application software life cycle to the next phase. If any V&V anomalies detected in any PSMS application software life cycle phase potentially require a functional change described in an output document produced in the Plant Requirements Phase or the System Requirements Phase, the DTM shall convene a Configuration Control Board activity as described in the SCMP (Section 3.11 of this SPM) before proceeding.
- c. The DTM and VVTM shall periodically assess and verify that the activities assigned to their teams comply with the requirements of this SPM and implementing procedures.

Management Review meetings shall accomplish the following objectives:

- 1) Evaluate project status and measures
- 2) Review the Project Plan, Risk Matrix, and Problem List
- 3) Review open V&V Anomaly Reports
- 4) Generate a list of action items
- 5) Document the meeting results

Management Reviews shall be performed using the method described Section 4 of IEEE Std 1028-1997.

## (2) Design Reviews

The objective of a Design Review is to evaluate PSMS application software configuration items (described in the SCMP; Section 3.11 of this SPM) to determine their suitability for their intended use and identify discrepancies from specifications and standards.

Design reviews also constitute “Inspections” and “Walkthroughs” as described in IEEE Std. 1028-1997 (Reference 9).

Design Reviews provide assurance that:

- a. Application software configuration items conform to specifications
- b. Application software life cycle phase outputs adhere to the requirements of this SPM and its implementing procedures
- c. Changes to application software configuration items are properly implemented and affect only those areas identified by the requested change.

Design Reviews shall be performed using the method described in Section 5 of IEEE Std 1028-1997 (Reference 9). Design Reviews shall be conducted by DT Engineers and who have the same training and qualifications as the DT Engineer who prepared the PSMS application software configuration item or design document. The results of design review comments and activities shall be documented and reported to the responsible DTE and the DTM.

The DTM shall confirm that internal design reviews have been adequately performed for the design output documents described in the SDP (Section 3.2 of this SPM). The DTM shall attend design review meetings convened as necessary in the course of design activities, and assess design review reports for clarity, completeness, and timeliness.

## (3) QA Audits

The objective of QA Audits is to provide an independent evaluation of conformance of the PSMS application software life cycle activities and outputs to this SPM and its implementing procedures.

QA Audits shall be conducted using the methods described in Section 8 of IEEE Std 1028-1997 (Reference 9). QA Engineers shall examine application software life cycle output products and document their observations, findings, and recommended corrective actions. QA Engineers shall be free from bias and influences that reduce their ability to make independent, objective evaluations.

QA Audits shall be performed as described below:

### a. Functional Audits

A functional audit shall be performed in the Test Phase, by the QA Department, prior to exiting the Test Phase. The functional audit shall independently confirm that all requirements specified in the output documents from the Plant Requirements Phase and the System Requirements Phase have been met, based on the Requirements

Traceability Matrix (RTM). The RTM is described in the SVVP (Section 3.10 of this SPM).

b. Physical Audits

A physical audit shall be performed by the QA Department in the Installation Phase to independently confirm that the PSMS application software configuration items and documents are complete and controlled in accordance with the SCMP (Section 3.11 of this SPM). The physical audit shall also confirm that all change requests and V&V Anomaly Reports are fully dispositioned and closed.

c. In-Process Audits

In-process audits shall be performed by the QA Department to confirm that System Requirements Phase, Design Phase, and Implementation Phase activities and outputs are being performed in accordance with this SPM and its implementing procedures.

All QA Audits shall be conducted and reported in accordance with Section 18 "Audits" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27).

The basic QA Audit process is as follows:

- 1) Management preparation
- 2) Planning the audit
- 3) Opening meeting
- 4) Examination (evidence collection and closing meeting)
- 5) Reporting

QA Audit Reports shall contain the following information, as a minimum:

- 1) Purpose and scope
- 2) Observations (strengths, or weaknesses that do not constitute a Nonconformance)
- 3) Findings (Nonconformance)
- 4) Summary Results
- 5) Recommendations

A QA Audit shall be considered complete when the QA Audit Report has been submitted and all actions include in the scope of the audit have been performed, reviewed and approved.

### 3.3.5.3 Software V&V

Independent V&V of the PSMS application software is performed to ensure that it meets the specified requirements for the PSMS. The scope of V&V is the PSMS application software

configuration items, documents and all aspects of PSMS that relate to the PSMS application software. V&V activities are described in the SVVP (Section 3.10 of this SPM).

#### **3.3.5.4 Problem Reporting and Corrective Action**

Application software hazards, problems and issues identified by management reviews, design reviews, independent V&V, QA audits and external sources (such as customer reports) shall be promptly acted upon in accordance with this SQAP and its implementing procedures.

Problem reporting and corrective action procedures shall span the entire PSMS application software life cycle described in this SPM. Identified application software hazards, problems and issues that constitute a condition adverse to quality shall immediately result in initiation of a Nonconformance Report as described in Section 15 “Nonconforming, Materials, Parts, or Components” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27)

The QA Department shall periodically assess application software related QA Audit reports and Nonconformance Reports to ensure that identified findings, hazards, problems and issues are promptly and properly resolved.

The QA Department is responsible for assuring compliance with this SQAP and its implementing procedures.

#### **3.3.5.5 Test**

Application software test activities shall cover all functional and performance requirements specified in the System Requirements Phase of the PSMS application software life cycle, as described in the SVVP and the STP (Sections 3.10 and 3.12 of this SPM, respectively).

#### **3.3.5.6 Code and Media Control**

The PSMS application software configuration items, including media, shall be controlled in accordance with the SCMP (Section 3.11 of this SPM).

#### **3.3.5.7 Training**

Training activities shall be planned and conducted as described in the STrngP (Section 3.7 of this SPM) for the roles and responsibilities of each organization described in this SPM. Training objectives shall be developed in a manner that assures high quality and reliability of the PSMS application software. Training records shall be documented and maintained.

#### **3.3.5.8 Risk Management**

Potential risks associated with the development, maintenance and assurance of high quality PSMS application software configuration items and life cycle process outputs shall be identified and managed. Risk management methods and tools are described in the SMP (Section 3.1 of this SPM).

### **3.3.6 Record Keeping**

Controlled documents and QA records produced by the activities described in this SPM shall be

controlled in accordance with the following Sections of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27):

- Section 3 "Design Control"
- Section 6 "Document Control"
- Section 7 "QA Records"

### 3.3.7 Methods/Tools

The following tools are used for executing the application software life cycle activities described in this SPM:

#### (1) Documented Checklists

Checklists shall be used by the DT to ensure the completeness of the design outputs from each phase of the PSMS application software life cycle process assigned to the DT. Checklists shall contain the following information, as a minimum:

##### Functional Characteristics

- a. Accuracy
- b. Functionality
- c. Reliability
- d. Robustness
- e. Safety
- f. Security
- g. Timing

##### Process Characteristics

- a. Completeness
- b. Consistency
- c. Correctness
- d. Style
- e. Traceability
- f. Unambiguity
- g. Verifiability

## (2) Requirements Traceability Matrix (RTM)

Traceability between design documents, test documents and configuration items shall be documented by the VVT using the RTM as described in the SVVP (Section 3.10 of this SPM). The RTM is updated at the end of the each PSMS application software life cycle phase.

### 3.3.8 Standards

This SQAP complies with the following guidance and standards.

- Clause 5.3.1 of IEEE Std 7-4.3.2-2003 (Reference 5), which is endorsed by RG 1.152 (Reference 17)
- Clause 3.3.3 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22)
- IEEE Std 1028 (Reference 9) which is endorsed by RG 1.168 (Reference 18)
- IEEE Std 730-2002 (Reference 8) which is referenced by IEEE Std 7-4.3.2 (Reference 5)
- Section 3.1.2 of NUREG/CR-6101 (Reference 26).

### 3.4 Software Integration Plan (SIntP)

#### 3.4.1 Purpose

This Software Integration Plan (SIntP) describes how developed application software units are integrated, and how the fully integrated application software is integrated with the MELTAC platform hardware and basic software. The SIntP is performed during the Implementation Phase to allow a complete system to be achieved and tested in the Test Phase.

System V&V Testing, described in the SVVP and STP (Sections 3.10 and 3.12 of this SPM, respectively), demonstrates that the integrated system correctly performs all requirements in the System Requirements Specification (SysRS) as described in the SDP (Section 3.2 of this SPM).

This SIntP complies with the guidance and standards identified in Section 3.4.6.

#### 3.4.2 Organization/ Responsibilities

The organization structure is described in Section 2.2.

The Design Team is responsible for the following;

- (1) Integrate the application software units, tested via Component V&V Tests (as described in the SVVP and STP), together to form one Application Execution Module for each target CPU hardware module in the system.
- (2) Integrate the Application Execution Module from Step (1) into the target CPU hardware modules.

The V&V Team is responsible for executing the Integration V&V Test Procedure as described in the SVVP and STP.

#### 3.4.3 Measurement

The Design Team shall perform the following tasks, using the MELTAC engineering tool, before releasing the integrated system to the VVT:

- (1) Confirm that all Application Execution Modules are properly installed in the target CPU hardware modules using MELTAC engineering tool.
- (2) Confirmed that the installed Application Execution Modules are identical to the data saved in the MELTAC engineering tool.

If any anomalies occur during these steps, the DT shall identify the cause and implement corrective actions.

If the anomaly indicates a software safety hazard as described in the SSP (Section 3.9 of this SPM), a Nonconformance Report shall be promptly initiated as described in the SQAP (Section 3.3 of this SPM).

If the PSMS application software change is required to resolve the integration anomaly, the DT shall initiate and process a Software Change Request (SCR) as described in the SCMP (Section 3.11 of this SPM).

#### 3.4.4 Procedures

#### 3.4.5 Methods/Tools

The MELTAC engineering tool shall be used for the Integration and Test activities described in this SIntP, the STP and the SVVP.

#### 3.4.6 Standards

This SIntP complies with the following guidance and standards.

- Section 5.3.7 and 5.3.8 of IEEE Std 1074-1995 (Reference 6) which are endorsed by RG 1.173 (Reference 23)

- Section 3.1.8 of NUREG/CR-6101 (Reference 26).

### 3.5 Software Installation Plan (SInstP)

#### 3.5.1 Purpose

This Software Installation Plan (SInstP) describes the methods used for installing the PSMS application software in a target system. If a software hazard arises as described in the SSP (Section 3.9 of this SPM), it shall be identified and reported, and necessary corrective actions shall be provided as described in the SQAP (Section 3.3 of this SPM).

The following activities shall be performed as described in this SInstP:

- Application software installation
- Inspect software configuration on installed PSMS at site
- Accept software in the Installation Phase

The SInstP complies with the guidance and standards identified in Section 3.5.6.

#### 3.5.2 Organization/Responsibilities

The organization structure is described in Section 2.2.

##### (1) Design Team (DT)

The DT shall perform application software installation activities as described in the Software Integration Plan (SIntP; Section 3.4 of this SPM). The DT shall document the results of the installation activity in a report to the DTM.

##### (2) V&V Team (VVT)

The VVT is responsible for the Implementation and Installation Phase V&V activities, including executing the Integration V&V Test, the System V&V Test, and the Acceptance V&V Test Procedures described in the SVVP and the STP. The VVT shall provide the V&V Test Reports to the VVTM.

##### (3) QA Department Responsibilities

The QA Department performs QA Audits as described in the SQAP (Section 3.3 of this SPM) to assure DT and the VVT activities are performed as described in this SInstP.

#### 3.5.3 Measurement

The following data shall be collected and analyzed to determine the success or failure of the installation effort of the PSMS application software:

- Progress status of installation activities in comparison to the schedule.
- The number of Nonconformances

- Number of installation related items on the Problem List
- The number of V&V Anomaly Reports.
- The number of Software Change Requests (SCR) required during installation.

### **3.5.4 Procedures**

The necessary steps, methods and tools require for installing the application software in the factory environment prior to Integration and System V&V Tests is described in the Software Integration Plan (SIntP). The following steps are for software installation steps that may occur in the Installation Phase of a US-APWR project. If no software changes occur between the System V&V Test and the Installation Phase, it is acceptable to proceed to Section 3.5.4.4.

#### **3.5.4.1 Installation Phase Planning**

The DT shall identify and analyze the plant installation environment of the PSMS application software for each US-APWR project which are described in the System Requirements Specification (SysRS), and provide the plant installation procedures for the PSMS application software.

##### **3.5.4.1.1 Installation Documents**

The DT shall provide the following installation documents of the PSMS application software:

- (1) Installation Procedure
- (2) Installation Reports

##### **3.5.4.1.2 Installation Procedure**

The Installation Procedure shall include the following information, as a minimum:

- (1) Overall installation strategy.
- (2) Software installation procedure.
- (3) Hardware and software integration procedure
- (4) System installation procedure.
- (5) All PSMS controllers are functional.
- (6) The correct software versions are installed in the correct controllers.
- (7) All communication links and networks are functional for all interfaced devices.
- (8) Software check and test, including self-testing, procedure for after installation

Acceptance Criteria for determining the success or failure of the installation effort of the PSMS shall be provided in the Installation Procedure.

### 3.5.4.2 Distribute Software

The PSMS application and basic software, which are verified and validated in the Implementation Phase as described by the SVVP (Section 3.10 of this SPM) shall be packaged onto the respective media as described by the SCMP (Section 3.11 of this SPM) and distributed, with the Installation Procedure, to the US-APWR plant for installation.

### 3.5.4.3 Install Software

The packaged PSMS application software, including the basic software shall be installed in the PSMS in each US-APWR site according to the installation procedures.

The installation report shall be documented and provided on the installation results and any problems encountered by the DT.

The Installation Reports shall include the following items:

- (1) Software version
- (2) Installation check results

### 3.5.4.4 Accept Software in Operational Environment

After the installed application software configuration items are inspected as required by the "Inspect Installation Configuration" task in the SVVP (Section 3.10.6.3.2.5) in the Installation Phase, the Acceptance V&V Test Procedure shall be executed by the VVT as described in the SVVP and the STP.

### 3.5.5 Methods/Tools

Software is installed in a MELTAC controller using the MELTAC engineering tool. The method used in this Installation Phase is the same as Implementation Phase described in Section 3.4.4.

### 3.5.6 Standards

This SInstP complies with the following guidance and standards.

- Clause 6.1 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22)
- Section 3.1.8 of NUREG/CR-6101 (Reference 26)

### 3.6 Software Maintenance Plan (SMaintP)

#### 3.6.1 Purpose

This Software Maintenance Plan (SMaintP) describes the processes of correcting faults of the PSMS application software during plant operation. This SMaintP does not include the changes of software derived from functional design changes, which are considered to be the development process described in the Section 3.2 of this SPM. Design changes shall be evaluated in accordance with 10 CFR 50.59. Defects and non-compliance shall be reported in accordance with 10 CFR 21.

The PSMS application and basic software are conducted with the resolution of software hazards, errors, faults, and failures. The requirement for the PSMS application and basic software maintenance initiate the software life cycle process changes. The software life cycle process is remained and executed, thereby treating the maintenance process as iterations of development.

This SMaintP complies with the guidance and standards identified in Section 3.6.8.

#### 3.6.2 Organization/ Responsibilities

If a PSMS fault or defect is identified during the Operations and Maintenance Phase of the PSMS application software life cycle, the following organizations shall have the following responsibilities (details are described in Section 3.6.6):

(1) Licensee (Customer)

The Licensee is responsible for determining operability of affected Systems, Structures and Components as described in the facility Technical Specifications, and for initiating internal and external reporting as described in Chapter 17 (Quality Assurance Program) of the facility Final Safety Analysis Report (FSAR). Application software maintenance activities performed by the Licensee shall be reported, evaluated and initiated in a manner equivalent to the steps described in this SMaintP.

(2) Mitsubishi Heavy Industries, Ltd (MHI).

MHI is responsible receiving the Licensee report described above, promptly initiating internal and external reports, and tracking identified corrective actions to closure as described in the SQAP (Section 3.3 of this SPM)

(3) Design Team (DT)

The DT is responsible for responding to internal reports of PSMS application software failures, defects or other nonconforming conditions, determining the root cause, extent of condition, and corrective actions, and implementing the identified corrective actions including initiating a Notice of Defect report, if required, as described in the SQAP (Section 3.3 of this SPM).

(4) Verification and Validation Team (VVT)

The VVT is responsible for Maintenance Phase V&V activities as described the SVVP (Section

3.10 of this SPM).

### 3.6.3 Risks

The DT shall assess the risks associated with maintenance related software changes as described in the SMP (Section 3.1 of this SPM).

### 3.6.4 Security

Security of the development environment shall be maintained as described in Appendix C of this SPM.

### 3.6.5 Measurement

The errors found during software maintenance activities should be collected, recorded and analyzed to determine the quality of the software maintenance program. Measurements and metrics shall be developed in accordance with the Section 3.4 of this SPM.

### 3.6.6 Procedures

The PSMS application and basic software maintenance plan describe three primary activities: reporting of failures that were detected during operation, correction of the faults that caused those failures, and release of new versions of the PSMS application and basic software product.

The following activities shall be performed for the maintenance of the PSMS application and basic software:

#### 3.6.6.1 Activity: Failure Detection and Reporting

The DT shall provide the methodology for identifying, assessing, and recording failures of the PSMS during plant operation in an Operation and Maintenance Manual to be provided to the Licensee before the Operations and Maintenance Phase. As a minimum, the methodology in the Operation and Maintenance Manual shall include requirements for identifying the date and time of a PSMS failure, a brief description of the failure (including the state of the system at the beginning of the occurrence), information retrieved using the MELTAC engineering tool, and a description of immediate corrective actions taken by the Licensee.

(1) Licensee

Upon discovery of a PSMS failure, the Licensee shall identify, assess, and record failure data as described in the Operation and Maintenance Manual, and attach it to an internal report to be initiated in accordance with their internal procedures for Issue Reporting and Corrective Action as described in Chapter 17 (QAP) of the facility FSAR.

If the error is likely due to a PSMS defect or nonconforming condition, the Licensee shall promptly report the condition to MHI, and if the nonconforming condition is determined by the Licensee to be a defect as described in 10 CFR 21, a Notice of Defect report shall be initiated in accordance with the Licensee's internal procedures as described in Chapter 17 of the facility FSAR.

The Licensee shall also determine operability of affected Systems, Structures and Components in accordance with the facility Technical Specifications.

(2) MHI

In response to the Licensee report provided in Step (1), MHI shall promptly initiate a Nonconformance Report as described in Section 15 “Nonconforming, Materials, Parts, or Components” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27). MHI shall assign the responsibility for determining the root cause, extent of condition, and corrective actions to the Design Team (described in Section 2.2 of this SPM).

### 3.6.6.2 Activity: Fault Correction

The DT shall collect and analyze the operational failure data to be provided by the Licensee as described in Section 3.6.6.1.

(1) Evaluation

The DT shall determine if the failures are caused by nonconforming conditions or defects in the PSMS application software, the basic software, or both. The DT shall determine the root cause, extent of condition, and corrective actions necessary to correct the nonconforming condition or defect as described in Section 15 “Nonconforming, Materials, Parts, or Components” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27).

The DT shall notify MELCO if the identified nonconforming condition or defect is in the basic software, and MELCO shall initiate a Nonconformance Report and take corrective actions as described in the Basic Software Program Manual (JEXU-1012-1132).

(2) Corrective Actions

The DT shall initiate the corrective actions identified in Step (1), above. If the corrective action requires the PSMS application software change, a Software Change Request (SCR) shall be promptly initiated as described in the SCMP (Section 3.11), and the necessary change activities shall be performed as described in this SPM.

The VVT shall perform the Maintenance Phase V&V activities described in the SVVP (Section 3.10 of this SPM), including regression analysis for the proposed application software change to determine the necessary V&V activities and tasks for the proposed change.

Basic software changes, if required, shall be initiated and performed as described in Basic Software Program Manual (JEXU-1012-1132).

### 3.6.6.3 Activity: Release and Installation

After completion of all required PSMS application software change activities and V&V tasks through the Test Phase as described in this SPM, the DT shall release it for installation.

Installation activities shall be performed as described in the SInstP, and Application V&V Test activities shall be performed as described in the SVVP and STP (Section 3.10 and 3.12 of this SPM, respectively).

#### 3.6.6.4 Maintenance of Commercial Dedication

There are no commercial grade items used in the PSMS including application software. All systems, structures and components in the PSMS use the qualified MELTAC Platform and basic software as described in Technical Report "Safety System Digital Platform –MELTAC-" (MUAP-07005), which are produced and maintained as basic components by MELCO under a 10 CFR 50 Appendix B QAP. Therefore, there is no maintenance of commercial dedication activities applicable to the PSMS.

#### 3.6.6.5 Configuration Management

PSMS application software shall be performed as described in the SCMP (Section 3.11 of this SPM).

#### 3.6.7 Methods/Tools

The MELTAC engineering tool shall be used for retrieving operational data as described in Section 3.6.6.1, and for PSMS application software change and V&V activities as described in Section 3.10 "SVVP" of this SPM.

#### 3.6.8 Standards

This SMaintP complies with the following guidance and standards.

- Clause 6.3 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22),
- Section 3.1.9 "Software Maintenance Plan" of NUREG/CR-6101 (Reference 26).

Clause 5.4.2.3 of IEEE Std 7-4.3.2-2003 (Reference 5) which is endorsed by RG1.152 (Reference 17), listed in B.3.1.6 of BTP7-14 (Reference 1), is not applicable to this SMaintP for the reason described in Section 3.6.6.4 of this SMaintP.

### 3.7 Software Training Plan (STrngP)

#### 3.7.1 Purpose

The development of quality software products is largely dependent upon knowledgeable and skilled personnel. These include MHI technical personnel and management as well as the potential for the customer's personnel to be qualified to install, operate and maintain the software. Training is therefore essential for technical personnel both for MHI and customer. This STrngP provides customer training for the MELTAC Platform and the application software.

This STrngP complies with the guidance and standards identified in Section 3.7.6.

#### 3.7.2 Organization/Responsibilities

There are two sets of organizations responsible for being trained and qualified for performing the PSMS application software lifecycle process described in this SPM:

(1) DT and VVT

Training for the Design Team (DT) and the V&V Team (VVT) personnel who are responsible for development, maintenance and V&V activities, such training is the responsibility of the manager of each organization and team as described in Section 2.2 of this SPM, and is outside the scope of this STrngP.

(2) Customers

Training for US-APWR plant personnel, including operators, I&C engineers and I&C technicians who are engaged in technical support, operations, and maintenance activities for the PSMS in the Operation and Maintenance Phase, specific training procedures for each US-APWR plant, as defined by IEEE Std 1074-1995, are post-development activities and are the responsibility of the customer.

(3) MHI/MELCO Training Department

MHI shall provide customer training for the application software using the training materials described in Section 3.7.4.1.1. MELCO shall provide customer training for the MELTAC Platform as described in Section 3.7.4.1.2.

The customer shall develop and maintain training procedures, and shall train and qualify their personnel, including operators, I&C engineers and I&C technicians in accordance with the facility FSAR.

#### 3.7.3 Measurement

Training effectiveness shall be measured in accordance with the customer training program as described in the facility FSAR.

### 3.7.4 Procedures

#### 3.7.4.1 Training Activities

The following activities shall be performed:

##### 3.7.4.1.1 Training for application software

###### (1) Develop Training Materials

The DT shall develop and maintain the training materials to be used for training customers, and shall contain information for performing technical support and the Operations and Maintenance activities described in the Operations and Maintenance Manual to be delivered to the customer as described in the SMaintP (Section 3.6 of this SPM). Training materials shall contain the following information as a minimum:

- a. Purpose
- b. Learning Objectives
- c. PSMS Application Level Content
  - Overview of US-APWR Plant
  - System Description
  - Functional Overview
  - Maintenance Methods
  - Troubleshooting Methods
- d. Suggested Test Questions (against the Learning Objectives)

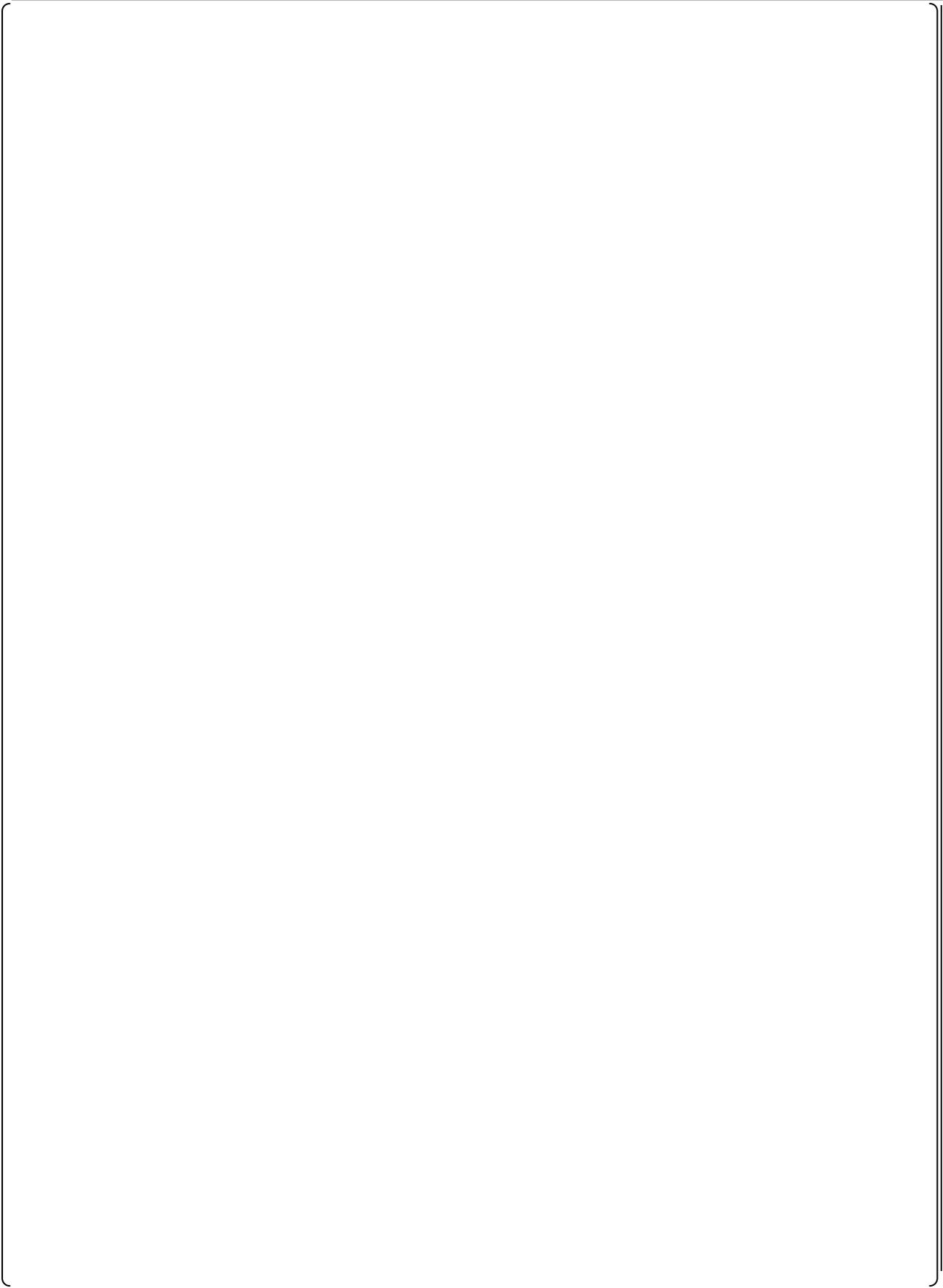
###### (2) Train the Customer Trainer

MHI shall train customer trainers using the Systematic Approach to Training methods developed by the National Academy for Training (INPO), using the materials developed in Step (1), above.

###### (3) Implement the Training Program

Customer trainers qualified in accordance with the facility FSAR shall implement the training of customer personnel, including operators, I&C engineers and I&C technicians, in accordance with this STrngP, using the training materials provided in Step (1), above.

##### 3.7.4.1.2 Training for the MELTAC Platform



### **3.7.5 Resources**

The PSMS application level software training is executed with training materials described in Section 3.7.4.1.1.

PSMS equipment level training, including use of the MELTAC engineering tool, is described in Section 3.7.4.1.2.

#### **3.7.5.1 Methods and Tools**

Methods and tools used to perform the PSMS application software training shall be defined in accordance with the customer training program as described in the facility FSAR.

#### **3.7.5.2 Training Facilities**

Operator training, qualification and licensing shall be performed in the facilities required and described by the customer training program described in the facility FSAR.

### **3.7.6 Standards**

This STrngP complies with the following guidance and standards.

- Section 7.4 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22)
- Section 3.1.10 "Software Training Plan" of NUREG/CR-6101 (Reference 26).

### **3.8 Software Operations Plan (SOP)**

#### **3.8.1 Purpose**

The purpose of the Software Operations Plan (SOP) is to define the process of operating the PSMS application software during the Operation and Maintenance phase.

This SOP complies with the guidance and standards identified in Section 3.8.7.

#### **3.8.2 Organization/Responsibilities**

(1) Design Team (DT)

The DT is responsible for providing Operation and Maintenance Manual and submits to customers.

(2) DT and/or Customers

The scope of the following responsibility depends on contract terms with customers

Problem reporting and corrective actions during the Operations and Maintenance Phase shall be performed in accordance with the Section 3.6 of this SPM.

#### **3.8.3 Security**

Security of the development environment shall be maintained as described in Appendix C of this SPM. |

#### **3.8.4 Measurement**

The following data shall be collect and analyzed to determine the PSMS reliability.

- (1) Error rate reported by self-diagnostics
- (2) Module failure rate

Measurements and metrics shall be developed in accordance with the Section 3.4 of this SPM.

#### **3.8.5 Procedures**

##### **3.8.5.1 Operations and Maintenance Manual**

An Operations and Maintenance manual shall be developed by the DT and provided to customers. This manual shall include the following information, as a minimum:

- (1) Startup and reset of PSMS controllers
- (2) De-energization of PSMS controllers
- (3) Response to failure alarms and indications

- (4) Initiating and removing maintenance bypasses
- (5) Periodic surveillance tests and calibration
- (6) Periodic performance monitoring
- (7) Periodic equipment maintenance or replacement
- (8) Security access and controls
- (9) Removing and installing PSMS modules
- (10) Failure reporting and corrective actions
- (11) Backup procedure of all program files, including data and code
- (12) Backup Interval
- (13) Instruction manual of MELTAC engineering tool

#### **3.8.5.2 Problem Reporting**

Problem reporting shall be performed in accordance with the SQAP (Section 3.3 of this SPM).

#### **3.8.6 Methods/Tools**

The Operational-VDU (O-VDU) and Safety-VDU (S-VDU) are the primary operator interfaces for operating the US-APWR systems as described in Chapter 7 of the US-APWR DCD.

The MELTAC engineering tool is the interface for operation and maintenance activities related to routine and corrective maintenance, including retrieving and assessing diagnostic information in response to a PSMS alarm. Instructions for use of the MELTAC engineering tool shall be provided in the Operation and Maintenance Manual.

#### **3.8.7 Standards**

This SOP complies with the following guidance and standards.

- Clause 3 of IEEE Std 1074-1995 Clause 3 (Reference 6) which is endorsed by RG 1.173 (Reference 22)

### 3.9 Software Safety Plan (SSP)

#### 3.9.1 Purpose

The purpose of the Software Safety Plan (SSP) is to describe methodologies for all life cycle process of the PSMS application software as described in Section 3.10 “SVVP” to minimize the potential of a software defect jeopardizing the health and safety of the public.

The SSP ensures that critical plant requirements, such as reactor trip functions, ESFAS functions, response times and fail-safe modes, etc. are identified. These critical requirements and functions are assured through implementation of this SSP throughout the PSMS application software life cycle. The SSP assures that precautions are defined for all life cycle phases to prevent software hazards that could result in failure of these critical requirements and functions. Then the SSP assures these precautions are followed in the design and implementation phases and for any changes to the PSMS application software during the operations and maintenance phases.

The scope of this SSP is the PSMS application software and all aspects of the PSMS that relate to the application software (i.e., the plant-specific configuration of standard MELTAC platform components, including hardware and software, which is unique to the PSMS application software). Each life cycle process within this SPM, including this SSP, considers the interaction between the unique application configuration of the PSMS application software and the generic MELTAC platform, as a completely integrated system. Life cycle process activities that are exclusive to the MELTAC platform are defined by the technical report JEXU-1012-1132 “MELTAC Platform Basic Software Program Manual”, which is referenced by this SPM. The Design Team (DT) shall create the PSMS application software and associated system configuration in accordance with the critical safety requirements.

This SSP defines technical requirements and organizational responsibilities for specific activities which are known to enhance software safety. The aggregate of these activities is referred to as Software Safety Management (SSM) and Software Safety Analyses (SSA). The SSM and the SSA include specific analysis conducted by the DT, as well as independent V&V of the DT outputs, during each life cycle process. Therefore, all SSM and SSA activities for the US-APWR project are governed by this SSP, as well as other plans within this SPM. Throughout this SSP, the entire system evaluated to determine the influence of a potential failure. The SSA are performed to follow the requirements of this SSP as part of the System Requirements Phase, the Design Phase, the Implementation Phase, the Test Phase, the Installation Phase and the Operation and Maintenance phase.

The SSA must ensure that:

- (1) All system safety requirements are correctly described in the System Requirements Specification (SysRS) which include the hardware requirements specification, the software requirements specification and the interface requirements specification. Requirements that are fulfilled by the generic MELTAC platform shall be uniquely identified.
- (2) The SysRS should covers all safety requirements in the DCD, including Chapter 7 and Chapter 15 “Transient and Accident Analyses”, Chapter 19 “Probabilistic Risk Assessment and Severe Accident Evaluation” and related technical reports, etc.

- (3) No additional hazards have been introduced in subsequent life cycle process.
- (4) Other software elements that may affect safety are identified.
- (5) Software and system elements that affect safety are protected from adverse influence from software and system elements that do not directly affect safety.
- (6) Software hazards and resolutions from each phase identified in the SSA are documented.

The purposes of the SSA are to ensure compliance with safety goals established for the final PSMS safety application software of the US-APWR plant. The principal safety goals associated with the PSMS for the US-APWR Plant are identified in the DCD Chapter 7.

This SSP complies with the guidance and standards identified in Section 3.9.9.

This SSP is conducted in accordance with Section B.3.1.9 of BTP 7-14 (Reference 1), Section C.3 of RG 1.173 (Reference 22), Sections 3.1.5 and 4.1.5 of NUREG/CR-6101 (Reference 26), and IEEE Std 1228-1994 (Reference 10).

Section C.3 of RG 1.173 defines the input information and the output information of the SSA, and requires the SSA to ensure the following items:

- (1) System safety requirements have been correctly addressed.
- (2) No new hazards have been introduced.
- (3) Software elements that can affect safety are identified.
- (4) There is evidence that other software elements do not affect safety.
- (5) Safety problems and resolutions identified in these analyses are documented.

Sections 3.1.5 and 4.1.5 of NUREG/CR-6101 define that the minimum requirements for the SSM and the SSA must be performed in each software of the safety I&C systems, and the descriptions and requirements in these sections are documented in accordance with IEEE Std 1228-1994.

### **3.9.2 Organization/Responsibilities**

Section 2.2 "Organization and Responsibilities" describes the organizational responsibilities in supporting the SSM and SSA activities. The DT has the following responsibilities for the execution of the SSM and SSA. Various parts of the US-APWR project organization perform the SSM described in Section 3.9.7 and the SSA listed in Section 3.9.8. The Design Team Manager (DTM) ensures that these analyses are completed in accordance with the SSP and the DT has responsibility for the completion of the SSM and SSA activities;

- (1) Obtain and allocate resources to ensure effective implementation of the SSM and the SSA within the DT scope of responsibility.

- (2) Coordinate safety task planning with other organizational activities, such as development, system safety, software QA, software reliability, software configuration management, V&V, and software testing.
- (3) Coordinate software safety tasks described in the SSP within the overall context of the activities described in the SPM.
- (4) Coordinate technical issues related to software safety with other components of the development and support organization, within the project sponsor, or with the licensee described on Section 3.11 "SCMP".
- (5) Ensure that required records are kept in accordance with Section 3.11 "SCMP" to document the conduct of the SSP.
- (6) Participate in audits of software plan implementation of the SSP.
- (7) Ensure training of safety and other appropriate personnel in the SSM and SSA methods, tools, and techniques described in the SSP.

The VVT is responsible for assuring the requirements of the SSP are followed throughout the PSMS application software life cycle process. The V&V Team Engineer (VVTE), having knowledge of the safety implications of hardware, software and interfaces between them, is responsible for performing verification and validation of software safety activities performed by the DT as described in the SSP. Software V&V activities are described in Section 3.10 "SVVP".

The VVTE confirms that system documents, such as, functional requirements, functional diagrams, P&ID and PRA reports, etc., define critical software functions, software hazards that can prevent the functions, and precautions to prevent these software hazards. If the PSMS application software deficiencies are detected, the VVTE will initiate a V&V anomaly report as described in Section 3.10 "SVVP", and the Design Team Engineer (DTE) will implement corrective actions. Subsequently, the VVTE will reassess design changes to ensure the changes have corrected the deficiencies originally identified and have not created any new deficiencies. V&V activities ensure the precautions are followed throughout the design/implementation process. This includes specific test cases which are created for the integration testing as described in Section 3.12 "STP" to confirm the precautions are properly implemented.

The V&V Team Manager (VVTM) shall be designated the single safety officer that has clear responsibility for the safety qualities of the PSMS application software. The VVTM has clear authority for enforcing safety requirements in the System Requirements Specification (SysRS), the design, and the implementation of the PSMS application software. The VVTM has the authority to stop work and ultimately reject the PSMS application software if the application software cannot be shown to be adequately safe.

### 3.9.3 Risks

The SSP shall be executed by the DT and VVT staff in accordance with approved procedures for each site-specific US-APWR project that implement the roles, responsibilities, activities and tasks described herein.

The general risk management requirements are described in Section 3.1.6.2 of the SMP, and

specific risks to related requirements for the SSP are described below.

In order to identify and resolve software hazards as early as possible in the project schedule, the SSA shall be performed during each life cycle process of the PSMS application software, as each of the principal documents is prepared in accordance with the SPM; requirements, design descriptions, software logic diagram and test specifications. The SSA shall assure complete and clear documentation of:

- (1) Critical safety functions
- (2) Potential software hazards that may adversely affect the critical safety functions, including abnormal events, conditions and malicious modifications
- (3) Mitigating design features or defensive measures to reduce the hazard potential
- (4) Special tests to ensure the hazard potential has been minimized

The PSMS consists of a complete integration of hardware and software, designed specifically for nuclear safety applications and is configured using the MELTAC platform, described in the technical report MUAP-07005 "Safety System Digital Platform –MELTAC- ". MELTAC has been fully qualified to nuclear standards and has significant nuclear operating experience as described in the technical report MUAP-07005 "Safety System Digital Platform –MELTAC- ". The generic qualification process included SSA, such as software hazards analysis, failure modes and effects analysis (FMEA), response time analysis and independent verification testing.

The MELTAC platform uses a comprehensive set of self-diagnostics functions to monitor system performance for internal software hazards, including software hazards due to random hardware failures and software hazards due to software errors. MELTAC's substantial nuclear operating experience helps to minimize the potential for hidden design defects in the MELTAC platform hardware or basic software.

New software engineering processes have been developed to reduce or simplify the complexity of project-specific engineering since IEEE Std 1228-1994 was issued. The software safety methodology for the PSMS application software of the US-APWR plant is based on the use of the MELTAC platform and the MELTAC engineering tool as described in the technical report MUAP-07005 "Safety System Digital Platform –MELTAC-".

The generic MELTAC platform is supplemented with the generic US-APWR SSA that addresses the application software engineering for all US-APWR projects. Section 3.9.8 describes the generic SSA that is performed for the US-APWR project to ensure that the PSMS application software satisfies the design basis safety requirements. These activities ensure high reliability for the generic PSMS application software. Section 3.9.8 also describes the SSA applied to recurring applications of the generic PSMS life cycle process, for each US-APWR project, including the SSA applied for any changes from the generic PSMS application software design.

When combined together these SSA conform to the requirements of Section C.3 "Software Safety Analyses of RG 1.173, Section 3.1.5 and 4.1.5 of NUREG/CR-6101 and Section 4 "Software Safety Analyses" of IEEE Std 1228-1994 for all software safety analyses which are needed for the US-APWR plant.

### 3.9.4 Measurement

Metrics shall be maintained throughout the entire life cycle process for safety analysis deficiencies that have been discovered by the VVT. The deficiency metrics related to software safety shall be recorded and maintained together with all other deficiencies. However, metrics related to the functions of PSMS application software shall be specifically identified. Metrics shall be periodically reported in the V&V phase summary reports.

The measurement of the success of the SSP is the passing of the Acceptance Test with all previously discovered software safety hazards corrected and closed.

### 3.9.5 Procedures

The life cycle process developed by the DT, and identified in Section 3.9.7 and 3.9.8 as being pertinent to the SSM and the SSA, shall include safety requirements as described in the DCD, including Chapter 7, Chapter 15 and Chapter 19" and related technical reports.

The VVT shall confirm the adequacy of the DT outputs, with regard to all SSM and SSA requirements, as an integral part of their V&V tasks as described in Section 3.10 "SVVP". By the V&V activities and tasks described in Section 3.10, hazards caused by software and hazards which software is expected to control shall be identified.

As a part of the SSM and the SSA, the VVT shall ensure that all requirements imposed by plant safety analysis, system safety analysis and security vulnerability assessments can be traced to DT outputs. Traceability shall be documented using the Requirements Traceability Matrix (RTM) as described in Section 3.10 "SVVP". These tasks shall be conducted throughout the PSMS application software life cycle process, from the Plant Requirements Phase through the Operations and Maintenance Phases.

Problems encountered in implementing the SSP or any SSM and SSA deficiencies which are identified by the VVT at any time after document or software release from the DT shall be recorded in a V&V anomaly report and tracked to closure as described in Section 3.10 "SVVP".

Problems that relate to the PSMS critical safety functions shall be specifically identified so they can be resolved expeditiously. If the application software requires a change, the effect on all life cycle process outputs, including the critical software safety functions shall be re-evaluated by the DT and VVT. Any safety hazard discovered after completion of appropriate SSA activities is

documented in accordance with the SQAP of this SPM and corrected as described in Section 3.9.8.5.

The SSA summary document shall be prepared to summarize the SSA activity for each US-APWR project. The SSA summary is documented as a quality record in accordance with the SQAP of this SPM.

### **3.9.6 Methods/Tools**

Following tools shall be used:

(1) Documented checklist

Checklists shall be used to identify hazards and perform software safety analysis.

(2) Traceability check sheet

Traceability shall be documented using the RTM as described in Section 3.10 "SVVP".

The content of the checklists used by the DT in document preparation, review and approval is described in Section 3.2 "SDP". The content of the checklists and the RTM used by the VVT in the conduct of V&V activities and tasks documentation review is described in Section 3.10 "SVVP".

The software development and verification tools are described in Section 3.2 "SDP".

### **3.9.7 Software Safety Management (SSM)**

Section 3.9.7.1 through 3.9.7.13 describes the organization, schedule, resources, responsibilities, tools, techniques and methodologies used in the development of the PSMS application software. The SSM activities are conducted by the DT and the VVT in accordance with Section 3.1.5 of NUREG/CR-6101 and Section 4.3 of IEEE Std 1228-1994.

Many requirements described in Section 3.1.5 of NUREG/CR-6101 and Section 4.3 of IEEE Std 1228-1994 are covered by other sections of the SPM and detail descriptions are described in other sections of the SPM. Therefore, the description of each sub-section of the following SSM only refers to the section numbers of other section of the SPM for this case.

#### **3.9.7.1 Organization and Responsibilities**

The overall organization and responsibilities plan to comply with Section 3.1.5-1 of NUREG/CR-6101 and Section 4.3.1 of IEEE Std 1228-1994 is described in Section 2.2 "Organization and Responsibilities" of the SPM.

The specific organization and responsibilities plan to comply with Section 3.1.5-1 of NUREG/CR-6101 and Section 4.3.1 of IEEE Std 1228-1994 to perform the SSP is described in Section 3.9.2 of the SSP.

#### **3.9.7.2 Resources**

The resources plan to comply with Section 3.1.5-2 of NUREG/CR-6101 and Section 4.3.2 of

IEEE Std 1228-1994 is described in Section 2.2 “Organization and Responsibilities” of the SPM.

### **3.9.7.3 Staff Qualifications and Training**

The staff qualifications and training plan to comply with Section 3.1.5-3 of NUREG/CR-6101 and Section 4.3.3 of IEEE Std 1228-1994 is described in Section 3.7 “STRngP” of the SPM.

### **3.9.7.4 Software Life Cycle**

The software life cycle plan to comply with Section 3.1.5-4 of NUREG/CR-6101 and Section 4.3.4 of IEEE Std 1228-1994 is described in all sections of the SPM.

### **3.9.7.5 Documentation Requirements**

The documentation requirements plan to comply with Section 3.1.5-5 of NUREG/CR-6101 and Section 4.3.5 of IEEE Std 1228-1994 is described in Section 3.3 “SQAP” of the SPM.

### **3.9.7.6 Software Safety Program Records**

The PSMS application software program records plan to comply with Section 3.1.5-6 of NUREG/CR-6101 and Section 4.3.6 of IEEE Std 1228-1994 is described in Section 3.3 “SQAP” and Section 3.10 “SVVP” of the SPM.

### **3.9.7.7 Software Configuration Management Activities**

The software configuration management activities plan to comply with Section 3.1.5-7 of NUREG/CR-6101 and Section 4.3.7 of IEEE Std 1228-1994 is described in Section 3.11 “SCMP” of the SPM.

### **3.9.7.8 Software Quality Assurance Activities**

The software quality assurance activities plan to comply with Section 3.1.5-8 of NUREG/CR-6101 and Section 4.3.8 of IEEE Std 1228-1994 is described in Section 3.3 “SQAP” and Section 3.10 “SVVP” of the SPM.

### **3.9.7.9 Software Verification and Validation Activities**

The software quality assurance activities plan to comply with Section 4.3.9 of IEEE Std 1228-1994 is described in Section 3.10 “SVVP” of the SPM.

### **3.9.7.10 Tool Support and Approval**

The tool support and approval plan to comply with Section 3.1.5-9 of NUREG/CR-6101 and Section 4.3.10 of IEEE Std 1228-1994 is described in Section 3.2 “SDP” of the SPM.

### **3.9.7.11 Previously Developed or Purchased Software**

The PSMS consists of a complete integration of hardware and software for the US-APWR project, designed specifically for nuclear safety applications and is configured using the MELTAC platform, described in the technical report MUAP-07005 “Safety System Digital

Platform –MELTAC- “. MELTAC platform has been fully qualified to nuclear standards and has significant nuclear operating experience as described in the technical report MUAP-07005 “Safety System Digital Platform –MELTAC- “. Other purchased basic and application software does not apply to the PSMS of the US-APWR project.

The application software to be installed in the PSMS for each US-APWR project shall be developed under controlled by this SPM. The basic software to be installed in the PSMS are previously developed software as described in the technical report MUAP-07005 “Safety System Digital Platform –MELTAC- “ and other related technical reports. The basic software shall be approved and installed in the PSMS by following process to comply with requirements in Section 3.1.5-10 of NUREG/CR-6101 and Section 4.3.11 of IEEE Std 1228-1994.

- (1) Determine the interfaces to and functionality of the previously developed software.
- (2) Identify relevant documents (e.g., product specification, design documents, usage documents) that are available to the obtaining organization and determine their status.
- (3) Determine the conformance of the previously developed software to published specifications.
- (4) Identify the capabilities and limitations of the previously developed software with respect to the project’s requirements.
- (5) Following an approved test plan, test the safety-critical features of the previously developed software independent of the project’s software.
- (6) Following an approved test plan, test the safety-critical features of the previously developed software with the project’s software.
- (7) Perform a risk assessment to determine if the use of the previously developed software will result in undertaking an unacceptable level of risk.

The software life cycle process control plan for the basic software is described in the technical report JEXU-1012-1132 “MELTAC Platform Basic Software Program Manual (Basic SPM)” to comply with all requirements of NUREG/CR-6101 and IEEE Std 1228-1994, and all design changes or up-grades shall be controlled by this Basic SPM.

### **3.9.7.12 Subcontractor Management**

The subcontractor management plan is to comply with Section 3.1.5-11 of NUREG/CR-6101 and Section 4.3.12 of IEEE Std 1228-1994.

The basic software shall be controlled to ensure that it is maintained in accordance with the "MELTAC Platform Basic Software Manual" (JEXU-1012-1132) (Reference 24) and meets the requirements of the software safety analyses for the PSMS application software.

### **3.9.7.13 Process Certification**

The process certification plan to comply with Section 3.1.5-12 of NUREG/CR-6101 and Section 4.3.13 of IEEE Std 1228-1994 is described in Section 3.3 "SQAP" and Section 3.10 "SVVP" of the SPM.

## **3.9.8 Software Safety Analysis (SSA)**

Sections 3.9.8.1 describes the generic non-recurring SSA that are performed during the Plant Requirements Phase of the generic PSMS application software life cycle process for the generic US-APWR plant. These activities ensure to provide high reliability for the PSMS application software for the generic US-APWR plant. Section 3.9.8.2 through 3.9.8.5 describe the recurring SSA for the PSMS application software life cycle process of the US-APWR project from the System Requirements Phase to the Operations and Maintenance phase of each US-APWR project, including the SSA applied for any changes from the generic PSMS application software design during the Operation and Maintenance Phase. When combined together these SSA conform to the requirements of NUREG/CR-6101 and IEEE Std 1228-1994 for a software hazards analysis.

### **3.9.8.1 Plant Requirements Phase SSA**

The purpose of the SSA conducted during the Plant Requirements Phase is to establish the fundamental US-APWR plant critical safety characteristics as they affect the design and implementation of application software used in the PSMS.

The Plant Requirements Phase SSA is referred to as the Software Safety Analysis Preparation in Section 4.4.1 of IEEE Std 1228-1994.

All design basis SSA activities which shall be performed during the Plant Requirements Phase have all been completed and finished for the generic US-APWR plant and the results of these SSA are described in the US-APWR DCD, including Chapter 7, Chapter 15, Chapter 19 and the related technical reports.

The DT shall review the US-APWR DCD, including Chapter 7, Chapter 15, Chapter 19 and the related technical reports to identify the following items for each US-APWR project.

- (1) Scope of safety functions which will be performed by software.
- (2) Interfaces between the software and the rest of the safety system.
- (3) MELTAC Platform design changes that resulted from the US-APWR DCD Phase.

The results of the above review shall be documented by the DT and shall be independently verified by the VVT.

If the scope, interfaces or the MELTAC Platform design is changed, the following Plant Requirements Phase SSA shall be performed for the changed portion and the results of each SSA shall be revised and documented.

Outputs of the following SSA, including necessary changes based on the above review, of the Plant Requirements Phase are inputs for the SSA during the System Requirements Phase in the PSMS application software life cycle process for each US-APWR project.

#### **3.9.8.1.1 Preliminary Hazard Analysis**

A preliminary hazard analysis is intended to address preparatory activities associated with high-level PSMS system design, and interfaces between the PSMS application software and the rest of the PSMS design to identify hazardous system states or actions that can cause the system to enter a hazardous state as follows:

- (1) An analysis performed on the entire system or any portion of the system that identifies
  - a. Hazardous system states
  - b. Sequences of actions that can cause the system to enter a hazardous state
  - c. Sequences of actions intended to return the system from a hazardous state to nonhazardous state

Hazardous states are the states that would prevent the PSMS from performing actions intended to mitigate the consequences of plant accidents.

- (2) An evaluation of the high-level system design to identify those functions that will be performed by software and specifying the software-related actions that will be required of the software to prevent the system from entering a hazardous state, or to move the system from a hazardous state to a nonhazardous state.
- (3) The interface between the software and the rest of the system.

The PSMS of each US-APWR project is implemented through the software and hardware of the MELTAC platform. The MELTAC platform hazard analysis described in the technical report JEXU-1015-1009 "MELTAC Platform Basic Software Safety Report", establishes the preliminary hazards analysis for the PSMS. This analysis confirms that the MELTAC platform can prevent hazardous systems states due to any conditions including software and hardware including the inter-division communication design. The analysis also confirms that internal hardware or software failures that result in hazardous system states can be either automatically or manually detected. Detection allows correction before the concurrence of hazardous states in multiple PSMS divisions.

#### **3.9.8.1.2 Response Time Analysis**

The response time analysis ensures that the PSMS satisfy the DCD Chapter 15 safety analysis performance requirements and assumptions.

Timing and sizing analysis of the PSMS application software and hardware requirements has been performed and all requirements and results are described in the DCD Chapter 7 and the technical report MUAP-09021 "Response Time of Safety I&C System".

The technical report MUAP-09021 provides response time allocations. It demonstrates that, with those allocations, the response time requirements in Chapter 15 can be met.

#### **3.9.8.1.3 Criticality Analysis**

The criticality Analysis determines the functionality of each software subsystem and assigns a safety classification for each software subsystem in accordance with the safety functions. As defined in Section 2.3.2, all PSMS application software are designed to Software Integrity Level (SIL) 4, as defined in IEEE std 1012-1998, which is the highest software integrity level. Therefore, no additional functional classification analysis is performed.

In addition, the communication interface with the PCMS must be assessed for impacts that can lead to the PSMS system failures. The criticality analysis of the PCMS and the PSMS communications interface is a structured evaluation of the software characteristics for severity of impact of system failure, system degradation, and failure to meet software requirements or system objectives. The criticality analysis for the communication interface between the PCMS and the PSMS has been performed in Appendix D of the technical report MUAP-07004 "Safety I&C System Description and Design Process".

#### **3.9.8.1.4 Diversity and Defense-in-Depth Analysis**

The Diversity and Defense-in-Depth (D3) analysis is performed to (1) assess the diversity afforded within the PSMS, to ensure that adequate defense-in-depth has been provided in the design, (2) to verify that the Diverse Actuation System (DAS), including the indications and manual controls for credited manual actions and for control of critical safety functions are diverse from the MELTAC platform used in the reactor protection and the ESF actuation functions of the PSMS, and (3) confirm that the functions provided by the DAS, including functions initiated by manual actions, are sufficient to mitigate anticipated operational occurrences (AOO) and postulated accidents (PA) concurrence with PSMS Common Cause Failure (CCF). The results of this analysis are incorporated into succeeding phases of the PSMS software development. The PSMS application software development methodology established in this SPM is intended to minimize the potential for software CCF.

The D3 analysis has been performed in the topical report MUAP-07006 "Defense-in-Depth and Diversity" with supplemental information provided in Table 7.8-7 of the US-APWR DCD, and the technical report MUAP-07014 "US-APWR Defense-in-Depth and Diversity Coping Analysis".

#### **3.9.8.1.5 FMEA and Reliability Analysis**

The failure modes and effects analysis (FMEA) ensures that the single failure requirements associated with the system safety analysis requirements and assumptions are satisfied. The reliability analysis ensures that the safety system reliability, including consideration of software and hardware CCF, is sufficient to satisfy the US-APWR safety goals for the Core Damage Frequency (CDF) and the Large Early Relief Frequency (LERF) which are required by the DCD Chapter 19 and the related technical reports.

The PSMS FMEA has been performed to establish conformance with the requirements of IEEE Std 603-1991, specifically the single failure criterion as stated in clause 5.1, as endorsed by RG 1.153. The FMEA has been performed in accordance with Section 6.5.1 of MUAP-07004, which complies with Section 6 of IEEE Std 379-2000 "Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems". The FMEA for the PSMS reactor trip function is documented in DCD Table 7.2-8. The FMEA for the PSMS ESF actuation function is documented in DCD Table 7.3-7. These FMEA demonstrate that the adverse effect of any single failure is limited to a single PSMS division. Therefore, the remaining three PSMS divisions are sufficient to perform the safety functions. The FMEA also demonstrates that all failures are detectable; therefore, all failures can be corrected before multiple failures would coexist in multiple PSMS divisions.

The PSMS reliability analysis has been performed in accordance with Section 6.5.2 of technical report MUAP-07004 "Safety I&C System Description and Process". The summary and result of the PSMS reliability analysis are documented in Chapter 19 of the US-APWR DCD and the related technical reports. The reliability of the PSMS is credited in the PRA Fault Tree Analysis (FTA) and the PRA sensitivity analysis, which are documented in the technical report MUAP-07030 "US-APWR Probabilistic Risk Assessment", Attachment 6A.12 and Attachment 18A.1, respectively.

### **3.9.8.2 System Requirements Phase SSA**

The purpose of the SSA performed during the System Requirements Phase of the software life cycle process is to evaluate potential errors and deficiencies in the requirements that may contribute to a hazard.

The System Requirements Phase SSA is referred to as the requirements safety Analysis in Section 3.2.2 and 4.2.2 of NUREG/CR-6101 and the software safety requirements analysis in Section 4.4.2 of IEEE Std 1228-1994.

During the System Requirements Phase, the DT shall review the results of the Plant Requirements Phase SSA, as defined in Section 3.9.8.1, to write the System Requirements Specification (SysRS) for the PSMS software and hardware. The SysRS shall define key testing requirements to confirm the SSA, to the extent practical. The SysRS shall be independently verified, by the VVT as described in Section 3.10 "SVVP", to ensure traceability of all SSA requirements from the Plant Requirements Phase. Traceability of the requirement shall be documented using the RTM as described in Section 3.10 "SVVP".

Outputs of the following System Requirements Phase SSA will be inputs for the Design Phase SSA in the software life cycle process.

#### **3.9.8.2.1 Preliminary Hazard Analysis**

The results of the preliminary hazard analysis are described in the technical report JEXU-1015-1009 "MELTAC Platform Basic Software Safety Report".

The DT shall analyze all results of the preliminary hazard analysis, and provide the SysRS to comply with this analysis.

The SysRS shall be independently verified, by the VVT, to ensure traceability of all related requirements from the preliminary hazard analysis at the Plant Requirements Phase as

described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

#### **3.9.8.2.2 Response Time Analysis**

The response time allocations are described in the technical report MUAP-09021 “Response Time of Safety I&C System”. As described in Section 2.3.1.3, during the System Requirements Phase, the DT shall perform the actual response time analysis of the MELTAC hardware and software configuration of the PSMS for each US-APWR project, in accordance with Section 6.5 of MUAP-07004 (including Section 4.4 of MUAP-07005). The response time analyses should be independently reviewed to ensure it demonstrates compliance to the response time allocations defined in MUAP-09021.

The DT shall analyze all results of the response time analysis, and provide the SysRS to comply with this analysis.

The SysRS shall be independently verified, by the VVT, to ensure traceability of all response time requirements at the Plant Requirements Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

#### **3.9.8.2.3 Criticality Analysis**

The results of the criticality analysis for the PSMS interdivision communication interfaces are described in Appendix D of the technical report MUAP-07004 “Safety I&C System Description and Design Process”.

The DT shall analyze all communication independence requirements, and provide the SysRS to comply with this analysis. The SysRS shall also reflect that all functions of the PSMS are software integrity level 4.

The SysRS shall be independently verified, by the VVT, to ensure traceability of all communications independence requirements at the Plant Requirements Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

#### **3.9.8.2.4 Diversity and Defense-in-Depth Analysis**

The results of the D3 analysis are described in the DCD Chapter 7, the related topical report MUAP-07006 “Defense-in-Depth and Diversity and the related technical report MUAP-07014 “US-APWR Defense-in-Depth and Diversity Coping Analysis”.

The DT shall analyze all these D3 requirements, and provide the SysRS to comply with this analysis.

The SysRS shall be independently verified, by the VVT, to ensure traceability of all D3 requirements at the Plant Requirements Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

### 3.9.8.2.5 FMEA and Reliability Analysis

The results of the PSMS FMEA and reliability analysis are described in the DCD Chapter 7, Chapter 19 and related the technical report MUAP-07030 “US-APWR Probabilistic Risk Assessment”.

The DT shall analyze all FMEA and reliability requirements, and provide the SysRS to comply with this analysis.

The SysRS shall be independently verified, by the VVT, to ensure traceability of all FMEA and reliability requirements at the Plant Requirements Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

### 3.9.8.2.6 Application Software Specification Analysis

All safety critical requirements for the PSMS application software have been analyzed and evaluated against the key safety qualities and have been described in the DCD Chapter 7 and the related technical reports. The DT shall analyze all these safety critical PSMS application software requirements, and provide the SysRS to comply with this analysis. The SysRS includes the Functional Diagram (FD) which described all functional requirements all PSMS functions, which is included in the DCD Chapter 7.

The SysRS shall be independently verified, by the VVT, to ensure traceability of all safety critical requirements from the Plant Requirements Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

### 3.9.8.3 Design and Implementation Phase SSA

The Design and Implementation Phase SSA are performed during the Design Phase of the PSMS hardware and application software and the Implementation Phase of the PSMS hardware and software to the PSMS during the software life cycle process. These SSA confirm that the safety critical functional requirements from the System Requirements Phase for the PSMS application software correctly implements the actual PSMS application software and the PSMS application software introduces no new hazards.

The Design and Implementation Phase SSA is referred to as the software design safety analysis in Section 3.3.3 and 4.3.3 of NUREG/CR-6101, the code safety analysis in Section 3.4.1 and 4.4.2 of NUREG/CR-6101, the software safety design analysis in Section 4.4.3 of IEEE Std 1128-1994 and the software safety code analysis in Section 4.4.4 of IEEE Std 1228-1994.

The purposes of the Design and Implementation Phase SSA are to provide adequate information for the DT to develop the detailed hardware and software configuration of the PSMS. Based on the Design Phase SSA described in the sections below, the DT shall generate the System Design Description (SysDD), including the hardware design description, the software design description and the interface design description.

Outputs of the following Design Phase SSA are inputs for the Test Phase SSA in the PSMS application software life cycle process.

#### **3.9.8.3.1 Functional Analysis**

Functional analysis ensures that each PSMS application software requirements and functions are translated and covered correctly in the Design Phase. All safety critical functional requirements for the PSMS in the SysRS have been analyzed and evaluated by the DT, and the DT shall provide the SysDD to comply with this analysis.

The SysDD shall be independently verified, by the VVT, to ensure traceability of all functional requirements at the Design Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”.

#### **3.9.8.3.2 Logic Analysis**

#### **3.9.8.3.3 Response Time Analysis**

The response time analysis conducted initially during the System Requirements Phase (see Section 3.9.8.2.3), should be revised and refined, as necessary, during the Design Phase. Revisions may not be needed if the detailed design configuration is bounded by the analysis conducted during the System Requirements Phase.

The results of the Design Phase response time analysis shall be independently verified to ensure traceability of all response time requirements at the Design Phase as described in Section 3.10 “SVVP”. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 “SVVP”. The VVT shall ensure the PSMS response time remains in compliance to the allocations defined in the technical report MUAP-09021 “Response Time of Safety I&C System”.

#### 3.9.8.3.4 Test Specification Evaluation

The validation test specifications are developed in this phase of the PSMS application software life cycle process.

The VVT shall provide validation test specifications based on the System Requirements Phase outputs to confirm that:

- (1) The fully integrated PSMS software and hardware will operate as intended.
- (2) Any task, or subtask, which cannot be tested, is documented and the impact on safety has been determined.

The DT may provide input to the validation test specifications for the VVT. The validation test specifications shall be independently reviewed to ensure traceability of all safety requirements from the System Requirements Phase as described in Section 3.10 "SVVP". Traceability of the requirements shall be documented using the RTM as described in Section 3.10 "SVVP".

#### 3.9.8.3.5 Software Safety Code Analysis

The software safety code analysis is performed during the Design Phase of the PSMS application software life cycle process to confirm that the safety-critical portions of the PSMS software design are correctly implemented in the software code, and the software coding introduces no new hazards. The Design and Implementation Phase SSA is referred to as the code safety analysis in Section 3.4.1 and 4.4.2 of NUREG/CR-6101 and the software safety code analysis in Section 4.4.4 of IEEE Std 1228-1994.

The VVT will review that the outputs of this analysis comply with all the input requirements from the SysDD, including the FBD, as described in Section 3.10 "SVVP". Traceability of the requirements shall be documented using the RTM as described in Section 3.10 "SVVP".

#### 3.9.8.4 Test Phase SSA

The Test Phase SSA are performed to confirm that the safety-critical portions of the PSMS application software design are correctly implemented in the actual PSMS application software, and the application software introduces no new hazards.

The Test Phase SSA is referred to as the integration safety analysis in Section 3.5.2 and 4.5.2 of NUREG/CR-6101, the validation safety analysis in Section 3.6.1 and 4.6.1 of NUREG/CR-6101, the installation safety analysis in Section 3.7.5 and 4.7.1 of NUREG/CR-6101 and the software safety test analysis in Section 4.4.5 of IEEE Std 1228-1994.

The DT and VVT shall review the SysRS and the SysDD, including the validation test specifications, etc., to perform the SSA described below during the Test Phase of the PSMS application software life cycle process. The outputs of the Test Phase shall be independently verified, by the VVT, to ensure traceability of all SSA requirements from the System Requirements Phase. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 "SVVP".

The Test Phase SSA is a recurring activity conducted for the PSMS application software for each US-APWR project. Test results, including safety problems and resolutions, shall be documented separately for each recurring system application on a project by project basis. Upon completion of the SSA conducted for the Test Phase, an SSA summary document shall be prepared to summarize the software safety analysis activities for each US-APWR project. The SSA summary is documented as a quality record in accordance with the SQAP of this SPM.

#### **3.9.8.4.1 Integration Test Analysis**

The integration test analysis ensures the comprehensiveness of the integration testing effort. The integration testing should ensure that the correct version of all hardware, the PSMS basic and application software are installed and operating together with no errors reported by the MELTAC self-diagnostics. Manual tests shall be conducted to confirm operability of all portions of the system that are not automatically tested, such as system binary/analog inputs and outputs. The PSMS integration test report for the PSMS of each US-APWR project summarizes the findings and the corrective actions of the integration testing.

The input documents for the integration test analysis are the SysRS, including the hardware and SRS. The DT provides the integration test specifications, procedures and reports as the output documents.

The VVT will verify the integration test outputs to ensure traceability and compliance with all input requirements. Traceability of the requirements shall be documented using the RTM. The Software Verification and Validation Plan (SVVP) is further described in Section 3.10 "SVVP". The Software Test Plan (STP) is further described in Section 3.12.

#### **3.9.8.4.2 Acceptance Test Analysis**

The acceptance test analysis ensures that all requirements of the SysRS are validated. The comprehensiveness of the testing effort should ensure that all testable requirements of the SysRS are confirmed. The acceptance testing is performed to validate that the functionality of the fully integrated system meets the design and licensee requirements. The acceptance test reports summarize the findings and the corrective actions of the system validation testing.

The input documents for the acceptance test analysis are the SysRS including the hardware and software requirements specifications. The VVT provides the acceptance test specifications, procedures and reports as the output documents.

The VVT will verify the acceptance test outputs to ensure traceability and compliance with all input requirements. Traceability of the requirements shall be documented using the RTM as described in Section 3.10 "SVVP". The SVVP is further described in Section 3.10. The STP is further described in Section 3.12.

### 3.9.8.5 Design Change SSA

The design change SSA are performed to identify the safety critical design elements of the PSMS application software that are affected directly or in-directly by a design change request as described in Section 3.11. The need for design changes is typically identified during the Operation and Maintenance Phase of the software life cycle. However, any design change needed after completion of any PSMS application software life cycle process, shall include the design change SSA.

The design change SSA shall examine the impact of the change on previously completed SSA. Previous SSA shall be repeated as necessary based on a regression analysis as described in Section 3.11 "SCMP".

This design change SSA is referred to as the change safety analysis in Section 3.8 of NUREG/CR-6101 and the software change analysis in Section 4.4.6 of IEEE Std 1228-1994.

The design change SSA shall include the following items:

- (1) The means for determining the impact of each change on safety.
- (2) The techniques used to determine which safety-critical software design elements (if any) are affected by changes.
- (3) The documentation to be revised to accurately reflect all software safety changes.
- (4) The Plant Requirements Phase SSA in Section 3.9.8.1 that must be repeated whenever the system or its environment is modified.
- (5) The extent to which regression testing in Section 3.9.8.4 is to be performed as a consequence of modifications to the system.

The above design change SSA shall also be performed, if the PSMS of a recurring US-APWR plant is changed from the generic documents generated during the PSMS application software life cycle process described in Sections 3.9.8.1 through 3.9.8.4, above.

The DT shall perform the design change SSA and all results of the design change SSA shall be documented as described in Section 3.11 "SCMP". All results of the design change SSA shall be independently review and verified by the VVT as described in Section 3.10 "SVVP".

### 3.9.8.6 Post Development

The purpose of the SSA conducted during the post development phase is to define the requirements for training, deployment, monitoring, maintenance, and retirement of the safety-critical software that are mercenary to ensure the continued safety of the system after deployment and until its orderly retirement.

### 3.9.8.6.1 Training

Training shall be provided in accordance with the systematic approach to training to assure safe operation of the software for US-APWR plant. The software training plan of the post development phase is described in Section 3.7 "STrngP".

### 3.9.8.6.2 Deployment

#### (1) Installation

All Software Safety Analysis (SSA) Tasks which are described in Section 3.9.8.2 through Section 3.9.8.5 assure installation of the software safety product consistent with the results of the SSA of the Plant Requirements Phase. The installation plan of the post development phase is described in Section 3.5 "SInstP".

#### (2) Startup and Transition

All requirements for safely starting the new system, and, if an old system is to be replaced, for making a safe transition from old system to the new system will be described in the operation and instruction manuals of the PSMS and the MELTAC platform which will be provided for each US-APWR project. The operation and instruction manuals shall include following items as minimum;

- a. Fallback modes for the new system
- b. Startup of backup components and subsystems
- c. Startup of the new systems
- d. Parallel operation with backups
- e. Parallel operation of the old system and the new system
- f. Subsystem vs. full system operation
- g. Switchover to full system operation
- h. Validation of results from the new system
- i. Cross validation of results between the old system and the new system
- j. Fallback in the case of failure of the new system, including fallback to an old system if one exists

#### (3) Operation Support

Operation Support shall be provided in accordance with the systematic approach to support plan to assure safe operation of the PSMS application software for US-APWR plant. The operation support plan of the post development phase is described in Section 3.8 "SOP".

### **3.9.8.6.3 Monitoring**

All requirements for the monitoring the safe operation of the PSMS application software within the PSMS are described in the DCD Chapter 7, Chapter 18 “Human Factors Engineering” and the related technical reports. All requirements for the procedures for documenting and reporting all safety concerns that are detected during the US-APWR plant operations and instruction phase will be described in the operation and instruction manuals which will be provided each US-APWR project. The operation and instruction manuals of each US-APWR project shall include procedures for verifying the integrity of the PSMS application software after its deployment.

### **3.9.8.6.4 Maintenance**

All requirements for the maintenance the PSMS application software for each US-APWR plant will be described in the operation and instruction manuals of the PSMS and the MELTAC platform which will be provided each US-APWR project. The operation and instruction manuals of the PSMS and the MELTAC platform shall include maintenance procedures for verifying the integrity of the safety critical software after its deployment.

The software maintenance is described in Section 3.6 “SMaintP”

### **3.9.8.6.5 Retirement and Notification**

The retirement and notification plan is described in Section 3.2 “SDP”.

### **3.9.9 Standards**

This SSP complies with the following guidance and standards.

- Section C.3 of RG 1.173 (Reference 22)
- Sections 3.1.5, 3.2.2, 3.3.3, 3.4.1, 3.5.2, 3.6.1, 3.7.5, 3.8 of NUREG/CR-6101 (Reference 26)
- All section IEEE Std 1228-1994 (Reference 10)

### 3.10 Software Verification and Validation Plan (SVVP)

#### 3.10.1 Purpose

The Software Verification and Validation Plan (SVVP) defines the verification and validation (V&V) activities during the PSMS application software life cycle, and also outlines procedures and methodologies for each of the V&V steps. The software V&V process based on this SVVP ensures that the developed software meets quality and the specified requirements for the PSMS.

##### 3.10.1.1 Scope

The scope of this SVVP is the PSMS application software and all aspects of the class 1E PSMS that relate to the application software (i.e., the plant-specific configuration of standard MELTAC digital platform components, including hardware and software, which is unique to the PSMS application). Each life cycle plan within this SPM, including this SVVP, considers the interaction between the unique application configuration of the PSMS and the generic MELTAC platform, as a completely integrated system. Life cycle activities that are exclusive to the MELTAC digital platform are defined by the BASIC SPM (JEXU-1012-1132), which is referenced by this SPM.

##### 3.10.1.2 General Description of V&V Process

This SVVP complies with the guidance and standards identified in Section 3.10.8.

The Software Integrity Levels (SIL) is defined in this SVVP. The SIL for all equipment covered by this SVVP shall be set to “level 4” in accordance with C.1 of RG 1.168 (Reference 18) unless otherwise specified.

V&V activities follow the PSMS application software life cycle model illustrated in Figure 3.10-2. Each V&V activity is consistent with each phase of the life cycle, with the exception of the plant requirements phase. The Plant Requirements Phase is concluded at the end of the US-APWR design certification process for the generic, reference design, or at the end of the COL process for a plant-specific application. The outputs from the plant requirements phase are inputs to the System Requirements Phase, where system-specific design and V&V activities begin. Application software V&V activities are concluded for a given plant-specific project at the end of the Installation phase. V&V activities are also initiated in response to reported problems or requested changes in the Operation and Maintenance Phase.

Each V&V activity is made up of V&V tasks as described in this SVVP. There is one V&V activity for each phase of the application software life cycle (with the exception of the plant requirements phase, as described above), and there are multiple V&V tasks for each V&V activity. Each V&V activity as listed in Figure 3.10-2 is described in a specific section of this SVVP, where V&V inputs, individual tasks, and V&V outputs are described, including the roles and responsibilities of the V&V individuals (by title) responsible for each V&V task. The acquisition phase and supply phase activities required by IEEE Std 1012-1998 are involved in Plant Requirements Phase. All V&V activities are conducted independently from design activities as described in Annex C of IEEE Std 1012-1998.

V&V activities are planned, scheduled, and directed by an independent V&V Team Manager (VVTM). Additional oversight is provided by the QA Manager (QAM) and the General Manager

(GM). V&V activities are not considered complete until the VVTM is satisfied that all tasks are complete, documented, and all identified V&V Anomaly Reports are properly disposed. Significant anomalies which QAM found out require the initiation of a Corrective Action Report (CAR) by QAM. The CAR process includes provisions for 10 CFR Part 21 reporting.

There are no project-specific or plant-specific SVVP. This SVVP serves the purpose of the V&V planning activity required by BTP 7-14 (Reference 1), and it demonstrates how the requirements of IEEE Std 1012-1998 are to be carried out in the form of implementing procedures, which are required to follow this SVVP.

### **3.10.2 Organization/Responsibilities**

#### **3.10.2.1 Organization**

Section 2.2 “Organization and Responsibilities” in this SPM describes the organization responsibilities in supporting the V&V activities. V&V activities are performed by an independent V&V Team (VVT).

The VVT shall be technically independent, managerially independent, and financially independent as defined in Annex C of IEEE Std 1012-1998.

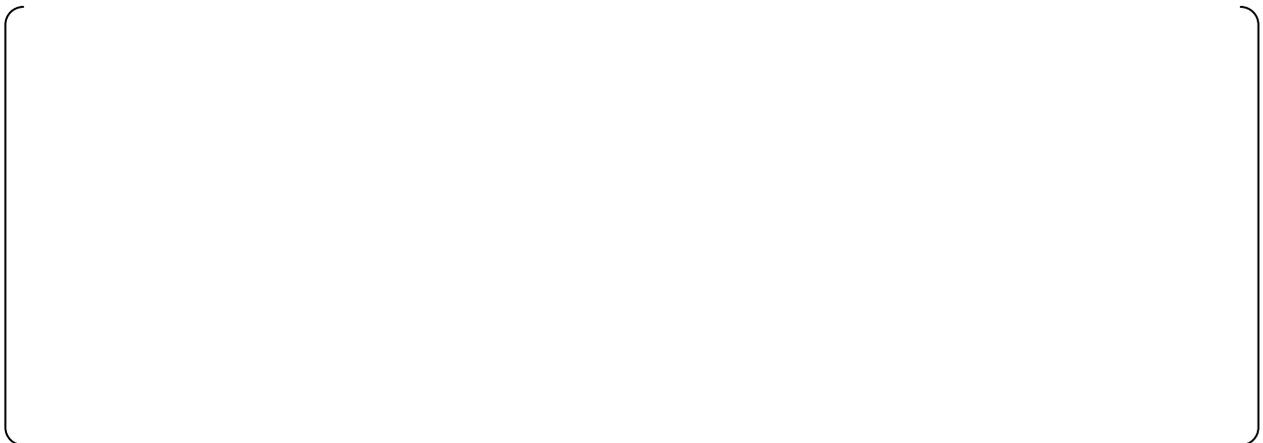
#### **3.10.2.2 Responsibilities**

##### **(1) VVT and VVTM Responsibilities**

The VVTM is responsible for all Independent V&V activities and tasks described in this SVVP and in Section 3.9.2 of the SSP (Section 3.9 of this SPM).

The VVT and VVTM are responsible for configuration management activities on V&V output documents and verification activities on design documents as described in Section 3.11 “Configuration Management Plan (SCMP)” of this SPM.

The VVTM is responsible for the initiation of V&V activities, development of Task Manuals, management of V&V tasks, and the final review and approval of V&V reports. The VVT and VVTM perform the following steps for each V&V phase activity (see numbered items in Figure 3.10-1):



The VVTM shall confirm that the qualifications and V&V independence criteria are met for the personnel selected for the VVT:

- 1) Technical, managerial and financial independence as defined in Annex C of IEEE Std 1012-1998.
- 2) V&V personnel, including assigned resources from other Design Teams, should have digital control system and US-APWR knowledge and experience equal to or greater than personnel on the Design Team (DT).

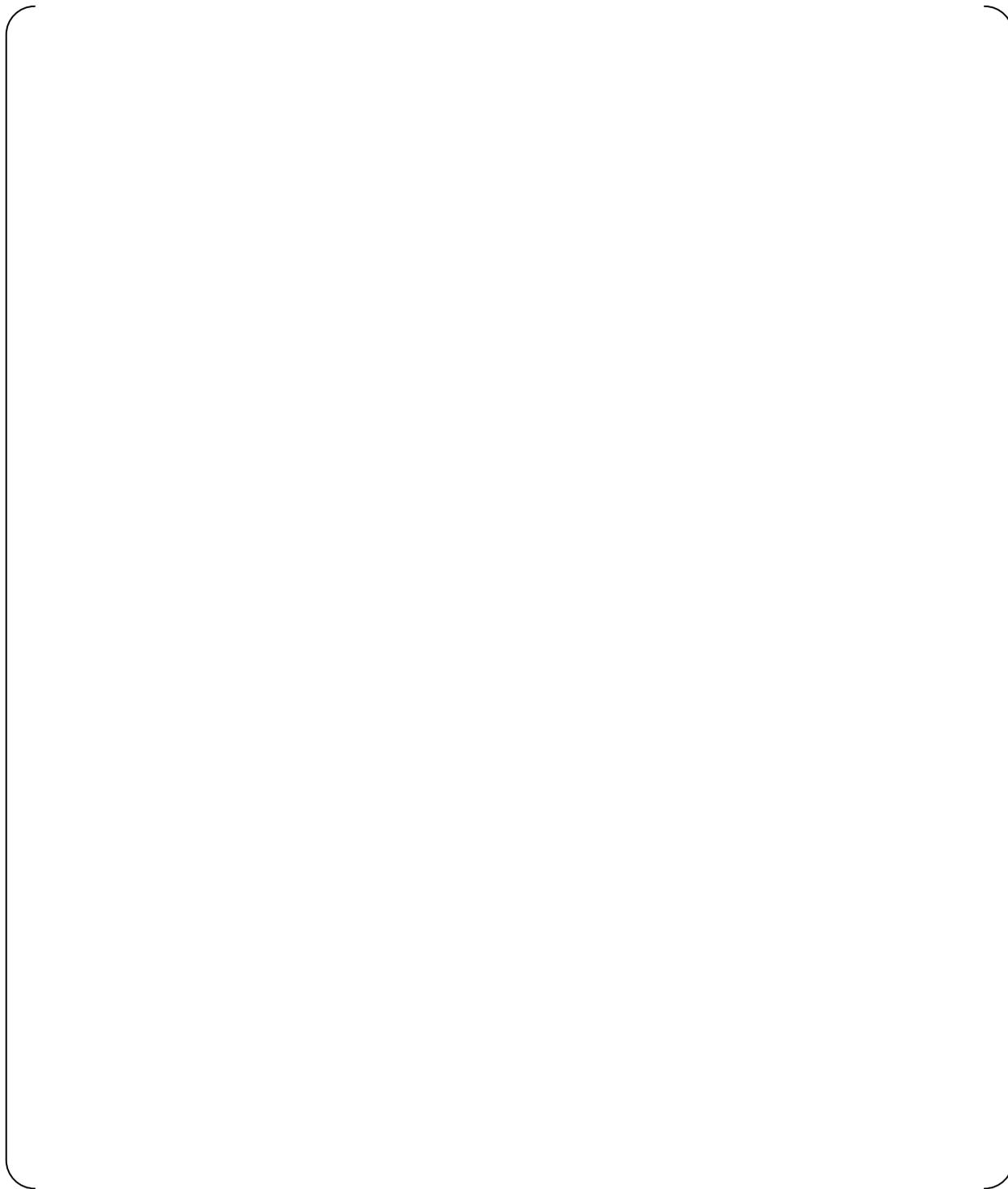
#### (2) QAM and QAE Responsibilities

The QAM is responsible for all activities that can affect the quality of items and services used in the PSMS. The QAM assigns QA Engineer (QAE) resources for reviewing V&V anomaly reports for adverse trends, and performing QA audits of V&V activities in accordance with Section 16 "Corrective Action" of PQD-HD-19005 "Quality Assurance Program (QAP) Description" (Reference 27). The QAM submits CAR to a related section, when there are significant anomalies in the V&V report. The QAM provides plans and manages schedules of the all QA audits activities.

#### (3) PJM Responsibilities

The Project Manager (PJM) oversees project-specific activities of the design and manufacturing departments, as well as the interfaces between the design and manufacturing departments and the VVT. The PJM has no authority to plan, schedule, or direct V&V activities.

The VVTM is responsible for all V&V activities and shall report the results of V&V activities to the responsible GM, QAM and PJM to assure oversight of any necessary corrective actions.



**Figure 3.10-1 V&V Activity Flow**

### 3.10.3 Management and Oversight of V&V Activities

Management of V&V spans all life cycle phases.

The QAM shall perform periodic assessments of the V&V process in the area of technical accomplishments, resource utilization, future planning, identified risks and lessons learned. VVT prepares V&V output documents, V&V anomaly reports and V&V phase summary reports. The summary reports are sent to QAM. QAM performs the review and/or audits by the way of required style explained in PQD-HD-19005 "Quality Assurance Program (QAP) Description" (Reference 27). V&V output documents and V&V phase summary reports shall be evaluated by QAM to determine if decisions to proceed to the next life cycle phase are correct, and to determine if any changes to V&V activities or tasks are required to improve the V&V process. Any V&V process changes that impact this SVVP shall force a revision of this SVVP.

The Project Plan, as described in the SMP (Section 3.1 of this SPM) identifies DT technical reviews and project milestones. The costs and the resources for performing V&V activities shall be identified by the VVTM and written into the Project Plan at the start of initial software life cycle.

### 3.10.4 Risks

The risks of the project related to VVT and DT are described in Section 3.1.6.2 "Risk management" of this SPM.

V&V activities are integrated into each life cycle phase. Experience has shown that the earlier an anomaly is discovered, the easier it is to resolve. Anomalies that are detected by the VVT in each phase of the life cycle process require the issuance and disposition of a formal V&V anomaly report as described in Section 3.10.6.5.1.

The potential risks of V&V activities shall be documented by the VVTM via the V&V Task Manuals prepared for each V&V phase activity. These risks shall be based on industry experience, US-APWR operating experience, QA audit findings, V&V Anomaly Reports, the Problem List, and project experience, and may include system risk, mechanical risk, hardware risk, size risk, complexity risk, pre-developed software risk, schedule risk, technical risks, and risks associated with program interfaces (project management, maintenance, users, etc.) risks. The Software Safety Plan (SSP) described in Section 3.9 of this SPM specifically addresses risks and activities associated with critical safety functions.

The VVTM shall identify contingency plans in the V&V Task Manuals, commensurate with identified risks, and report these contingency plans to the GM and PJM. Contingency plans

shall identify which department is responsible for managing the risk, and the potential magnitude of any issues or problems that can emerge if not managed correctly.

### **3.10.5 Measurement**

The VVT shall measure the effectiveness of the software development activities and describe how these metrics support the V&V objectives. These metrics should conform to the requirements in IEEE Std 7-4.3.2-2003 Clause 5.3.1.1 (Reference 5). A key measure is the number and severity of anomalies identified by the VVT during V&V activities. V&V anomalies shall be measured, recorded, analyzed and reported. V&V anomaly severity levels shall be classified as follows:

- (1) Severe (could have an impact on one or more critical safety functions as described in the SSP (Section 3.9 in this SPM))
- (2) Major (could affect one or more non-critical functions)
- (3) Minor (no effect on any critical or non-critical functions)

V&V phase activities are considered complete only if all V&V Anomaly Reports are resolved, and V&V output documents are approved by the VVTM. Evaluation criteria for the V&V tasks associated with each V&V phase activity are described in Section 3.10.6.1 to Section 3.10.6.4.

### **3.10.6 Procedures**

#### **3.10.6.1 Scope**

The scope of the PSMS application software V&V includes activities, tasks, and V&V output documents produced in the following life cycle phases as illustrated in Figure 3.10-2:

- (1) System requirements
- (2) Design
- (3) Implementation
- (4) Test
- (5) Installation
- (6) Operation and Maintenance

The Plant Requirements Phase illustrated in Figure 3.10-2 is defined as the activities that are conducted in the course of US-APWR Design Certification (DC) and COL Applications. There are no V&V activities, tasks or outputs for the plant requirements phase.

#### **3.10.6.2 Software Integrity Level (SIL)**

The intensity and rigor of V&V activities are commensurate with the SIL as defined in IEEE Std 1012-1998. The software subject to V&V activities under this SVVP is associated with PSMS, which requires a SIL "4" determination in accordance with C.1 of RG 1.168.

**Table 3.10-1 Software Integrity Level (SIL)**

Criticality	Description	Level
High	The selected function affects the critical features of the system. The PSMS application software is in this level.	4
Relatively high	The selected function affects the important features of the system.	3
Medium	The selected function affects the features of the system, but a second best strategy can be implemented to compensate for the features lost.	2
Low	The selected function affects the features of the system to a certain extent, but only causes inconvenience to the user if it is not performed according to the requirements.	1

### 3.10.6.3 V&V Activities

The following task items shall be performed in the conduct of V&V activities associated with PSMS application software used in the US-APWR.

These task items have been formulated in accordance with the items required for SIL 4 software as described in Section 5 of IEEE Std 1012-1998.

#### 3.10.6.3.1 Process: Management

The management process comprises the following generic activities and tasks that are applied to each V&V activity as described in this SVVP.

- (1) Preparing the plans for the V&V processes (satisfied by this SVVP)
- (2) Initiating the implementation of the plan (Section 3.10.2)
- (3) Monitoring the execution of the plan (Sections 3.10.3 through 3.10.5)
- (4) Analyzing problems discovered during the execution of the plan (Sections 3.10.2 through 3.10.5)
- (5) Reporting progress of the V&V processes (Section 3.10.5)
- (6) Ensuring products satisfy requirements (Section 3.10.6)

- (7) Assessing evaluation results (Section 3.10.6)
- (8) Determining whether a task is complete (Section 3.10.2)
- (9) Checking the results for completeness (Section 3.10.6)
- (10) Checking processes for efficiency and effectiveness (Section 3.10.5)
- (11) Reviewing project quality (Sections 3.10.3 through 3.10.5)
- (12) Reviewing project risks (Section 3.10.4)
- (13) Reviewing project measures (Section 3.10.5)

#### **3.10.6.3.1.1 Activity: Management of the V&V effort**

This activity comprises continual examination of V&V outputs, and any revisions of this SVVP that may be determined by the VVTM. Figure 3.10-2 provides an overall illustration of the relationships between design activities and V&V activities in the application software life cycle as described in this SVVP and the SPM.



**Figure 3.10-2 Overview of Application Software V&V Activities, Tasks and Outputs**

**3.10.6.3.1.1.1 Tasks**

## (1) Prepare SVVP.

- a. Generate the SVVP for all life cycle processes. This step is completed as evidenced by this SVVP.

## (2) Proposed change assessment

- a. Proposed software changes, including changes to design documents shall be evaluated by the DT and the VVT. Changes can arise from proposed modifications, enhancements, and additions as a result of anomaly corrections or requirement changes. The change evaluation shall determine the effects on the reference system designs, this SVVP, and previously completed V&V activities.
- b. The change assessment shall reiterate recurring tasks or initiate a revision to this SVVP to address changes to SVVP activities or tasks as required.
- c. Changes to the reference design or a plant-specific design shall be verified and validated in accordance with this SVVP.

## (3) Management review of V&amp;V activities

- a. The VVTM shall periodically assess and summarize V&V activities to determine if any V&V task changes are necessary, or to redirect VVT members on any specific V&V tasks.
- b. The VVTM shall recommend whether to proceed to the next phase of the development life cycle and associated V&V tasks, provide V&V outputs, including V&V Anomaly Reports, and the V&V Phase Summary Report to the organizations identified in Figure 3.10-1 of this SVVP.
- c. The VVTM shall verify that all V&V tasks conform to task requirements defined in the SVVP.
- d. The VVTM shall verify that V&V task results have a basis of evidence supporting the results.
- e. The VVTM shall assess all V&V results and provide recommendations for software product acceptance and certification. This assessment shall be an input to and described in the V&V Final Report.

The management reviews of V&V uses the review methodology in accordance with PQD-HD-19005 "Quality Assurance Program (QAP) Description" (Reference 27).

## (4) Project management and technical review support

## a. Project management support tasks:

- 1) The PJM shall check whether the release and updating of the design team documents subject to V&V have been performed in the proper sequence.

- 2) Task criterion: Release dates of the design output documents subject to V&V shall be later than the release dates of design input documents.

b. Technical review tasks:

- 1) The DTM shall confirm that internal design reviews have been adequately performed for the design output documents subject to V&V.
- 2) The DTM shall attend technical evaluation review meetings convened as necessary in the course of design activities, and assess design review reports for clarity, completeness, and timeliness.

The technical reviews use the review methodology in accordance with PQD-HD-19005 "Quality Assurance Program (QAP) Description" (Reference 27).

### **3.10.6.3.2 Process: Development (Initial and Changes)**

The development process phases are illustrated in Figure 3.10-2. V&V activities are performed to verify and validate the software items and documents produced by these life cycle phases.

#### **3.10.6.3.2.1 Activity: System Requirements Phase V&V**

The system requirements V&V activity addresses software requirements analysis. The objective of this V&V activity is to assure the appropriateness, completeness, correctness, testability, and consistency of the specified requirements.

The eight V&V topics listed in Clause 7.5.1 of IEEE 1012-1998 are described below:

(1) System Requirements Phase V&V tasks

- a. Prepare V&V Task Manual
- b. System Requirements Phase traceability analysis
- c. System requirements evaluation
- d. Interface analysis
- e. System Requirements Phase software safety analysis V&V
- f. Prepare System V&V Test Specification
- g. Prepare Acceptance V&V Test Specification
- h. System Requirements Phase V&V Anomaly Reports
- i. System Requirements Phase V&V Summary Report

---

(2) System Requirements Phase V&V methods and procedures

a. Prepare V&V Task Manual

The VVTM shall prepare a Task Manual for this activity as described in Section 3.10.2. The VVTM shall use the project plan and the V&V input documents listed above to inform the development of the Task Manual.

b. System requirements phase traceability analysis

The VVT shall record the Requirements Traceability Matrix (RTM) as described in Section 3.3 of this SPM.

The VVT shall trace the requirements specified in the system requirements specification to the following documents that are used as design inputs (by the DT) in the system requirements phase design activity, and analyze the identified relationships for correctness, consistency, completeness, and accuracy:

c. System requirements evaluation

The VVT shall evaluate the software requirements specified in the SysRS (e.g., functional, performance, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified or validated in later life cycle phases.

d. Interface analysis

The VVT shall evaluate the interface requirements specified in the SysRS (e.g., hardware, operator, maintenance, interface type, interface characteristics, safety, and security) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified

or validated in later life cycle phases.

e. System Requirements Phase software safety analysis V&V

The VVT shall evaluate the outputs of the SSA activities described in Section 3.9.8.2 of the SSP (Section 3.9 of this SPM) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified or validated in later life cycle phases.

f. Prepare System V&V Test Specification

The VVT shall develop a System V&V Test Specification as described in the STP (Section 3.12 of this SPM) for validating software requirements in the test phase. The system V&V test design shall describe the specific system-level test activities, target hardware system, input conditions and constraints, expected results and acceptance criteria. The System V&V Test Specification shall enable tracing of requirements specified in the system requirements specification to system level test designs, test cases, test procedures and test reports.

The VVT shall verify that the System V&V Test Specification conforms to the requirements of the STP (Section 3.12 of this SPM).

g. Prepare Acceptance V&V Test Specification

For recurring, plant-specific initial development or change projects, the VVT shall develop an Acceptance V&V Test Specification as described in the STP (Section 3.12 of this SPM) for validating software requirements in the test phase. The Acceptance V&V Test Specification is used to validate that the software correctly implements system and software requirements in an operational environment.

The Acceptance V&V Test Specification shall describe the specific test activities, target hardware system, input conditions and constraints, expected results and acceptance criteria. The Acceptance V&V Test Specification shall enable tracing of requirements specified in the system requirements specification to system level test designs, test cases, test procedures and test reports.

The VVT shall verify that the Acceptance V&V Test Specification conforms to the requirements of the STP (Section 3.12 of this SPM).

h. System Requirements Phase V&V Anomaly Reports

If the VVT detects any anomalies, they shall initiate V&V Anomaly Reports as described in Section 3.10.6.5.1.

i. System Requirements Phase V&V Summary Report

The VVTM shall prepare and issue a System Requirements Phase V&V Summary Report that describes the V&V inputs, V&V tasks, V&V outputs, and disposition of V&V Anomaly Reports.

(3) System requirements phase V&V inputs

[ ]

(4) System requirements phase V&V outputs



(5) System requirements phase V&V schedule

The V&V schedule is described below, including milestones, hold points, review schedules. The schedule of each task is addressed in the Task Manual.

(6) System requirements phase V&V resources

The resources for the performance of the V&V task are described below, including staffing, equipment, facilities, travel, and training. The Resources of each task are addressed in the Task Manual.

(7) System requirements phase V&V risk and assumptions

The Risks (Section 3.10.4) and assumptions of each task are addressed in the Task Manual.

(8) System requirements phase V&V roles and responsibilities

The typical roles and responsibilities are described in Section 3.10.2.2. The roles and responsibilities of each task are addressed in the Task Manual.

### **3.10.6.3.2.2 Activity: Design Phase V&V**

The design phase V&V activities address the software architectural design and the software detailed design. The objective of this V&V activity is to demonstrate that the application software design is correct, accurate, and is a complete transformation of the software requirements and that no unintended features are introduced.

The eight V&V topics listed in Clause 7.5.1 of IEEE 1012-1998 are described below:

(1) Design Phase V&V Tasks

- a. Prepare V&V Task Manual
- b. Design phase traceability analysis
- c. Software design evaluation

- d. Interface analysis
- e. Design phase software safety analysis V&V
- f. Prepare Component V&V Test Specification
- g. Prepare Component V&V Test Design
- h. Prepare Integration V&V Test Specification
- i. Prepare Integration V&V Test Design
- j. Prepare System V&V Test Design
- k. Prepare Acceptance V&V Test Design
- l. Design Phase V&V Anomaly Reports
- m. Design Phase V&V Summary Report

(2) Design Phase V&V Methods and procedures

- a. Prepare V&V Task Manual

The VVTM shall prepare a Task Manual for this activity as described in Section 3.10.2. The VVTM shall use the project plan and the V&V input documents listed above to inform the development of the Task Manual.

- b. Design Phase Traceability Analysis

The VVT shall update the Requirements Traceability Matrix (RTM) as described in Section 3.3 of this SPM.

The VVT shall trace the software design characteristics described in the SysDD (where FBD are included) to the SysRS (where FD are included) and analyze the identified relationships for correctness, consistency, completeness, and accuracy. The VVT shall verify that there are no characteristics described or shown in the SysDD that are not specified in the SysRS.

The VVT shall also verify that all of the requirements specified in the SysRS are fully and completely translated into the SysDD.

- c. Software design evaluation

The VVT shall evaluate the software design characteristics described in the SysDD (e.g., functional, performance, safety, security, human factors, data definitions,) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified or validated in later life cycle phases.

- d. Interface analysis

The VVT shall verify that the SysDD (an I/O List is included) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified or validated in later life cycle phases.

e. Design phase software safety analysis V&V

The VVT shall evaluate the outputs of the Design Phase SSA activities described in Section 3.9.8.3 of the SSP (Section 3.9 of this SPM) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified or validated in later life cycle phases.

f. Prepare Component V&V Test Specification

The VVT shall develop a Component V&V Test Specification as described in the STP (Section 3.12 of this SPM) for validating software component (e.g., software units, execution modules) requirements in the Implementation Phase. The Component V&V Test Specification shall describe the specific component test activities, target software component modules, input conditions and constraints, expected results and acceptance criteria. The Component V&V Test Specification shall enable tracing of requirements specified in the Software Requirements Specification to component level test designs, test cases, test procedures and test reports.

The VVT shall verify that the Component V&V Test Specification conforms to the requirements of the STP (Section 3.12 of this SPM).

g. Prepare Component V&V Test Design

The VVT shall develop a Component V&V Test Design as described in the STP (Section 3.12 of this SPM) for implementing the Component V&V Test Specification in the implementation phase. The Component V&V Test Design shall enable tracing of requirements specified in the Software Requirements Specification to component level test cases, test procedures and test reports.

The VVT shall verify that the Component V&V Test Specification conforms to the requirements of the STP (Section 3.12 of this SPM).

h. Prepare Integration V&V Test Specification

The VVT shall develop an Integration V&V Test Specification as described in the STP (Section 3.12 of this SPM) for validating the application software requirements as specified in the SRS on a target hardware system in the test phase. The Integration V&V Test Specification shall describe the specific integration test activities, target hardware modules or sub-systems, input conditions and constraints, expected results and acceptance criteria. The Integration V&V Test Specification shall describe the methods, tools, resources constraints and applicable procedures required for integration testing.

The VVT shall verify that the Integration V&V Test Specification conforms to the requirements of the STP (Section 3.12 of this SPM).

i. Prepare Integration V&V Test Design

The VVT shall develop an Integration V&V Test Design as described in the STP (Section 3.12

of this SPM) for implementing the Integration V&V Test Specification on target hardware modules or sub-systems in the Test Phase. The Integration V&V Test Design shall enable tracing of requirements specified in the Software Requirements Specification and Integration V&V Test Specification to test cases, test procedures and test reports.

The VVT shall verify that the Integration V&V Test Specification conforms to the requirements of the STP (Section 3.12 of this SPM).

j. Prepare System V&V Test Design

The VVT shall develop a System V&V Test Design as described in the STP (Section 3.12 of this SPM) for implementing the System V&V Test Specification on a target hardware system. The System V&V Test Design shall describe the specific system-level test activities, target system, input conditions and constraints, expected results and acceptance criteria. The System V&V Test Design shall enable tracing of requirements specified in the System Requirements Specification and System V&V Test Specification to system-level test cases, test procedures and test reports.

The VVT shall verify that the System V&V Test Design conforms to the requirements of the STP (Section 3.12 of this SPM).

k. Prepare Acceptance V&V Test Design

For recurring, plant-specific initial development or change projects, the VVT shall develop an Acceptance V&V Test Design as described in the STP (Section 3.12 of this SPM) for validating software requirements in the test phase. The Acceptance V&V Test Design is used to validate that the software correctly implements system and software requirements in an operational environment.

The Acceptance V&V Test Design shall enable tracing of requirements specified in the System Requirements Specification to system level test cases, test procedures and test reports.

The VVT shall verify that the Acceptance V&V Test Design conforms to the requirements of the STP (Section 3.12 of this SPM).

l. Design Phase V&V Anomaly Reports

If the VVT detects any anomalies, they shall initiate V&V Anomaly Reports as described in Section 3.10.6.5.1.

m. Design Phase V&V Summary Report

The VVTM shall prepare and issue a Design Phase V&V Summary Report that describes the V&V inputs, V&V tasks, V&V outputs, and disposition of V&V Anomaly Reports.

(3) Design phase V&V inputs

{ }

---

(4) Design phase V&V outputs

(5) Design phase V&V schedule

The V&V schedule is described below, including milestones, hold points, review schedules. The schedule of each task is addressed in the Task Manual.

(6) Design phase V&V resources

The resources for the performance of the V&V task are described below, including staffing, equipment, facilities, travel, and training. The resources of each task are addressed in the Task Manual.

(7) Design phase V&V risk and assumptions

The Risks (Section 3.10.4) and assumptions of each task are addressed in the Task Manual.

(8) Design phase V&V roles and responsibilities

The typical roles and responsibilities are described in Section 3.10.2.2. The roles and responsibilities of each task are addressed in the Task Manual.

**3.10.6.3.2.3 Activity: Implementation Phase V&V**

The implementation phase V&V activities address the application source code and execution modules that run on the MELTAC hardware platform. The objective of this V&V activity is to demonstrate that the source code and execution modules are correct, accurate, and are a complete transformation of the software design, and that no unintended features are introduced.

The eight V&V topics listed in Clause 7.5.1 of IEEE 1012-1998 are described below:

---

(1) Implementation phase V&V tasks

- a. Prepare V&V Task Manual
- b. Implementation phase traceability analysis
- c. Code evaluation
- d. Interface analysis
- e. Prepare Component V&V Test Cases
- f. Prepare Integration V&V Test Cases
- g. Prepare System V&V Test Cases
- h. Prepare Acceptance V&V Test Cases
- i. Prepare Component V&V Test Procedures
- j. Prepare Integration V&V Test Procedures
- k. Prepare System V&V Test Procedures
- l. Execute Component V&V Tests
- m. Implementation Phase V&V Anomaly Reports
- n. Implementation Phase V&V Summary Report

(2) Implementation phase V&V methods and procedures

- a. Prepare V&V Task Manual

The VVTM shall prepare a Task Manual for this activity as described in Section 3.10.2. The VVTM shall use the project plan and the V&V Input documents listed above to inform the development of the Task Manual.

- b. Implementation phase traceability analysis
-

c. Code evaluation

d. Interface analysis

The VVT shall verify that the software execution module interfaces with hardware, users, operators, and other systems are correct, consistent, complete, accurate, and can be validated.

e. Prepare Component V&V Test Cases

The VVT shall develop Component V&V Test Cases as described in the STP (Section 3.12 of this SPM). The Test Cases shall implement the Component V&V Test Design, and enable tracing to component-level test procedures and test reports.

The VVT shall verify that the Component V&V Test Cases conform to the requirements of the STP (Section 3.12 of this SPM).

f. Prepare Integration V&V Test Cases

The VVT shall develop Integration V&V Test Cases. The Test Cases shall implement the Integration V&V Test Design, and enable tracing to integration test procedures and test reports.

The VVT shall verify that the Integration V&V Test Cases conform to the requirements of the STP (Section 3.12 of this SPM).

g. Prepare System V&V Test Cases

The VVT shall develop System V&V Test Cases as described in the STP (Section 3.12 of this SPM). The Test Cases shall implement the System V&V Test Design, and enable tracing to system-level test procedures and test reports.

The VVT shall verify that the System V&V Test Cases conform to the requirements of the STP (Section 3.12 of this SPM).

#### h. Prepare Acceptance V&V Test Cases

For plant-specific projects, the VVT shall develop Acceptance V&V Test Cases as described in the STP (Section 3.12 of this SPM). The Test Cases shall implement the Acceptance V&V Test Design, and enable tracing to system-level test procedures and test reports.

The VVT shall verify that the Acceptance V&V Test Cases conform to the requirements of the STP (Section 3.12 of this SPM).

#### i. Prepare Component V&V Test Procedures

The VVT shall develop Component V&V Test Procedures as described in the STP (Section 3.12 of this SPM). The Test Procedures shall implement the Component V&V Test Design and Test Cases, and enable tracing to component-level test reports.

The VVT shall verify that the Component V&V Test Procedures conform to the requirements of the STP (Section 3.12 of this SPM).

#### j. Prepare Integration V&V Test Procedures

The VVT shall develop Integration V&V Test Procedures as described in the STP (Section 3.12 of this SPM). The Test Procedures shall implement the Integration V&V Test Design and Test Cases, and enable tracing to integration test reports.

The VVT shall verify that the Integration V&V Test Procedures conform to the requirements of the STP (Section 3.12 of this SPM).

#### k. Prepare System V&V Test Procedures

The VVT shall develop System V&V Test Procedures as described in the STP (Section 3.12 of this SPM). The Test Procedures shall implement the System V&V Test Design and Test Cases, and enable tracing to system-level test reports.

The VVT shall verify that the System V&V Test Procedures conform to the requirements of the STP (Section 3.12 of this SPM).

#### l. Execute Component V&V Tests

The VVT shall execute the Component V&V Tests and record the results in accordance with the Component V&V Test Procedures.

The VVT shall validate that the component test results demonstrate that the component software modules correctly implement the design requirements.

The VVT shall validate that the component test results are traceable to the Component V&V Test Specification acceptance criteria, and that the test results meet the acceptance criteria.

Any discrepancies between the actual and expected test results shall be documented by way of a V&V Anomaly Report.

The VVT shall prepare a Component V&V Test Report as described in the STP (Section 3.12

of this SPM).

m. Implementation Phase V&V Anomaly Reports

If the VVT detects any anomalies, they shall initiate V&V Anomaly Reports as described in Section 3.10.6.5.1.

n. Implementation Phase V&V Summary Report

The VVTM shall prepare and issue an Implementation Phase V&V Summary Report that describes the V&V inputs, V&V tasks, V&V outputs, and disposition of V&V Anomaly Reports.

(3) Implementation phase V&V inputs



(4) Implementation phase V&V outputs



(5) Implementation phase V&V schedule

The V&V schedule is described below, including milestones, hold points, review schedules. The schedule of each task is addressed in the Task Manual.

(6) Implementation phase V&V resources

The resources for the performance of the V&V task are described below, including staffing, equipment, facilities, travel, and training.

The resources of each task are addressed in the Task Manual.

(7) Implementation phase V&V risk and assumptions

The Risks (Section 3.10.4) and assumptions of each task are addressed in the Task Manual.

(8) Implementation phase V&V roles and responsibilities

The typical roles and responsibilities are described in Section 3.10.2.2. The roles and responsibilities of each task are addressed in the Task Manual.

**Figure 3.10-3 Implementation V&V**

**3.10.6.3.2.4 Activity: Test Phase V&V**

The test phase V&V activities assures that the software requirements and systems requirements allocated to software are properly design and implemented by execution of integration, system, and acceptance test activities on the application source code and execution modules running on the MELTAC hardware platform. This V&V activity requires the execution of system and acceptance test specifications, test designs, test cases and test procedures prepared in earlier life cycle phases.

The eight V&V topics listed in Clause 7.5.1 of IEEE 1012-1998 are described below:

**(1) Test Phase V&V tasks**

- a. Prepare V&V Task Manual
- b. Test phase traceability analysis
- c. Test phase software safety analysis V&V
- d. Execute integration V&V test
- e. Execute System V&V Test
- f. Prepare Acceptance V&V Test Procedure
- g. Test Phase V&V Anomaly Reports
- h. Test Phase V&V Summary Report

**(2) Test Phase V&V Methods and procedures**

- a. Prepare V&V Task Manual

The VVTM shall prepare a Task Manual for this activity as described in Section 3.10.2. The VVTM shall use the Project Plan and the V&V Input documents listed above to inform the development of the Task Manual.

- b. Test Phase Traceability Analysis

The VVT shall update the Requirements Traceability Matrix (RTM) as described in Section 3.3 of this SPM.

**1) Integration Test Traceability**

The VVT shall trace the integration test characteristics in the Integration Test Cases and Procedures to the Integration V&V Test Specification and the Integration V&V Test Design, and analyze the identified relationships for correctness, consistency, completeness, and accuracy. The VVT shall verify that there are no characteristics described or shown in the Integration Test Cases and Procedures that are not specified or described in the Integration V&V Test Specification and the Integration V&V Test Design.

The VVT shall also verify that all of the test requirements and design characteristics described in the Integration V&V Test Specification and the Integration V&V Test Design are described in the Integration Test Cases and Procedures.

## 2) System Test Traceability

The VVT shall trace the system test characteristics in the System Test Cases and Procedures to the System V&V Test Specification and the System V&V Test Design, and analyze the identified relationships for correctness, consistency, completeness, and accuracy. The VVT shall verify that there are no characteristics described or shown in the System Test Cases and Procedures that are not specified or described in the System V&V Test Specification and the System V&V Test Design.

The VVT shall also verify that all of the test requirements and design characteristics described in the System V&V Test Specification and the System V&V Test Design are described in the System Test Cases and Procedures.

## 3) Acceptance Test Traceability

The VVT shall trace the acceptance test characteristics in the Acceptance Test Cases to the Acceptance V&V Test Specification and the Acceptance V&V Test Design, and analyze the identified relationships for correctness, consistency, completeness, and accuracy. The VVT shall verify that there are no characteristics described or shown in the Acceptance Test Cases that are not specified or described in the Acceptance V&V Test Specification and the Acceptance V&V Test Design.

The VVT shall also verify that all of the test requirements and design characteristics described in the Acceptance V&V Test Specification and the Acceptance V&V Test Design are described in the Acceptance Test Cases.

### c. Test Phase Software Safety Analysis V&V

The VVT shall evaluate the outputs of the SSA activities described in Section 3.9.8.4 of the SSP (Section 3.9 of this SPM) and verify that they are correct, complete, accurate, readable, unambiguous, and can be verified or validated in later life cycle phases.

### d. Execute Integration V&V Test Procedures

The VVT shall execute the Integration V&V Tests and record the results in accordance with the Integration V&V Test Procedures.

The VVT shall validate that the integration test results demonstrate that the integrated system correctly implements the Software Requirements Specification and the Integration V&V Test Specification.

The VVT shall validate that the integration test results are traceable to the Integration V&V Test Specification acceptance criteria, and that the test results meet the acceptance criteria.

Any discrepancies between the actual and expected test results shall be documented by way of a V&V Anomaly Report.

The VVT shall prepare an Integration V&V Test Report as described in the STP (Section 3.12 of this SPM).

e. Execute System V&V Test

The VVT shall execute the System V&V Tests and record the results in accordance with the System V&V Test Procedures. The System V&V Test is conducted in the factory environment, and may be witnessed by the US-APWR customer.

The VVT shall validate that the system test results demonstrate that the integrated system correctly implements the System Requirements Specification and the System V&V Test Specification.

The VVT shall validate that the system test results are traceable to the System V&V Test Specification acceptance criteria, and that the test results meet the acceptance criteria.

Any discrepancies between the actual and expected test results shall be documented by way of a V&V Anomaly Report.

The VVT shall prepare a System V&V Test Report as described in the STP (Section 3.12 of this SPM).

f. Prepare Acceptance V&V Test Procedure

For plant-specific initial development or change projects, the VVT shall develop Acceptance V&V Test Procedures as described in the STP (Section 3.12 of this SPM). The Acceptance V&V Test Procedures shall implement the Acceptance V&V Test Design and Test Cases, and enable tracing to Acceptance Test Reports.

The VVT shall verify that the Acceptance V&V Test Procedures conform to the test procedure requirements described in the STP (Section 3.12 of this SPM)

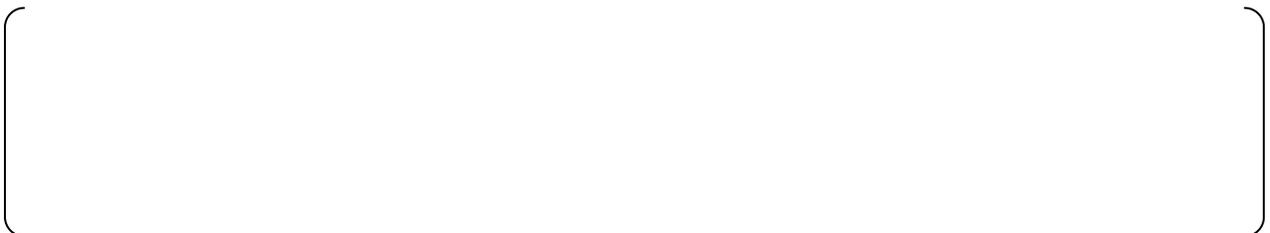
g. Test Phase V&V Anomaly Reports

If the VVT detects any other anomalies, they shall initiate V&V Anomaly Reports as described in Section 3.10.6.5.1.

h. Test Phase V&V Summary Report

The VVT shall prepare and issue a Test Phase V&V Summary Report that describes the V&V inputs, V&V tasks, V&V outputs, and disposition of V&V Anomaly Reports.

(3) Test Phase V&V Inputs



---

(4) Test Phase V&V Outputs



(5) Test Phase V&V Schedule

The V&V schedule is described below, including milestones, hold points, review schedules. The Schedule of each task is addressed in the Task Manual.

(6) Test Phase V&V Resources

The resources for the performance of the V&V task are described below, including staffing, equipment, facilities, travel, and training. The Resources of each task are addressed in the Task Manual.

(7) Test Phase V&V Risk and assumptions

The Risks (Section 3.10.4) and assumptions of each task are addressed in the Task Manual.

(8) Test Phase V&V Roles and responsibilities

The typical roles and responsibilities are described in Section 3.10.2.2. The roles and responsibilities of each task are addressed in the Task Manual.

**3.10.6.3.2.5 Activity: Installation Phase V&V**

The Installation V&V effort supports the system installation and software acceptance activities.

The objective of the Installation V&V activity is to verify and validate the correctness of the software installation in the target system environment.

The eight V&V topics listed in Clause 7.5.1 of IEEE 1012-1998 are described below:

(1) Installation Phase V&V Tasks

- a. Prepare V&V Task Manual
- b. Installation Configuration Inspection

- c. Execute Acceptance V&V Test
- d. Installation Phase V&V Anomaly Reports
- e. Prepare Installation Phase V&V Summary Report
- f. Prepare Final V&V Report

(2) Installation Phase V&V Methods and procedures

- a. Prepare V&V Task Manual

The VVTM shall prepare a Task Manual for this activity as described in Section 3.10.2. The VVTM shall use the Project Plan and the V&V Input documents listed above to inform the development of the Task Manual.

- b. Installation Configuration Inspection

The VVT shall inspect the installed system and its configuration items and verify they match the Installation Configuration Listing. The VVT shall confirm there are no hardware or software configuration items in the installed systems that are not listed in the Installation Configuration Listing.

- c. Execute Acceptance V&V Test

For plant-specific initial development or change projects, the VVT shall execute the Acceptance V&V Tests and record the results in accordance with the Acceptance V&V Test Procedures. The Acceptance V&V Test constitutes customer acceptance.

The VVT shall validate that the acceptance test results demonstrate that the system to be delivered correctly implements the System Requirements Specification and the Acceptance V&V Test Specification.

The VVT shall validate that the system test results are traceable to the System V&V Test Specification acceptance criteria, and that the test results meet the acceptance criteria.

Any discrepancies between the actual and expected test results shall be documented by way of a V&V Anomaly Report.

The VVT shall prepare an Acceptance V&V Test Report as described in the STP (Section 3.12 of this SPM).

- d. Installation Phase V&V Anomaly Reports

If the VVT detects any other anomalies, they shall initiate V&V Anomaly Reports as described in Section 3.10.6.5.1.

- e. Prepare Installation Phase V&V Summary Report

The VVTM shall prepare and issue an Installation Phase V&V Summary Report that describes the V&V inputs, V&V tasks, V&V outputs, and disposition of V&V Anomaly Reports.

f. Prepare Final V&V Report

The VVTM shall prepare and issue a Final V&V Report that describes the V&V phase-specific activities, results, disposition of V&V Anomaly Reports, and lessons learned.

The Final V&V Report shall also provide an assessment of the overall software life cycle and recommendations, if needed, for updating this SVVP, the SPM, or implementing procedures.

(3) Installation Phase V&V Inputs

[ ]

(4) Installation Phase V&V Outputs

[ ]

(5) Installation Phase V&V Schedule

The V&V schedule is described below, including milestones, hold points, review schedules. The Schedule of each task is addressed in the Task Manual.

(6) Installation Phase V&V Resources

The resources for the performance of the V&V task are described below, including staffing, equipment, facilities, travel, and training. The Resources of each task are addressed in the Task Manual.

(7) Installation Phase V&V Risk and assumptions

The Risks (Section 3.10.4) and assumptions of each task are addressed in the Task Manual.

(8) Installation Phase V&V Roles and responsibilities

The typical roles and responsibilities are described in Section 3.10.2.2. The roles and responsibilities of each task are addressed in the Task Manual.

---

### 3.10.6.3.3 Process: Operation and Maintenance

#### 3.10.6.3.3.1 Activity: Maintenance Phase V&V

The Maintenance Phase V&V activity encompasses problem reporting and resolution, change analysis, change initiation, maintenance review/acceptance, migration, and software disposal.

The objectives of the Maintenance V&V activity are to:

- (1) Assess proposed changes and their impact on the software
- (2) Evaluate anomalies discovered during operation
- (3) Assess migration requirements and disposal requirements
- (4) Initiate V&V activities

The eight V&V topics listed in Clause 7.5.1 of IEEE 1012-1998 are described below:

#### (1) Maintenance Phase V&V Tasks

- a. Prepare V&V Task Manual
- b. Perform Change Evaluation
- c. Anomaly Evaluation
- d. Regression Analysis

#### (2) Maintenance Phase V&V Methods and procedures

- a. Prepare V&V Task Manual

The VVTM shall prepare a Task Manual for this activity as described in Section 3.10.2. The VVTM shall use the Project Plan and the V&V Input documents listed above in the development of the Task Manual.

- b. Perform Change Evaluation

The VVT shall assess the proposed changes to determine the potential impact on the system requirements and design.

- c. Anomaly Evaluation

If the proposed change is a result of a reported problem, the VVT shall initiate a V&V Anomaly Report as described in Section 3.10.6.5.1.

The VVT shall evaluate the reported problem and determine if any changes are necessary for this SVVP or this SPM.

The VVT shall evaluate the V&V Anomaly Report disposition proposed by the responsible

department and determine if any changes are necessary for this SVVP or this SPM.

d. Regression Analysis

The VVT shall perform a Regression Analysis for the proposed change and determine the extent to which V&V activities, tasks and testing as described in this SVVP should be performed.

The VVTM shall assess the results of the Regression Analysis and determine the required resources, budget and other needs, and shall provide them to the PJM for inclusion in the Project Plan associated with the proposed change.

(3) Maintenance Phase V&V Inputs

[ ]

(4) Maintenance Phase V&V Outputs

[ ]

(5) Maintenance Phase V&V Schedule

The V&V schedule is described below, including milestones, hold points, review schedules. The Schedule of each task is addressed in the Task Manual.

(6) Maintenance Phase V&V Resources

The resources for the performance of the V&V task are described below, including staffing, equipment, facilities, travel, and training. The Resources of each task are addressed in the Task Manual.

(7) Maintenance Phase V&V Risk and assumptions

The Risks (Section 3.10.4) and assumptions of each task are addressed in the Task Manual.

(8) Maintenance Phase V&V Roles and responsibilities

The typical roles and responsibilities are described in Section 3.10.2.2. The roles and responsibilities of each task are addressed in the Task Manual.

### 3.10.6.4 V&V Reporting Requirements

V&V activities, tasks and results shall be documented in accordance with Clause 6.1 of IEEE Std 1012-1998.

V&V reports shall be prepared at the conclusion of each V&V task or activity as described within this SVVP.

The V&V reports to be prepared shall consist of the following five reports:

(1) Task-specific documents and reports

- a. As called out in Sections 3.10.6.3.2 and 3.10.6.3.3 in this SVVP
- b. Any specific task identified in this SVVP that does not describe a task-specific report (e.g., an Interface Analysis) shall be described in the V&V Phase Summary report.

(2) V&V Phase Summary Reports

- a. As described in Sections 3.10.6.3.2 and 3.10.6.3.3 in this SVVP

V&V Summary Reports shall contain the following items, as a minimum:

- 1) Summary report number and date
- 2) Project name, number and applicable phase
- 3) List of input documents reviewed (title, number and revision number)
- 4) Phase-specific deviations from SPM as noted in the Project Plan
- 5) Description of specific V&V activities, tasks, analyses and results
- 6) List of V&V Phase output documents
- 7) Summary of reported anomalies and their dispositions
- 8) Summary of lessons learned

(3) V&V Anomaly Reports

- a. As described in Section 3.10.6.5.1 in this SVVP

(4) V&V Final Report

- a. As described in Section 3.10.6.3.2.5 in this SVVP

V&V Final Reports shall contain the following items, as a minimum:

- 1) Summary of V&V activities at all phases
- 2) Summary of V&V task results
- 3) Summary of V&V anomalies and resolutions, including the number and severity of anomalies

- 4) Assessment of overall software project
- 5) Lessons learned/best practices
- 6) Recommendations

(5) V&V Optional Reports

- a. Any specific V&V studies conducted V&V activities are reported as special studies report.

### **3.10.6.5 V&V Administrative Requirements**

The Verification and Validation Administrative Requirements used in conjunction with the V&V activities described in this SVVP are outlined in the following Subsections.

#### **3.10.6.5.1 V&V Anomaly Reporting and Resolution**

A V&V anomaly is anything observed in the documentation or operation of the software that deviates from expectations based on this SVVP, V&V reference documents (i.e., the documents to which V&V Inputs are compared), or previous technical experience and/or calculations.

The VVTM shall provide V&V Anomaly Reports to the DTM or other responsible manager for evaluation, resolution, and disposition. The VVTM shall review the final disposition of each V&V Anomaly Report and determine if it is complete, correct, and appropriate for the identified V&V anomaly.

Any detected V&V Anomalies shall be documented by way of one or more V&V Anomaly Reports in each phase of the life cycle. V&V Anomaly Reports shall contain the following information, as a minimum:

- (1) Anomaly Report number
- (2) Project name, number and applicable phase
- (3) The date the anomaly was detected
- (4) The name of the V&V engineer that detected the anomaly
- (5) The V&V Activity and Task that were underway when the anomaly was detected
- (6) The V&V Input document that was being verified or validated
- (7) The V&V reference document that was being used for the V&V task
- (8) A detailed description and summary of the anomaly
- (9) The severity level of the V&V anomaly (See Section 3.10.5 of this SVVP)
- (10) The impact of the V&V anomaly

- (11) The date the V&V Anomaly Report was sent to the responsible manager for resolution
- (12) The final disposition of the anomaly, including documents and/or software that were affected, and the V&V activities and tasks that were performed
- (13) The date when the VVTM accepts the final disposition

#### **3.10.6.5.2 V&V Task Iterations**

If any revisions or changes are made to any Design Outputs and/or V&V inputs, including documents and software configuration items, the VVTM shall determine which V&V activities and tasks must be performed again, and direct the VVT accordingly.

The VVTM shall update Task Manuals if necessary.

Identified V&V Activities and Tasks shall be repeated until the VVTM confirms all V&V Anomaly reports are fully disposition and closed.

#### **3.10.6.5.3 Deviations**

When a deviation from the Project Plan, SPM or implementing procedures is considered necessary for a given project or life cycle phase activity, the Design Team Manager shall prepare a Deviation Request and present it to the PJM and the VVTM. Deviation Reports shall include the following:

- (1) Identification of the design activity/task and V&V activity/task to be amended or deleted
- (2) The basis for the requested deviation
- (3) An assessment of the impact on software quality
- (4) Indication of VVTM acceptance or rejection of the Deviation Request

The VVTM shall evaluate the Deviation Request and after discussion with the Design Team Manager, accept or reject the request. If any Deviation Requests are initiated, they shall be described in the V&V Phase Summary Report and the V&V Final Report.

#### **3.10.6.5.4 Record Retention**

All reports and records of V&V activities produced in the course of development or change projects, as described in this SVVP, shall be retained in accordance with Topical Report, PQD-HD-19005, "The Quality Assurance Program (QAP) Description" (Reference 27).

The VVTM shall determine the dates for retention of V&V records.

#### **3.10.6.6 V&V Documentation Requirements**

The test documents shall be composed of the purpose, format and contents as described in the STP (Section 3.12 of this SPM).

The test documents to be prepared shall consist of the following:

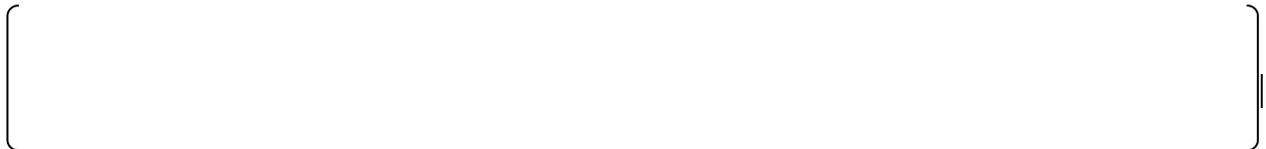
- (1) Test Specifications
- (2) Test Designs
- (3) Test Cases
- (4) Test Procedures
- (5) Test Reports, each consisting of
  - a. A test transmittal
  - b. A test log
  - c. Test incidents (with references to corresponding V&V Anomaly Reports)

### 3.10.7 Methods/Tools

The basic tasks performed in each stage of the V&V process in the software life cycle are described below. The specific tasks are described for each life cycle phase in this SVVP.

In each task of the V&V process, consistency between the upstream document and the downstream document at each life cycle phase shall be verified or validated.

- (1) Checking of basic software and MELTAC engineering tools



- (2) V&V Procedures

The procedures that implement the requirements of this SVVP shall include a check sheet, including check results against acceptance criteria. Check sheets and results shall be documented in the associated V&V Output document or V&V Phase Summary Report. V&V results include these check sheets and results. V&V procedures shall also list the interfacing procedures for record retention and V&V anomaly reporting.

### 3.10.8 Standards

This SVVP complies with the following guidance and standards.

- Clause 5.3 of IEEE Std 7-4.3.2-2003 (Reference 5) which is endorsed by RG 1.152 (Reference 17)
- IEEE Std 1012-1998 (Reference 11) which is endorsed by RG 1.168 (Reference 18)
- Section 3.1.4 of NUREG/CR6101-1993 (Reference 26)

### 3.11 Software Configuration Management Plan (SCMP)

This software configuration management plan (SCMP) describes the methods for maintaining generic and project-specific US-APWR PSMS application software configuration items (CIs) in a controlled configuration. An overview and a description of the general requirements for the PSMS application software life cycle process and a US-APWR project are described in Section 2.3 “General Requirements” of this SPM.

This SCMP addresses the six classes of information required by IEEE Std 828-1990 (Reference 13), as listed in Table 3.11-1. The referenced sections of the SCMP provide the detailed descriptions for each class of information.

**Table 3.11-1 IEEE Std 828-1990 vs. SCMP Section**

Class of Information	Description	Section in IEEE Std 828-1990	Section in this SCMP
Introduction	Describes the SCMP purpose, scope of application, key terms, and references	2.1	3.11.1
SCM Management	Identifies the responsibilities and authorities for accomplishing the planned activities	2.2	3.11.2
SCM Activities	Identifies all activities to be performed in applying to the project	2.3	3.11.3
SCM Schedules	Identifies the required coordination of SCM activities with the other activities in the project	2.4	3.11.4
SCM Resources	Identifies tools and physical and human resources required for execution of the SCMP	2.5	3.11.5
SCMP Maintenance	Identifies how the SCMP will be kept current while in effect	2.6	3.11.6

#### 3.11.1 Purpose, Scope and Applicability

##### 3.11.1.1 Purpose

The purpose of this SCMP is to describe the methods required for maintaining the project specific US-APWR PSMS application software CIs in a controlled configuration.

This SCMP defines the process for identifying PSMS application software CIs, developing and maintaining the CI list, controlling the implementation and changes to PSMS application software CIs and software documentation, and recording and reporting the status of changes. This SCMP is intended to be utilized throughout the PSMS application software life cycle.

The following minimum set of SCM activities shall be performed throughout the application software life cycle under implementing procedures that conform to the requirements of Topical Report “US-APWR Quality Assurance Program Description” (PQD-HD-19005) (Reference 27):

- (1) Identification and control of all PSMS application software designs and code

- (2) Identification and control of all PSMS application software design functional data (e.g., data templates and databases)
- (3) Identification and control of all PSMS application software design interfaces
- (4) Control of all PSMS application software design changes
- (5) Control of PSMS application software documentation (user, operating, and maintenance documentation)
- (6) Control and retrieval of qualification information associated with the PSMS application software designs and code
- (7) PSMS application software configuration audits
- (8) Status accounting

### 3.11.1.2 Scope

This SCMP shall be applied to all PSMS application software CIs for all US-APWR projects. Procedures that implement the requirements of this SCMP shall be controlled in accordance with the requirement in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005), and shall be referenced in the Project Plan as described in Sections 1.0 and 3.1 of this SPM. The application Software Development Plan (SDP) is described in Section 3.2 of this SPM.

The CIs for the PSMS application software to which this SCMP shall be applied includes the following PSMS application software items, associated documentation, and databases. See Section 3.11.3.1 for more detail.

- System Requirement Specification (SysRS)
- System Design Description (SysDD)
- V&V related documents
- PSMS application software

Execution of changes after software development, software V&V, software release, software test, or other activities described in this SPM that could impact the cost, schedule, or ability to perform defined SCM activities shall be identified using the Project Plan, Risk Matrix or Problem List tools described in the SMP (Section 3.10 of this SPM).

### 3.11.1.3 Key Terms

Key terms are defined here, as they apply to this SCMP in order to establish a common terminology.

The specific terms and these definitions as used within this SCMP (i.e., control point, release) are described in Appendix A of this SPM. Additional terms that are relevant are defined in IEEE Std 610.12-1990 (Reference 25), which are also described in Appendix A of this SPM, and are as follows:

- Baseline
- Component
- Configuration
- Configuration Audit
- Configuration Control
- Configuration Control Board
- Configuration Identification
- Configuration Item
- Configuration Management
- Configuration Status Accounting
- Interface
- Interface Control
- Software
- Software Library
- Software Life Cycle
- Unit
- Version

### 3.11.1.4 References

This SCMP complies with the guidance and standards identified in Section 3.11.12.

Each section of this SCMP identifies its specific requirements, directives, procedures, standards, terminology, and related documents.

### 3.11.2 SCM Management

This section describes the allocation of responsibilities and authorities for SCM activities to organizations and individuals within those organizations that are responsible PSMS application software life cycle activities and configuration items. This section includes three topics:

- (1) The organizations responsible for SCM activities described in this SCMP
- (2) The specific SCM responsibilities of these organizations
- (3) SCM policies and directives that apply to the PSMS application software.

#### 3.11.2.1 Organizations

All organizations that participate in or are responsible for any SCM activities and relationships between organizations for the PSMS application software project are described in Section 2.2 and Figure 2.2-1 of this SPM.

The functional roles of these organizational units within the PSMS application software life cycle activities are also described in Section 2.2 of this SPM.

#### 3.11.2.2 SCM Responsibilities

Table 3.11-2 provides a matrix that relates the organizations defined above to the SCM functions, activities, and tasks as described in this SCMP.

The DT is responsible for SCM activities on design outputs (described in the SDP; Section 3.2 of this SPM) that are generated by DTE.

The DTM is responsible for all SCM activities related to DT inputs and outputs described in the SDP. All SCM activities, with the exception of V&V and QA activities, shall be documented by the DT and approved by the DTM.

The DTM has the following specific responsibilities for PSMS application software SCM:

- (1) After the completion of each design activity in the application software life cycle process, the DTM releases design outputs for independent V&V as described in the SVVP
- (2) Upon completion of Implementation Phase design activities, the DTM releases the application software configuration items for Implementation Phase and Test Phase V&V activities described in the SVVP.
- (3) The DTM shall release the final version of the application software after successful completion of Installation Phase V&V activities described in the SVVP.

All SCM activities assigned to the DT shall be verified by the VVT. The VVT is responsible for SCM on the specific V&V activities that they generate.

The QA organization shall perform QA audits of SCM activities to ensure adherence to this SCMP and its implementing procedures. QA audits shall be performed as described in the SQAP (Section 3.3.5.2 of this SPM), and shall be coordinated with the PJM, DTM and VVTM.

The PJM and the DTM have final approval of change requests; however, the DTM is responsible for convening Change Control Board (CCB) activities as described in Section 3.11.2.2.1 of this SCMP.

**Table 3.11-2 Matrix of SCM Responsibilities**

<b>Organization / Individual</b>	<b>SCM Function, Activities, and Tasks</b>
DT	- SCM for design activities and design outputs
DTM	- Coordination with QA audits - Overall responsibility of SCMP implementation of DT - Documentation and review of SCM activities - Release of PSMS application software - Chairman and member of CCB - Final approval of change requests
VVT	- SCM on V&V activities
VVTM	- Coordination of QA audits - Overall responsibility of SCMP implementation of VVT - CCB member
QA	- Audit of SCM activities
QAM	- Overall responsibility of QA audit - CCB member
PJM	- Coordination of QA audits - Contact to Customer - CCB member

### 3.11.2.2.1 Configuration Control Boards (CCB)

CCBs shall be utilized prior to development of or changes to the PSMS application software under the following conditions:

- Proposed changes that affect functional or performance requirements defined in the Plant Requirements or System Requirements Phases
- Any PSMS application software changes required during the Test Phase that affect design outputs from the System Requirements or Design Phase

The PSMS application software CCB shall function as described in IEEE Std 1042-1987 (i.e., software CCB focused on technical issues). The purpose of the software CCB is to control major changes, such as changes to system functions and overall configuration of the application software, before proceeding with detailed change activities in the application software life cycle phases. The application software CCB members shall be the PJM, DTM, VVTM, and QAM as a minimum. As needed, representatives from engineers their respective organizations, or other organizations, may be included on the CCB.

The DTM is the CCB chairman and calls CCB meetings when required.

A CCB meeting is not required for minor changes that do not affect functional or performance requirements or design specifications, or changes to PSMS application software documents that do not affect a software release. This approach is acceptable because these changes (i.e., input/output format changes, clarifications, correction of typos, etc.) are limited by the existing functional requirements. All such changes shall be reviewed and approved as described in the SDP and SQAP (Sections 3.2 and 3.3 of this SPM, respectively), and require independent V&V as described in the SVVP (Section 3.10 of this SPM).

The application software CCB has the authority to approve or disapprove proposed change requests that require CCB activity. The CCB may also define required changes to application software CIs.

### **3.11.2.3 Applicable Policies, Directives, and Procedures**

Applicable policies, directives and procedures related to this SPM are described in Section 1.3 of this SPM.

### **3.11.3 SCM Activities**

The SCM activities described in this SCMP are grouped into four basic functions:

- (1) Configuration Identification
- (2) Configuration Control
- (3) Status Accounting
- (4) Configuration Audits and Reviews

The minimum information requirements for each function are described in Sections 3.11.3.1 through 3.11.3.4. The requirements for interface control and subcontractor/vendor control activities are identified separately in 3.11.3.5 and 3.11.3.6.

#### **3.11.3.1 Configuration Identification**

PSMS application software units shall be identified by a unique identifier (e.g., name or number), and their physical, functional or performance characteristics shall be described in a design output document (e.g., SysRS, SysDD per the SDP).

Sections 3.11.3.1.1 and 3.11.3.1.3 describe the minimum information required for configuration identification of the items listed in Section 3.11.1.2 (2).

##### **3.11.3.1.1 Identifying Configuration Items**

A CI List for all CIs that are to be delivered and maintained for the PSMS application software shall be developed and maintained by the DT.

The CI List shall be controlled and stored in the same manner as any other application software

document, and it shall retain the revision history of each CI so that it may be retrieved and so that the latest revision of each CI may be easily identified.

The DT is responsible for identification of all separately identifiable modules comprising the software CIs, along with the design output documents described in the SDP (Section 3.2 of this SPM).

An application software baseline shall be established at the end of Implementation Phase in the software life cycle. Approved changes that are created subsequent to a baseline shall be added to the baseline. The PSMS application software baseline is described in the SDP (Section 3.2 of this SPM).

#### **3.11.3.1.2 Naming Configuration Items**

PSMS application software documents described in this SPM shall be uniquely identified by name or number, with revision levels, and they shall be controlled and stored in accordance with the document control and record keeping requirements described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).

The application software CIs stored on media shall be uniquely identified and labeled when they are released by the DT. The labeling of application software CIs and media shall include unique identification of each CI, and revision and/or date time stamps for each CI. Configuration management sheets shall record the unique identifiers and versions of the released configuration items to be stored.

#### **3.11.3.1.3 Control of Configuration Items**

The format, location, and documentation requirements of PSMS application software CIs as described in this SCMP shall be controlled under implementing procedures. Access control procedures shall specify the storage locations and storage requirements of documents and magnetic media, including the physical marking and labeling of items.

Archived copies of each baseline of the PSMS application software used or created for US-APWR projects shall be kept in a fire-proof software library, and additional back-up copies shall be created and stored in a separate location for disaster recovery. Storage media shall be clearly and indelibly marked for easy and unambiguous identification. The versions of the basic software and development tools for application software used on each release of the application software shall be controlled and recorded.

The status accounting of the PSMS application software CIs is described in Section 3.11.3.3.

#### **3.11.3.2 Configuration Changes**

An application software baseline shall be established at the Implementation Phase in the software life cycle. Approved changes that are created subsequent to a baseline shall be added to the baseline. The PSMS application software baseline is described in the SDP (Section 3.2 of this SPM).

Changes to the PSMS application software shall be formally documented and approved as described in this SCMP. The documentation shall include the reason for the change, identification of the affected application software CIs, and the impact of the change on the plant

design and operation. Additionally, the documentation associated with an application change shall describe the plan for implementing the change in the plant (e.g., immediately implementing the change, or scheduling the change for a future version).

Changes to CIs shall be initiated by a Software Change Request (SCR) as described below:

#### **3.11.3.2.1 SCR Initiation**

The DT shall be responsible for receiving and processing SCRs, which may be initiated by any organization described in this SPM.

The minimum information required in a SCR is as follows:

- (1) Originator's name and organization
- (2) Date of request
- (3) The name(s) and version(s) of the affected application software CIs
- (4) SysDD (Functional Block Diagram, etc.) affected
- (5) Associated V&V anomaly reports or nonconformance reports (if any)
- (6) The need for the change
- (7) Description of the requested change
- (8) Requested completion date

#### **3.11.3.2.2 SCR Evaluation**

The PJM, DTM and VVTM shall each evaluate the requested change and independently determine the potential impact of the proposed change. If the proposed change requires CCB review and approval, the DTM shall call a CCB meeting as described in Section 3.11.2.2.1.

#### **3.11.3.2.3 SCR Approval or Disapproval**

The PJM is responsible for approving or disapproving SCRs with the exception of those that require CCB approval.

#### **3.11.3.2.4 SCR Implementation**

If an SCR is approved, the PJM shall prepare a Project Plan for new projects to implement of SCR as described in the SMP (Section 3.1 of this SPM). If the SCR is associated with an active project, the PJM shall update the Project Plan as necessary.

#### **3.11.3.3 Configuration Status Accounting**

The PSMS application software CIs, including documents, shall be recorded on Configuration Management Sheets that include the following information for each CI, as a minimum:

- Unique identifier and current version number
- Current status (under development, under test, or released)
- Last release date
- Associated design and test documents
- Associated V&V anomaly reports (if any)
- Associated nonconformance reports (if any)

The Configuration Management Sheets for design activities are the responsibility of the DT, and shall be verified by the VVT. The Configuration Management Sheets for V&V activities are the responsibility of the VVT. Configuration Management Sheets shall be controlled documents as described in Section 6 “Document Control” of Topical Report “US-APWR Quality Assurance Program Description” (PQD-HD-19005).

#### 3.11.3.4 Design Reviews and QA Audits

Design Reviews and QA Audits shall be performed as described in the SQAP (Section 3.3 of this SPM) to confirm that CIs conform to their required physical and functional characteristics.

#### 3.11.3.5 Interface Control

The following interface controls describe the methods for coordinating changes to the PSMS application software CIs that may be driven by activities that are outside the scope of this SCMP. The external items which are examined for potential interfacing effects on the PSMS application software include outputs from the Plant Requirements Phase and the basic software (controlled under the Basis Software Program Manual (JEXU-1012-1132)).

##### (1) Interface with Plant Requirements

PSMS application software CIs shall conform to the requirements produced in the Plant Requirements Phase as described in the SVVP (Section 3.10 of this SPM). Any proposed changes to the PSMS application software that do not fully and completely meet Plant Requirements shall not proceed until the associated Plant Requirements Phase documents are changed and approved in accordance with NRC regulations.

##### (2) Interface with Basic Software

### 3.11.3.6 Subcontractor / Vendor Control

Subcontractor/vendor control is to comply with Section 2.3.6 of IEEE Std. 828-1990.

The basic software shall be controlled to ensure that it is maintained in accordance with the "MELTAC Platform Basic Software Manual" (JEXU-1012-1132) (Reference 24) and the correct version of the basic software is used in the PSMS application software lifecycle.

### 3.11.4 SCM Schedules

PSMS application SCM activities described in this SCMP shall be performed in accordance with the schedule described in the Project Plan.

### 3.11.5 SCMP Resources

The tools and procedures, equipment, personnel, and training necessary for the implementation of the SCM activities in each phase are described in Sections 3.11.9 and 3.11.11. Personnel assigned to work on the PSMS application software development projects are trained in the requirements of the SQAP and the SCMP and skilled in the use of the tools as required by their individual job functions.

### 3.11.6 SCMP Maintenance

This SCMP is the only SCM plan for the US-APWR PSMS application software.

### 3.11.7 Security

All application software documents and software CI under configuration control shall be protected against the secure development/operational environment threats. Each organization described in this SPM shall be responsible for ensuring that the security related configuration controls and restrictions are maintained, as described in other sections and Appendix C of this SPM.

### 3.11.8 Measurement

SCM activities shall be measured as follows:

- Number of SCRs
- Number and severity level of V&V anomaly reports related to SCM activities
- Number of nonconformance reports related to SCM activities

The DTM and VVTM shall periodically assess these measures, and if an adverse trend is detected, shall initiate additional corrective actions.

### 3.11.9 Procedures

In addition to the SCM activities described above, phase-specific SCM activities are described in Sections 3.11.9.1 to 3.11.9.5.

**3.11.9.1 Plant Requirements and System Requirements Phases**

- (1) Requirements documents shall be controlled as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).
- (2) Independent V&V of design outputs from these phases shall be performed and documented as described in the SVVP. V&V documents shall be controlled as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).
- (3) V&V anomaly reports shall be dispositioned, including changes to affected design documents, as described in the SVVP.

**3.11.9.2 Design and Implementation Phases**

- (1) Design and implementation documents shall be controlled as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).
- (2) PSMS application software CIs shall be controlled as described in Section 3.11.3.3.
- (3) Independent V&V of design outputs from these phases shall be performed and documented as described in the SVVP. V&V documents shall be controlled as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).
- (4) V&V anomaly reports shall be dispositioned, including changes to affected design documents, as described in the SVVP.

**3.11.9.3 Test Phase**

- (1) All software/hardware configurations and design documents shall be frozen before entering the Test Phase.
- (2) Test phase V&V test documents shall be controlled as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).
- (3) The final as-tested application software configuration shall be documented in the V&V test reports.
- (4) V&V anomaly reports shall be dispositioned, including changes to affected design outputs, as described in the SVVP.
- (5) SCR documents shall be controlled and used to track software changes or required enhancements. An SCR may be used to disposition more than one V&V anomaly report.

**3.11.9.4 Installation Phase**

- (1) Ensure that all as-built documentation is under configuration control.
- (2) Acceptance test specifications, procedures and reports shall be controlled as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).

- (3) V&V anomaly reports shall be dispositioned, including changes to affected design outputs, as described in the SVVP.
- (4) SCR documents shall be controlled and used to track software changes or required enhancements. An SCR may be used to disposition more than one V&V anomaly report.

#### **3.11.9.5 Operation and Maintenance Phase**

- (1) The DTM releases the final version of the application software, and related documentation, to the customer after successful completion of the acceptance V&V test as described in the SVVP and the STP (Sections 3.10 and 3.12 of this SPM, respectively).
- (2) Nonconformance reports shall be initiated in response to PSMS application software problems reported by customers or other outside organizations. Nonconformance reports shall be assigned to a responsible organization, evaluated, and dispositioned as described in Topical Report "US-APWR Quality Assurance Program Description" (PQD-HD-19005).
- (3) SCRs shall be initiated in response to customer requests for changes to the PSMS application software as described in Section 3.11.3.2.
- (4) The DT shall maintain the configuration status accounting of the installed PSMS application software as described in Section 3.11.3.3.

#### **3.11.10 Record Keeping**

All records and records of SCM activities shall be prepared and retained as QA records as described in Section 3 "Design Control" of Topical Report PQD-HD-19005 "Quality Assurance Program Description".

#### **3.11.11 Methods/Tools**

The following methods/tools shall be used:

- (1) Configuration Item List

A CI List shall be developed and maintained by the DT and VVT as described in Section 3.11.3.1.

- (2) Configuration Management Sheet

Configuration management sheets shall be developed and maintained by the DT as described in Section 3.11.3.3.

- (3) Backups

Software backups of all program files, including tools, shall be initiated by the DT when a baseline is determined and shall be updated regularly. Backup methods shall be established and maintained the DTM. Backup files shall be kept in a separate area.

### 3.11.12 Standards

This SCMP complies with the following guidance and standards.

- IEEE Std 828-1990 (Reference 13) which is endorsed by RG 1.169 (Reference 23), with the following exception:  
Clause 3 is not applicable to this SCMP. Tailoring of this SCMP shall not be allowed because changes of plans described in this SPM shall be handled under control of the DCD.
- IEEE Std 1042-1987 (Reference 14) which is endorsed by RG 1.169 (Reference 23)
- Clause 7.2.3 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22)
- Clause 5.3.5 of IEEE Std 7.4.3-2-2003 (Reference 5) which is endorsed by RG 1.152 (Reference 17)
- Sections 3.1.3 and 4.1.3 of NUREG/CR-6101 (Reference 26)

Clause 5.4.2.1.3 of IEEE Std 7-4.3.2-2003, listed in B.3.1.11 of BTP7-14 (Reference 1) is not applicable to this SCMP. Commercial Off The Shell (COTS) items are not applied to the PSMS application software.

## 3.12 Software Test Plan (STP)

### 3.12.1 Purpose

This Software Test Plan (STP) complements the SVVP (described in Section 3.10 of this SPM), and provides additional details and minimum information requirements for the following V&V test activities:

- (1) Component V&V Test
- (2) Integration V&V Test
- (3) System V&V Test
- (4) Acceptance V&V Test

All tests of the application software are executed as V&V tests. In addition, for approved changes, regression analysis tasks are performed by the VVT to determine the extent to which these four test activities may be repeated as described in Section 3.10.6.3.3.1 (2) of the SVVP (Section 3.10 of this SPM).

### 3.12.2 Organization/Responsibilities

The V&V Team (VVT) shall perform all test activities described in this STP and the SVVP (Section 3.10 of this SPM).

The organization and responsibilities of the VVT are described in Section 2.2 and 3.10.2 of this SPM.

### 3.12.3 Security

The secure development/operational environment for the PSMS testing activities as described in this STP and the SVVP shall be assured in accordance with RG 1.152 (Reference 17) in the Test Phase. The detailed discussion on security issues is described in Section 3 of Appendix C of this SPM.

### 3.12.4 Measurement

Measurement of test activities is described in Section 3.10.5 of the SVVP (Section 3.10 of this SPM).

### 3.12.5 Procedures

Alignment with IEEE Std 1012-1998 (Reference 11) testing activities is shown in Table 3.12-1.

**Table 3.12-1 Alignment with IEEE Std 1012-1998 Testing Activities**

IEEE Std 1012-1998 Testing activity	Testing activity for the application software
Component Testing	Component V&V Test (Section 3.10.6.3 and 3.12.5.1 (1) of this SPM)
Integration Testing	Integration V&V Test (Section 3.10.6.3 and 3.12.5.1 (2) of this SPM)
System Testing	System V&V Test (Section 3.10.6.3 and 3.12.5.1 (3) of this SPM)
Acceptance Testing	Acceptance V&V Test (Section 3.10.6.3 and 3.12.5.1 (4) of this SPM)

The following test documents shall be prepared and reviewed by the VVT for each test activity described in this STP and the SVVP. The minimum required information for each test document type is described in Section 3.12.5.2. The VVTM is responsible for approving these test documents:

- (1) Test Specifications
- (2) Test Designs
- (3) Test Cases
- (4) Test Procedures
- (5) Test Reports

### **3.12.5.1 Testing Activities**

The following tests shall be demonstrated by the requirement of clause 5.4.1 of IEEE Std. 7-4.3.2-2003.

#### **(1) Component V&V Test**

#### **(2) Integration V&V Test**

**(3) System V&V Test**

**(4) Acceptance V&V Test**

### 3.12.5.2 Test Documents

The test documents for all application software tests described in this STP and the SVVP shall be prepared as described in the SVVP and this STP, via implementing procedures, in accordance with IEEE Std 829-1983 (Reference 15) and IEEE Std 1012-1998(Reference11). Test documents are listed in Table 3.12-2 and Table 4.0-1.

**Table 3.12-2 Alignment with IEEE Std 829-1983 Test Documents**

<b>IEEE Std 829-1983 Test Document</b>	<b>Application Software Test Document</b>
Test Plan	Test Specifications - Section 3.12.5.2 (1)
Test design specifications	Test Designs - Section 3.12.5.2 (2)
Test case specifications	Test Cases - Section 3.12.5.2 (3)
Test procedure specifications	Test Procedures - Section 3.12.5.2 (4)
Test summary reports	Test Reports - Section 3.12.5.2 (5)
Test logs	
Test incident reports	
Test item transmittal reports	

#### (1) Test Specifications:

Test specification documents shall contain the following information, as a minimum, as described in IEEE Std 829-1983 and this information shall be defined by the requirements of IEEE Std 1008-1987(Reference 16):

- a. Test specification identifier
- b. Introduction
- c. Test items
- d. Features to be tested
- e. Features not to be tested
- f. Approach

- g. Item pass/fail criteria
- h. Suspension criteria and resumption requirements
- i. Test deliverables
- j. Testing tasks
- k. Environmental needs, including required tools and equipment
- l. Responsibilities
- m. Staffing and training needs
- n. Schedule
- o. Risks and contingencies
- p. Approval

**(2) Test Designs:**

Test Design documents shall contain the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test design identifier
- b. Features to be tested
- c. Approach refinements
- d. Test identification
- e. Feature pass/fail criteria

**(3) Test Cases:**

Test Case documents shall contain the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test case identifier
- b. Related Test Specifications and Test Designs
- c. Input specifications
- d. Output specifications
- e. Environmental needs

- f. Special procedural requirements
- g. Interface dependencies

**(4) Test Procedures:**

Test Procedures shall contain the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test procedure identifier
- b. Purpose
- c. Test Cases to be executed
- d. Special requirements
- e. Procedure steps

**(5) Test Reports:**

Test reports consist of the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test report identifier
- b. Summary
- c. Variances
- d. Comprehensive assessment
- e. Summary of results
- f. List of V&V Anomaly Reports
- g. Evaluation
- h. Summary of activities
- i. Test Log
  - (1) Test log identifier
  - (2) List of tools and equipment used
  - (3) Description
  - (4) Activity and event entries
- j. Transmittal

- (1) Transmittal identifier
- (2) Transmitted items
- (3) Location
- (4) Status
- (5) Approvals

k. Approvals

V&V Anomaly Reports shall be prepared separately from Test Reports, as described in the SVVP (Section 3.10 of this SPM).

### 3.12.6 Record Keeping

All test documents described in the SVVP and this STP shall be prepared and retained as QA records as described in Section 3 “Design Control” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27).

### 3.12.7 Methods/Tools

V&V Testing shall be executed in accordance with the procedures described in Section 3.12.5 (4).

The MELTAC engineering tool shall be used for the test activities described in this STP and the SVVP and be required to be confirmed to be suitable for use with a test tool validation program by the clause 5.3.2 of IEEE Std 7-4.3.2-2003.

### 3.12.8 Standards

This STP shall be executed as described herein, in conjunction with the SVVP, via implementing procedures, in accordance with the following standards:

- (1) IEEE Std 829-1983 (Reference 15), as endorsed by RG 1.170 (Reference 20)
- (2) IEEE Std 1008-1987 (Reference 16), as endorsed by RG 1.171 (Reference 21)
- (3) IEEE Std 1012-1998 (Reference 11), as endorsed by RG 1.168 (Reference 18)
- (4) IEEE Std 7-4.3.2-2003 ( Reference 5), as endorsed by RG 1.152 (Reference17)
- (5) IEEE Std 1074-1995 ( Reference 6), as endorsed by RG 1.173 (Reference22)

## 3.12 Software Test Plan (STP)

### 3.12.1 Purpose

This Software Test Plan (STP) complements the SVVP (described in Section 3.10 of this SPM), and provides additional details and minimum information requirements for the following V&V test activities:

- (1) Component V&V Test
- (2) Integration V&V Test
- (3) System V&V Test
- (4) Acceptance V&V Test

All tests of the application software are executed as V&V tests. In addition, for approved changes, regression analysis tasks are performed by the VVT to determine the extent to which these four test activities may be repeated as described in Section 3.10.6.3.3.1 (2) of the SVVP (Section 3.10 of this SPM).

### 3.12.2 Organization/Responsibilities

The V&V Team (VVT) shall perform all test activities described in this STP and the SVVP (Section 3.10 of this SPM).

The organization and responsibilities of the VVT are described in Section 2.2 and 3.10.2 of this SPM.

### 3.12.3 Security

The secure development/operational environment for the PSMS testing activities as described in this STP and the SVVP shall be assured in accordance with RG 1.152 (Reference 17) in the Test Phase. The detailed discussion on security issues is described in Section 3 of Appendix C of this SPM.

### 3.12.4 Measurement

Measurement of test activities is described in Section 3.10.5 of the SVVP (Section 3.10 of this SPM).

### 3.12.5 Procedures

Alignment with IEEE Std 1012-1998 (Reference 11) testing activities is shown in Table 3.12-1.

**Table 3.12-1 Alignment with IEEE Std 1012-1998 Testing Activities**

IEEE Std 1012-1998 Testing activity	Testing activity for the application software
Component Testing	Component V&V Test (Section 3.10.6.3 and 3.12.5.1 (1) of this SPM)
Integration Testing	Integration V&V Test (Section 3.10.6.3 and 3.12.5.1 (2) of this SPM)
System Testing	System V&V Test (Section 3.10.6.3 and 3.12.5.1 (3) of this SPM)
Acceptance Testing	Acceptance V&V Test (Section 3.10.6.3 and 3.12.5.1 (4) of this SPM)

The following test documents shall be prepared and reviewed by the VVT for each test activity described in this STP and the SVVP. The minimum required information for each test document type is described in Section 3.12.5.2. The VVTM is responsible for approving these test documents:

- (1) Test Specifications
- (2) Test Designs
- (3) Test Cases
- (4) Test Procedures
- (5) Test Reports

### 3.12.5.1 Testing Activities

The following tests shall be demonstrated by the requirement of clause 5.4.1 of IEEE Std. 7-4.3.2-2003.

#### (1) Component V&V Test

#### (2) Integration V&V Test



**(3) System V&V Test**



**(4) Acceptance V&V Test**



### 3.12.5.2 Test Documents

The test documents for all application software tests described in this STP and the SVVP shall be prepared as described in the SVVP and this STP, via implementing procedures, in accordance with IEEE Std 829-1983 (Reference 15) and IEEE Std 1012-1998(Reference11). Test documents are listed in Table 3.12-2 and Table 4.0-1.

**Table 3.12-2 Alignment with IEEE Std 829-1983 Test Documents**

<b>IEEE Std 829-1983 Test Document</b>	<b>Application Software Test Document</b>
Test Plan	Test Specifications - Section 3.12.5.2 (1)
Test design specifications	Test Designs - Section 3.12.5.2 (2)
Test case specifications	Test Cases - Section 3.12.5.2 (3)
Test procedure specifications	Test Procedures - Section 3.12.5.2 (4)
Test summary reports	Test Reports - Section 3.12.5.2 (5)
Test logs	
Test incident reports	
Test item transmittal reports	

#### (1) Test Specifications:

Test specification documents shall contain the following information, as a minimum, as described in IEEE Std 829-1983 and this information shall be defined by the requirements of IEEE Std 1008-1987(Reference 16):

- a. Test specification identifier
- b. Introduction
- c. Test items
- d. Features to be tested
- e. Features not to be tested
- f. Approach
- g. Item pass/fail criteria

- h. Suspension criteria and resumption requirements
- i. Test deliverables
- j. Testing tasks
- k. Environmental needs, including required tools and equipment
- l. Responsibilities
- m. Staffing and training needs
- n. Schedule
- o. Risks and contingencies
- p. Approval

**(2) Test Designs:**

Test Design documents shall contain the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test design identifier
- b. Features to be tested
- c. Approach refinements
- d. Test identification
- e. Feature pass/fail criteria

**(3) Test Cases:**

Test Case documents shall contain the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test case identifier
- b. Related Test Specifications and Test Designs
- c. Input specifications
- d. Output specifications
- e. Environmental needs
- f. Special procedural requirements
- g. Interface dependencies

**(4) Test Procedures:**

Test Procedures shall contain the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test procedure identifier
- b. Purpose
- c. Test Cases to be executed
- d. Special requirements
- e. Procedure steps

**(5) Test Reports:**

Test reports consist of the following information, as a minimum, as described in IEEE Std 829-1983:

- a. Test report identifier
- b. Summary
- c. Variances
- d. Comprehensive assessment
- e. Summary of results
- f. List of V&V Anomaly Reports
- g. Evaluation
- h. Summary of activities
- i. Test Log
  - (1) Test log identifier
  - (2) List of tools and equipment used
  - (3) Description
  - (4) Activity and event entries
- j. Transmittal
  - (1) Transmittal identifier

(2) Transmitted items

(3) Location

(4) Status

(5) Approvals

k. Approvals

V&V Anomaly Reports shall be prepared separately from Test Reports, as described in the SVVP (Section 3.10 of this SPM).

### 3.12.6 Record Keeping

All test documents described in the SVVP and this STP shall be prepared and retained as QA records as described in Section 3 “Design Control” of Topical Report PQD-HD-19005 “Quality Assurance Program Description” (Reference 27).

### 3.12.7 Methods/Tools

V&V Testing shall be executed in accordance with the procedures described in Section 3.12.5 (4).

The MELTAC engineering tool shall be used for the test activities described in this STP and the SVVP and be required to be confirmed to be suitable for use with a test tool validation program by the clause 5.3.2 of IEEE Std 7-4.3.2-2003.

### 3.12.8 Standards

This STP shall be executed as described herein, in conjunction with the SVVP, via implementing procedures, in accordance with the following standards:

- (1) IEEE Std 829-1983 (Reference 15), as endorsed by RG 1.170 (Reference 20)
- (2) IEEE Std 1008-1987 (Reference 16), as endorsed by RG 1.171 (Reference 21)
- (3) IEEE Std 1012-1998 (Reference 11), as endorsed by RG 1.168 (Reference 18)
- (4) IEEE Std 7-4.3.2-2003 ( Reference 5), as endorsed by RG 1.152 (Reference17)
- (5) IEEE Std 1074-1995 ( Reference 6), as endorsed by RG 1.173 (Reference22)

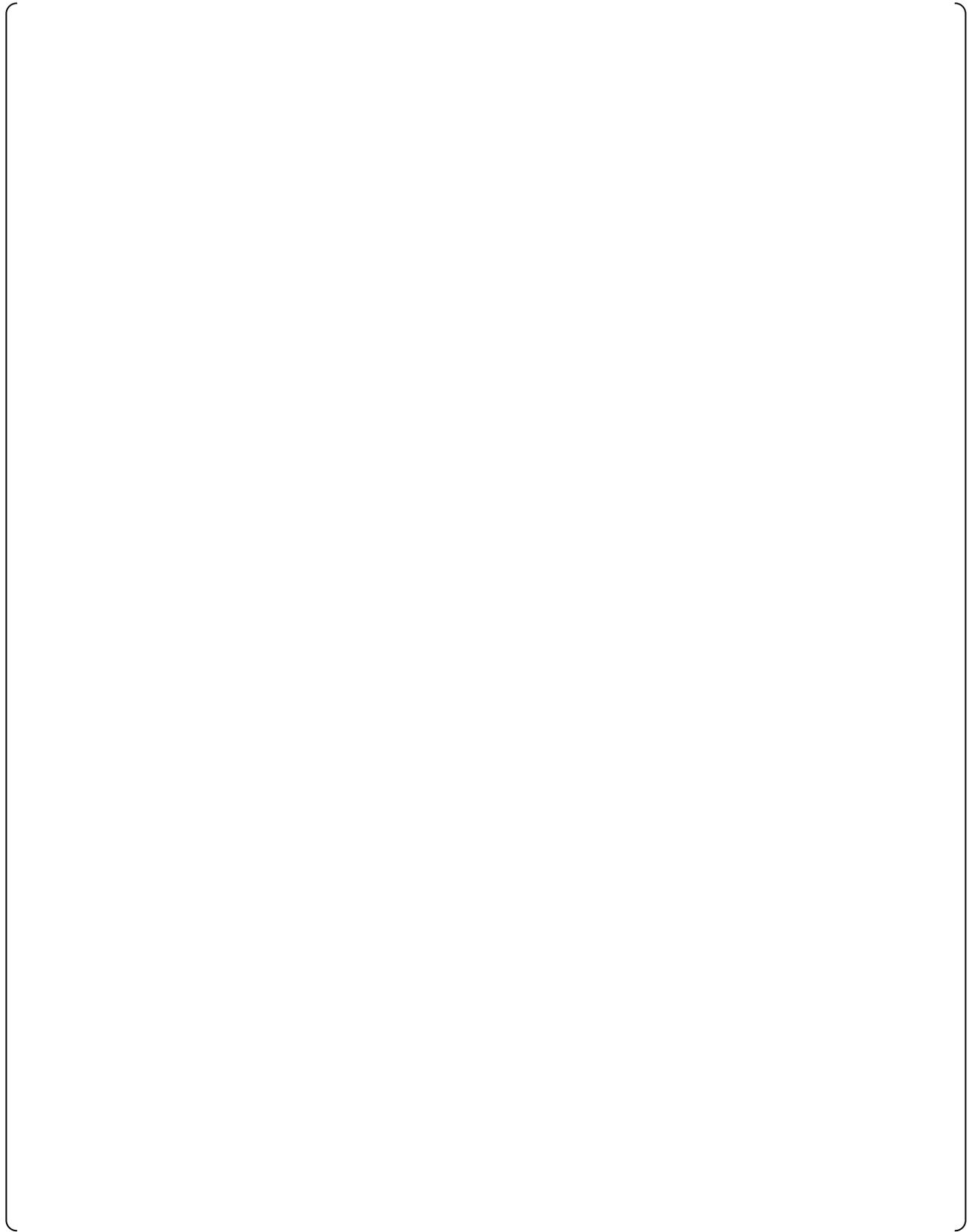
#### 4. OUTPUT DOCUMENTS

The following documents are created as the software life cycle process progresses. The table defines the organization responsible for creating the document.

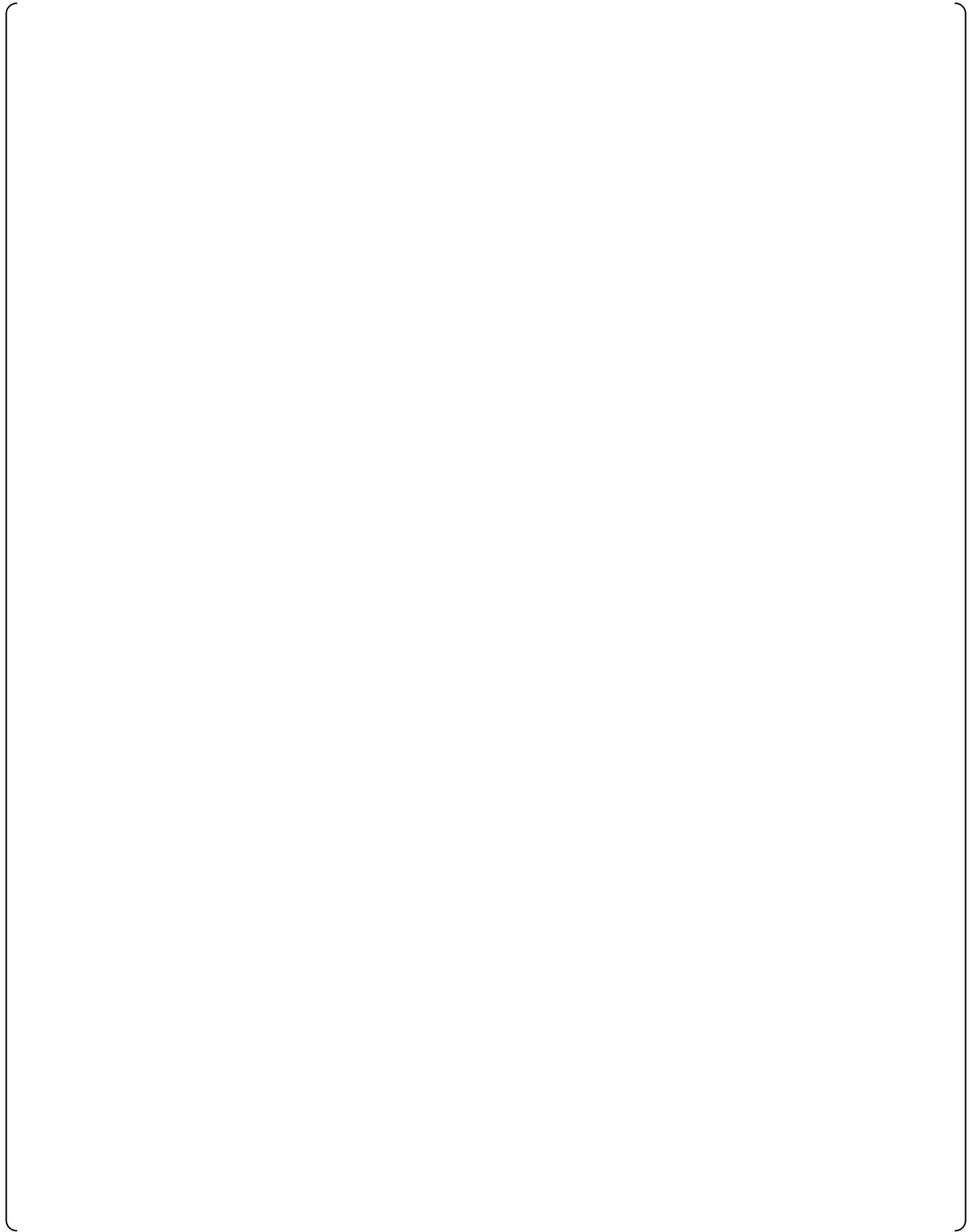
**Table 4-1 Output Documents of Project Department**



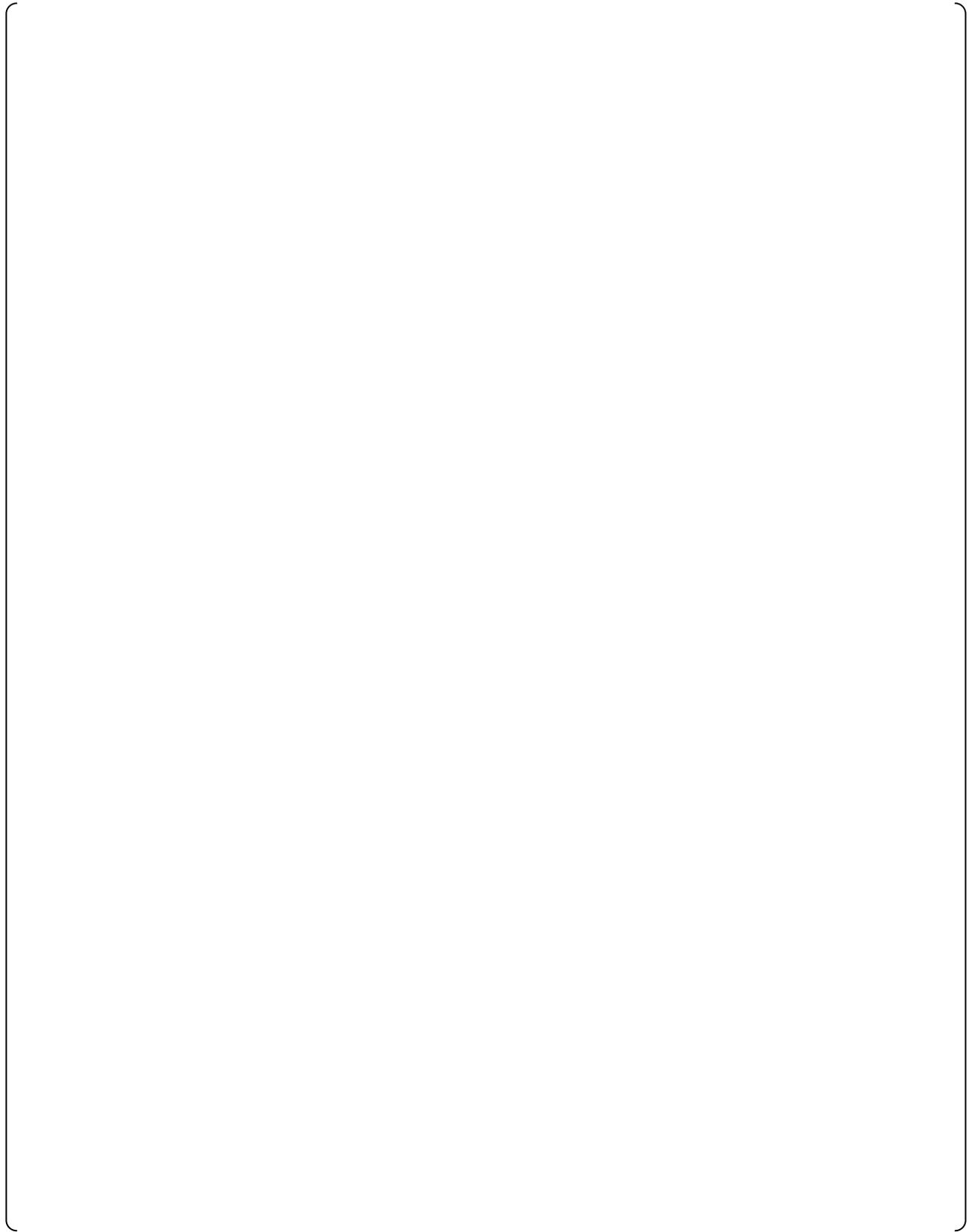
**Table 4-2 Output Documents of Design Team (1/2)**



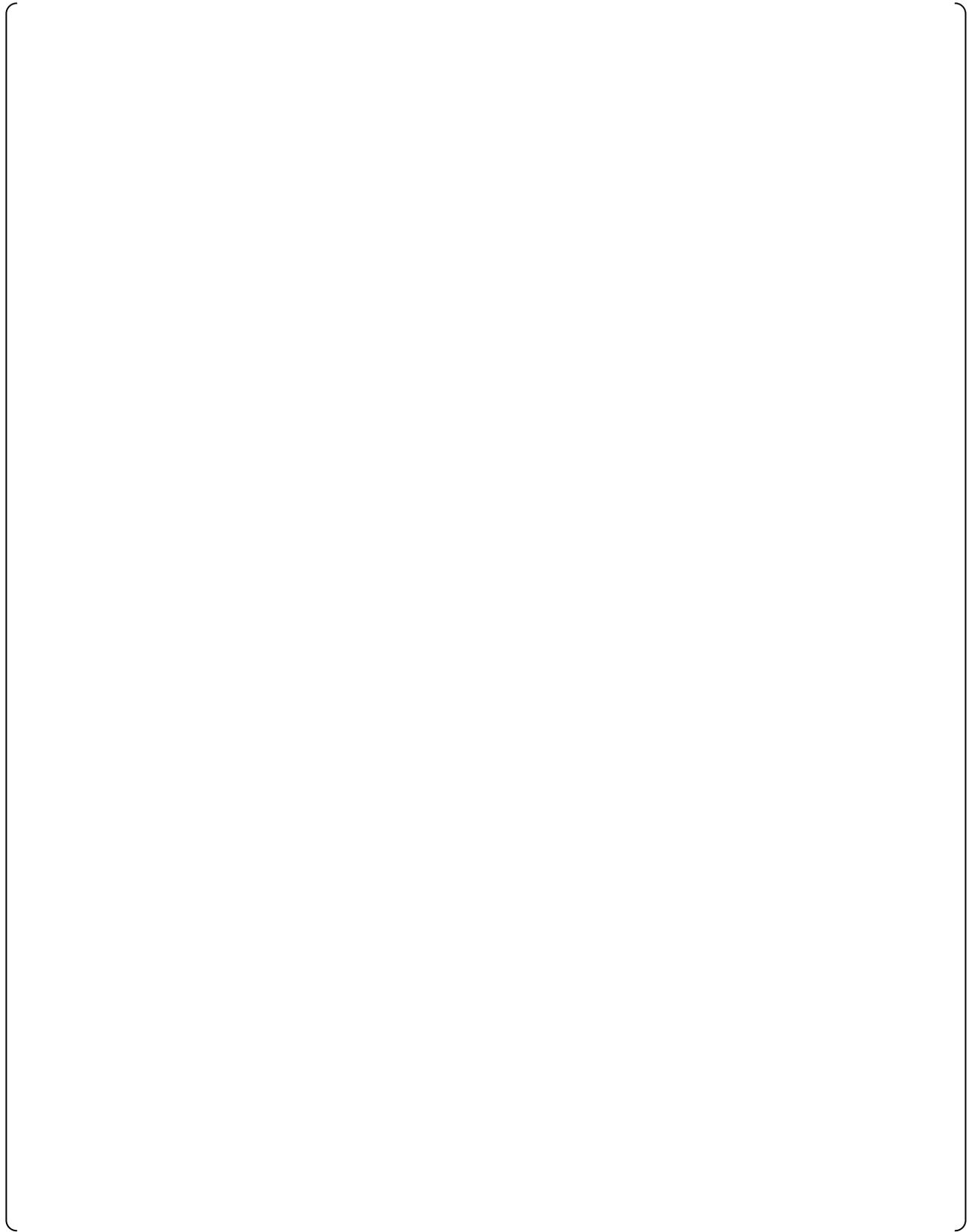
**Table 4-2 Output Documents of Design Team (2/2)**



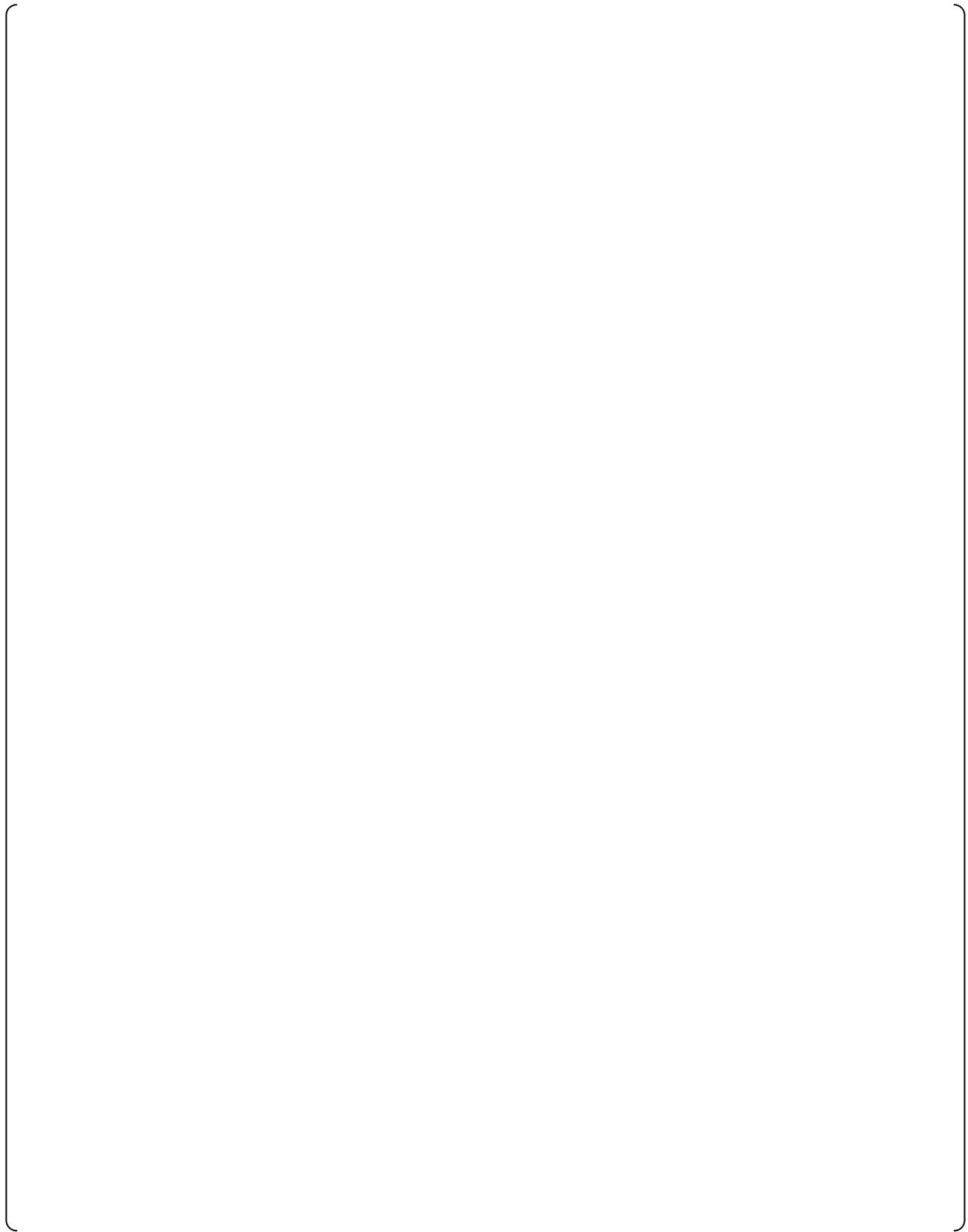
**Table 4-3 Output Documents of V&V Team (1/3)**



**Table 4-3 Output Documents of V&V Team (2/3)**



**Table 4-3 Output Documents of V&V Team (3/3)**



**Table 4-4 Output Documents of QA Department**

A large, empty rectangular frame with rounded corners, intended for the content of Table 4-4. The frame is currently blank.

## 5. REFERENCES

In this section, specific references referred in this SPM are provided.

Other general applicable codes and regulatory guidance are described in US-APWR DCD Chapter 7, MUAP-07004 and MUAP-07005.

1. NUREG-0800, BTP7-14 Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control System", March 2007.
2. Technical Report MUAP-07005 Revision 7, "Safety System Digital Platform – MELTAC –".
3. Technical Report MUAP-07004 Revision 7, "Safety I&C System Description and Design Process".
4. IEEE Std 603-1991, "IEEE Standard Criteria for Safety System for Nuclear Power Generating Stations".
5. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations".
6. IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes".
7. IEEE Std 830-1993, "IEEE Recommended Practice for Software Requirements Specifications".
8. IEEE Std 730-1989, "IEEE Standard for Software Quality Assurance Plans".
9. IEEE Std 1028-1997, "IEEE Standard for Software Reviews and Audits".
10. IEEE Std 1228-1994, "IEEE Standard for Software Safety Plan".
11. IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation".
12. Regulatory Guide 1.169 Revision 0 "Configuration Management Plans for Digital Computer Software Used in Safety System of Nuclear Power Plants", September 1997.
13. IEEE Std 828-1990, "IEEE Standard for Configuration Management Plans".
14. IEEE Std 1042-1987, "IEEE Guide for Software Configuration Management".
15. IEEE Std 829-1983, "IEEE Standard for Software Test Documentation".
16. IEEE Std 1008-1987, "IEEE Standard for Software Unit Testing".
17. Regulatory Guide 1.152 Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants".

18. Regulatory Guide 1.168 Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", February 2004.
19. Regulatory Guide 1.170 Revision 0, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
20. Regulatory Guide 1.171 Revision 0, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
21. Regulatory Guide 1.172 Revision 0, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
22. Regulatory Guide 1.173 Revision 0, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
23. Regulatory Guide 1.169 Revision 0, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", September 1997.
24. Technical Report JEXU-1012-1132 Revision 3, "MELTAC Platform Basic Software Program Manual".
25. IEEE Std 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology".
26. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems", 1993.
27. Topical Report, PQD-HD-19005 Revision 4, "The Quality Assurance Program (QAP) Description for Design Certification of the US-APWR".
28. IEEE Std 1058-1998, "IEEE Standard for Software Project Management Plans".
29. ANSI/ASME NQA-1-1983, "Quality Assurance Program Requirements for Nuclear Facilities".
30. Regulatory Guide 1.153 Revision 1, "Criteria for Safety Systems", June 1996.
31. IEEE/EIA 12207.0-1996, "Industry Implementation of International Standard ISO/IEC 12207:1995".

## Appendix A Definitions

**Acceptable System:**

The system which test phase completed containing both hardware and application software.

**Acceptance Testing [IEEE Std 610.12-1990]:**

Formal testing conducted in an operational environment to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system. Formal testing conducted to enable a user, customer, or other authorized entity to determine whether to accept a system or component.

**Accident:**

An unplanned event or series of events that result in death, injury, illness, environmental damage to or loss of equipment or property.

**Anomaly [IEEE Std 610.12-1990]:**

Any condition that deviates from the expected condition based on requirements, specification, design, documents, user documents standards, or from someone's perceptions or experiences. Anomalies may be found during but are not limited to, the review, test, analysis, compilation, or use of software products or applicable documentation.

**Application Software:**

The application software reflects the plant specific functionality of the Mitsubishi Electric Total Advanced Controller (MELTAC) I&C system. It is documented and generated by the MELTAC engineering tool. The platform system software (i.e., basic software) uses this configuration data to carry out the application specific functionality of the I&C system.

**Application Executable Module:**

The application module installed in hardware generated by the MELTAC engineering tool.

**Application Source Code Listings:**

The list of the application software outputted from the MELTAC engineering tool. Specifically, it is Graphic Block Diagram (GBD) currently written by Problem Oriented Language (POL).

**Audit:**

An independent examination of a software product, software process, or set of software processes to assess compliance with specifications, standards, contractual agreements, or other criteria.

**Baseline [IEEE Std 610.12-1990]:**

A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. Formal review and agreement means that design team management has reviewed and approved a baseline. Baselines are subject to change control.

**Baseline Management [IEEE Std 610.12-1990]:**

In configuration management, the application of technical and administrative direction to designate the documents and changes to those documents that formally identify and establish baselines at specific times during the life cycle of a configuration item.

**Code:**

Computer instructions and data definitions expressed in a programming language or in a form that is outputted by an assembler, compiler, or another translator.

**Component [IEEE Std 610.12-1990]:**

One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components.

**Component Testing [IEEE Std 610.12-1990]:**

Testing of individual hardware or software components or groups of related components

**Configuration [IEEE Std 610.12-1990]:**

The arrangement of a computer system or component as defined by the number, nature, and interconnections of its constituent parts. In configuration management, the functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product.

**Configuration Audit [IEEE Std 610.12-1990]:**

**Functional Configuration Audit (FCA).** An audit conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and functional characteristics specified in the functional or allocated configuration identification, and that its operational and support documents are complete and satisfactory.

**Physical Configuration Audit (PCA).** An audit conducted to verify that a configuration item, as built, conforms to the technical documentation that defines it.

**Configuration Control [IEEE Std 610.12-1990]:**

An element of configuration management, consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.

**Configuration Control Board (CCB) [IEEE Std 610.12-1990]:**

A group of people responsible for evaluating and approving or disapproving proposed changes to configuration items, and for ensuring implementation of approved changes.

**Configuration Identification [IEEE Std 610.12-1990]:**

- (1) An element of configuration management, consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation.
- (2) The current approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and documents referenced therein.

**Configuration Item (CI) [IEEE Std 610.12-1990]:**

An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.

**Configuration Management (CM) [IEEE Std 610.12-1990]:**

A discipline applying technical and administrative direction and surveillance to:

- Identify and document the functional and physical characteristics of a configuration item
- Control changes to those characteristics
- Record and report change processing and implementation status

-Verify compliance with specified requirements

**Configuration Status Accounting [IEEE Std 610.12-1990]:**

An element of configuration management, consisting of the recording and reporting of information needed to manage a configuration effectively. This information includes a listing of the approved configuration identification, the status of proposed changes to the configuration, and the implementation status of approved changes.

**Control Point [IEEE Std 828-1990]:**

It is a point at which controls are to be applied to manage configuration. A project agreed-on point in time or times when specified agreements or controls are applied to the software configuration items being developed, e.g., an approved baseline or release of a specified document/code.

**Criticality:**

A subjective description of the intended use and application of the system. Software criticality properties may include safety, security, complexity, reliability, performance, or other characteristics.

**Criticality Analysis:**

A structured evaluation of the software characteristics (e.g., safety, security, complexity, performance) for severity of impact of system failure, system degradation, or failure to meet software requirements or system objectives.

**Customer:**

The individual or organization that specifies and accepts the project deliverables. The customer may be internal or external to the parent organization of the project, and may or may not be the end user of the software product. A financial transaction between customer and developer is not necessarily implied.

**Design Level [IEEE Std 610.12-1990]:**

The design decomposition of the software item (for example, system, subsystem, program, or module).

**Design Review [IEEE Std 610.12-1990]:**

A process or meeting during which a system, hardware, or software design is presented to project personnel, managers, users, customers, or other interested parties for comment or approval. Types include critical design review, preliminary.

**Engineering Tool:**

The MELTAC platform engineering tool provides various functions aimed at more stable and more efficient software management during all system life cycle phases (including design, fabrication, test, adjustment and maintenance). (Refer to MUAP-07005)

**External Consistency:**

A state in which there is consistency in external attributes. An external attribute is an attribute that can be identified as the behavior of a system when the software is executed as a system and is measured by executing the software. An example of an external attribute is a measured response time.

**Factory Acceptance Testing [IEEE Std 1012-1998]:**

Testing conducted in a factory environment to determine whether a system satisfies its acceptance criteria (i.e., initial requirements and current needs of its user) and to enable the customer to determine whether to accept the system.

**Field Programmable Gate Array (FPGA):**

An **FPGA** is an integrated circuit designed to be configured by the customer or designer after manufacturing—hence "field-programmable". An FPGA typically has multiple internal logical blocks consisting of logic gates and arithmetic circuits. Internal logical blocks are located on a matrix. A required circuit configuration can be realized by connecting these internal logical blocks in a manner suitable for a functional application.

**Firmware:**

Computer programs and data loaded in a class of memory that cannot be dynamically modified by the computer during processing.

**Flash Read Only Memory (F-ROM):**

One of the nonvolatile semiconductor memories where data does not disappear after powering off.

**Functional Testing [IEEE Std 610.12-1990]:**

Testing that ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions. Testing conducted to evaluate the compliance of a system or component with specified functional requirements.

**Hazard:**

A source of potential harm or a situation with a potential for harm in terms of human injury, damage to health, property, or the environment, or some combination of these.

**Hazard Identification:**

A systematic qualitative or quantitative evaluation of software for undesirable outcomes resulting from the development or operation of a system. These outcomes may include injury, illness, death, mission failure, economic loss, property loss, environmental loss, or adverse social impact. This evaluation may include screening or analysis methods to categorize, eliminate, reduce, or mitigate hazards.

**Independent Verification and Validation (IV&V) [IEEE Std 610.12-1990]:**

V&V processes performed by an organization with a specified degree of technical, managerial, and financial independence from the development organization.

**Inspection:**

A visual examination of a software product to detect and identify software anomalies, including errors and deviations from standards and specifications. Inspections are peer examinations led by impartial facilitators who are trained in inspection techniques. Determination of remedial or investigative action for an anomaly is a mandatory element of a software inspection, although the solution should not be determined in the inspection meeting.

**Installation Configuration Listings:**

Listing that includes all of the functional characteristics of the software application. This is equivalent to the "Installation Configuration Table" referenced in NUREG 0800, Branch Technical Position, BTP 7-14.

**Installed System:**

The system which the installation phase completed used for an operation system.

**Integration Testing [IEEE Std 610.12-1990]:**

Testing in which software components, hardware components, or both are combined and tested to demonstrate correct interaction between them.

**Integrity Level:**

A denotation of a range of values of a property of an item necessary to maintain system risks within acceptable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.

**Integrated System:**

A system where the application software is installed in the hardware and the implementation phase is completed.

**Interface [IEEE Std 610.12-1990]:**

A shared boundary across which information is passed. This boundary includes design interfaces between design organizations (as interpreted by RG 1.168). A hardware or software component that connects two or more other components for the purpose of passing information from one to the other. To connect two or more components for the purpose of passing information from one to the other. To serve as a connecting or connected component as in 2 above.

**Interface Control [IEEE Std 610.12-1990]:**

- (1) In configuration management, the process of:
  - (a) identifying all functional and physical characteristics relevant to the interfacing of two or more configuration items provided by one or more organizations, and (b) ensuring that proposed changes to these characteristics are evaluated and approved prior to implementation.
- (2) In configuration management, the administrative and technical procedures and documentation necessary to identify functional and physical characteristics between and within configuration items provided by different developers, and to resolve problems concerning the specified interfaces

**Interface Design Document (IDD):**

Documentation that describes the architecture and design of interfaces between system and components. These descriptions include control algorithms, protocols, data contents and formats, and performance.

**Interface Requirements Specification (IRS):**

Documentation that specifies requirements for interfaces between systems or components. These requirements include constraints on formats and timing.

**Internal Consistency:**

A state in which there is consistency in internal attributes. An internal attribute is an attribute that can be identified by each software product and can be measured without executing the software. An example of an internal attribute is the consistency of the description of specifications and an execution module.

**Life Cycle Process:**

A set of interrelated activities that result in the development or assessment of software products. Each activity consists of tasks. The life cycle processes may overlap one another. For V&V purposes, no process is concluded until its development products are verified and validated according to the defined tasks in the Software Verification & Validation Plan (SVVP).

**Maintenance [IEEE Std 610.12-1990]:**

The process of modifying a software system or component after delivery to correct faults, improve performance (or other attributes), or adapt to a changed environment. The process of retaining or restoring a hardware system or component in a state in which it can perform its required functions.

**Management Review:**

A systematic evaluation of a software acquisition, supply, development, operation, or maintenance process performed by or on behalf of management that monitors progress, determines the status of plans and schedules, confirms requirements and their system allocation, or evaluates the effectiveness of management approaches used to achieve fitness for purpose.

**MELTAC Platform Basic Software:**

The MELTAC basic software is the low-level software that operates the MELTAC controllers. This software consists of initialization code, device drivers, communication layers, function blocks, diagnostics, etc. for the MELTAC platform.

**Metric [IEEE Std 610.12-1990]:**

A quantitative measure of the degree to which a system, component, or process possesses a given attribute.

**Minimum Tasks:**

Those V&V tasks required for the software integrity level assigned to the software to be verified and validated.

**Mitsubishi Electric Total Advanced Controller (MELTAC):**

A safety system digital platform for nuclear power plants.

**Operation and Maintenance Phase [IEEE Std 610.12-1990]:**

The period of the time in the software life cycle during which a software product is employed in its operational environment, monitored for satisfactory performance, and modified as necessary to correct problems or to respond to changing requirements.

**Optional Tasks:**

Those V&V tasks that may be added to the minimum V&V tasks to address specific application requirements.

**Pass/fail Criteria:**

Decision rules used to determine whether a software item or a software feature passes or fails a test.

**Protection and Safety Monitoring System (PSMS):**

The PSMS consists of safety-related digital control system and safety-related Human System Interface System (HSIS).

**Plant Control and Monitoring System (PCMS):**

The PCMS consists of non-safety digital control system and non-safety Human System Interface System (HSIS).

**Plant Requirements Phase:**

This phase is a concept phase defined by IEEE Std 1012-1998, and contains DCD for US-APWR and COL.

**Problem Oriented Language (POL):**

Application software is described in a graphically symbolized manner, using the problem oriented language (POL), so that functions can be easily understood.

**Project Agreement:**

A document or set of documents agreed to by the designated authority for the project and the customer. Documents in a project agreement may include some or all of the following: a contract, a statement of work, system engineering specifications, user requirement specifications, functional specifications, the software project management plan, a business plan, or a project charter.

**Project Deliverables:**

The work product(s) to be delivered to the customer. The quantities, delivery dates, and delivery locations are specified in the project agreement.

**Project Function:**

An activity that spans the entire duration of a software project. Examples of project functions include project management, configuration management, quality assurance, and verification and validation.

**Promotion:**

To indicate a transition in the level of authority needed to approve changes to a controlled entity, such as a baseline configuration item.

**Release:**

The formal notification and distribution of an approved version.

**Required Inputs:**

The set of items necessary to perform the minimum V&V tasks mandated within any life cycle activity.

**Required Output:**

The set of items produced as a result of performing the minimum V&V tasks mandated within any life cycle activity.

**Requirement Traceability Matrix (RTM) [IEEE Std 610.12-1990]**

A matrix that records the relationship between two or more products of the development process; for example, a matrix that records the relationship between the requirements and the design of a given software component.

**Review:**

A process or meeting during which a software product is presented to project personnel, managers, users, customers, user representatives, or other interested parties for comment or approval.

**Risk:**

A measure that combines both the likelihood that a software hazard will cause some problem and the severity of that problem.

**Risk Analysis:**

The systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment.

**Self-diagnosis:**

The integrity of digital I&C components is continuously checked by their self-diagnosis features. These self-diagnostic features result in early detection of failures.

**Software [IEEE Std 610.12-1990]:**

Computer programs, procedures, and in some cases, associated documentation and data pertaining to the operation of a computer system.

**Software Design Description (SDD) [IEEE Std 610.12-1990]:**

A representation of software created to facilitate analysis, planning, implementation, and decision making. The software design description is used as a medium for communicating software design information, and may be thought of as a blueprint model of the system.

**Software Failure:**

A distinguishing characteristic of a software item (for example, performance, portability, or functionality).

**Software Hazard [Based on IEEE Std 610.12-1990]:**

A software error that could result in failure of functions or unintended operation including abnormal events, conditions and malicious modifications.

**Software Integrity Level (SIL):**

The integrity level of a software item.

**Software Item:**

Source code, object code, job control code, control data, or a collection of these items.

**Software Library [IEEE Std 610.12-1990]:**

A controlled collection of software and related documentation designed to aid in software development, use, or maintenance. Types include master library, production library, software development library, software repository, and system library.

**Software Life Cycle [IEEE Std 610.12-1990]:**

The period of time that begins when a software product is conceived and ends when the software is no longer available for use.

**Software Product:**

A set of computer programs, procedures, related documents, and data.

**Software Project:**

The set of all project functions, activities, and tasks, both technical and managerial, required to satisfy the terms and conditions of the project agreement. A software project may be self-contained or may be part of a larger project. A software project may span only a portion of the software product lifecycle.

**Software Project Management:**

The process of planning, organizing, staffing, monitoring, controlling, and leading a software project.

**Software Project Management Plan (SPMP):**

The controlling document for managing a software project. A software project management plan defines the technical and managerial project functions, activities, and tasks necessary to satisfy the requirements of a software project, as defined in the project agreement.

**Software Quality Metric:**

A function whose inputs are software data and whose output is a single numerical value that can be interpreted as the degree to which software possesses a given attribute that affects its quality.

**Software Risk [Based on IEEE Std 1228-1994]:**

A measure that combines both the likelihood that a software hazard will cause some problem and the severity of that problem.

**Software Verification & Validation Plan (SVVP):**

A plan describing the conduct of software V&V.

**Software Verification & Validation Report:**

Documentation of V&V results and software quality assessments.

**Specification [IEEE Std 610.12-1990]:**

A document that specifies, in a complete, precise, verifiable manner, the requirement, design, behavior, or other characteristics of a system or component, and often, the procedure for determining whether these provisions have been satisfied.

**System:**

A combination of more than one process, hardware, software, equipment, and humans, designed to provide the ability to meet specific requirements.

**System Design Description (SysDD):**

Documents which are SDD and IDD Which are defined by IEEE Std 1012-1998, and outputted from design phase.

**System Requirements Specification (SysRS):**

Documents which correspond to SRS and IRS which are defined by IEEE Std 1012-1998, and outputted from design phase.

**System Software [IEEE Std 610.12-1990]:**

Software designed to facilitate the operation and maintenance of a computer system and its associated application programs; for example, operating systems, assemblers, utilities.

**System Testing:**

The activities of testing an integrated hardware and software system to verify and validate whether the system meets its original objectives.

**Task:**

The smallest unit of work subject to management accountability. A task is a well-defined work assignment for one or more project members. The specification of work to be accomplished in completing a task is documented in a work package. Related tasks are usually grouped to form activities.

**Technical Review:**

A systematic evaluation of a software product by a team of qualified personnel that examines the suitability of the software product for its intended use and identifies discrepancies from specifications and standards. Technical reviews may also provide recommendations of alternatives and examination of various alternatives.

**Test:**

- (1) A set of one or more test cases, or
- (2) A set of one or more test procedures, or
- (3) A set of one or more test cases and procedures.

**Test Case:**

Documentation that specifies inputs, predicted results, and a set of execution conditions for a test item.

**Test Case Specification:**

A document specifying inputs, predicted results, and a set of execution conditions for a test item.

**Test Design [IEEE Std 610.12-1990]:**

Documentation that specifies the details of the test approach for a software feature or combination of software features and identifying the associated tests.

**Test Design Specification:**

A document specifying the details of the test approach for a software feature or combination of software features and identifying the associated tests.

**Test Incident Report:**

A document reporting on any event that occurs during the testing process which requires investigation.

**Test Item:**

A software item which is an object of testing.

**Test Item Transmittal Report:**

A document identifying test items. It contains current status and location information.

**Test Log:**

A chronological record of relevant details about the execution of tests.

**Test Phase [IEEE Std 610.12-1990]:**

The period of time in the software life cycle after which the components of a software product are integrated, whereby the software product is evaluated to determine whether or not its specified requirements have been satisfied.

**Test Plan [IEEE Std 610.12-1990]:**

A document describing the scope, approach, resources, and schedule of intended test activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks may require contingency planning.

**Test Procedure:**

Documentation that specifies a sequence of actions for the execution of a test.

**Test Procedure Specification:**

A document specifying a sequence of actions for the execution of a test.

**Test Report [IEEE Std 610.12-1990]:**

A document that describes the conduct and results of the testing carried out for a system or component.

**Test Summary Report:**

A document summarizing testing activities and results. It also contains an evaluation of the corresponding test items.

**Test Unit [IEEE Std 610.12-1990]:**

A set of one or more computer program modules together with associated control data, (for example, tables), usage procedures, and operating procedures that satisfy the following conditions:

All modules are from a single computer program

At least one of the new or changed modules in the set has not completed the unit test

The set of modules together with its associated data and procedures are the sole object of a testing process

**Testability:**

The ability of a software product to allow its functional and performance features to be determined.

**Testing:**

The process of analyzing a software item to detect the differences between existing and required conditions (that is, bugs) and to evaluate the features of the software item.

**Traceability Matrix [IEEE Std 610.12-1990]:**

A matrix that records the relationship of verifiable characteristics between two or more products of the development process.

**Transaction:**

A unit of a set of inseparable information processing tasks. Execution of a typical transaction involves a user interface, an application program, a persistent memory resource, and various I/O operations.

**Unit [IEEE Std 610.12-1990]:**

A separately testable element specified in the design of a computer software component. A logically separable part of a computer program. A software component that is not subdivided into other components.

**Unit Testing [IEEE Std 610.12-1990]:**

Testing of individual hardware or software units or groups of related units.

**Validation [IEEE Std 610.12-1990]:**

The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

**Verification [IEEE Std 610.12-1990]:**

The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. Contrast with: validation.

**Verification and Validation (V&V) [IEEE Std 610.12-1990]:**

The process of determining 1) whether the requirements for a system or component are complete and correct, 2) whether the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and 3) whether the final system or component complies with specified requirements.

**Version [IEEE Std 610.12-1990]:**

An initial release or re-release of a computer software configuration item that is associated with a complete compilation or recompilation of the computer software configuration item. The baseline should be the target for review and if it should be revised, the revised new documents or software configuration items should be numbered to be identified as new one.

**Walk-through [IEEE Std 610.12-1990]:**

A static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a software product, and the participants ask questions and make comments about possible errors, violation of development standards, and other problems.

**Work Package:**

A specification for the work to be accomplished in completing an activity or task. A work package defines the work product(s), the staffing requirements, the expected duration, the resources to be used, the acceptance criteria for the work products, the name of the responsible individual, and any special considerations for the work.

**Work Product:**

Any tangible item that results from a project function, activity, or task. Examples of work products include customer requirements, project plan, functional specifications, design documents, source and object code, users' manuals, installation instructions, test plans, maintenance procedures, meeting minutes, schedules, budgets, and problem reports. Some subset of the work products will form the set of project deliverables.

## Appendix B Deleted

This Appendix is intentionally left blank.

## Appendix C Software Secure Development and Operational Environment Features

### 1. Introduction

This Appendix C describes conformance of the design, production and maintenance of the PSMS application software to the secure development and operational environment requirements of RG 1.152, Rev.3.

The PSMS provides many design features and defensive strategies to addressing the issue of application software secure development and operational environment design features as described in this Technical Report, MUAP-07017 "US-APWR Software Program Manual", and the following related documents;

- a. Design Control Document (DCD) for the US-APWR Section 7.9
- b. Safety I&C System Description and Design Process, MUAP-07004
- c. Safety System Digital Platform -MELTAC-, MUAP-07005
- d. MELTAC Platform Basic Software Program Manual, JEXU-1012-1132

The secure development and operational environment for the design, production and maintenance of the PSMS application software is described in this Technical Report, MUAP-07017 "US-APWR Software Program Manual".

The MELTAC digital platform is applied to the PSMS. Technical Report, JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual" describes compliance to the secure development and operational environment requirements of RG 1.152, Rev. 2 for future changes to the basic software.

### 2. Conformance to RG 1.152 Rev.3

This Appendix C describes conformance of the secure development and operational environment for the design, production and maintenance of the PSMS application software to the requirements of RG 1.152, Rev. 3. The section numbers follow the sections in RG 1.152, rev.3. This conformance description excludes PSMS application software life cycle process phases for Section 2.6 "Installation, Checkout, and Acceptance Testing", Section 2.7 "Operations Phase", Section 2.8 "Maintenance Phase", and Section 2.9 "Retirement Phase". Security features for these life cycle process phases are addressed in other regulatory guidance, such as RG 5.71 "Cyber Security Programs for Nuclear Facilities". Therefore addressing compliance to security related regulatory criteria for these life cycle process phases is outside the scope of this Appendix C.

#### C.2.1 Concepts Phase

##### Staff Position 1

Requirement
In the concepts phase, the licensee and developer should identify digital safety system design features that should be implemented to establish a secure operational environment for the system. A licensee should describe these design features as part of its application.
Analysis
Security Related and Proprietary Information - Withheld Under 10CFR2.390

<div style="border: 1px solid black; padding: 5px; display: inline-block;">                 Security Related and Proprietary Information - Withheld Under 10CFR2.390             </div>
<b>Evaluation</b>
Compliance

**Staff Position 2**

<b>Requirement</b>
The licensee and developer should perform an assessment to identify the digital safety system’s potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system’s lifecycle that could degrade the system’s reliable operation. This assessment should identify the potential challenges to maintain a secure operational environment for the digital safety system and the challenges to maintaining a secure development environment for the system’s development lifecycle phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures that are required to maintain a secure development environment.
<b>Analysis</b>
<div style="border: 1px solid black; padding: 5px; display: inline-block;">                 Security Related and Proprietary Information - Withheld Under 10CFR2.390             </div>
<b>Evaluation</b>
Compliance

**Staff Position 3****Requirement**

The licensee should not implement remote access to the safety system. For the purpose of this guidance, remote access is defined to be the ability to access a computer, node, or network resource that performs a safety function or that can impact the safety function from a computer or node that is located in an area with less physical security (e.g., outside the protected area) than the safety system.

Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

**Evaluation**

Compliance

**C.2.2 Requirements Phase****C.2.2.1 System Features****Staff Position 1****Requirement**

The licensees and developers should define the secure operational environment functional performance requirements and system configuration; interfaces external to the systems; and the requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Security Related and Proprietary Information - Withheld Under 10CFR2.390

**Evaluation**

Compliance

**Staff Position 2****Requirement**

The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification and validation process of the overall system should ensure the correctness, completeness, accuracy, testability, and consistency of the system secure operational environment design feature requirements.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

**Evaluation**

Compliance

**Staff Position 3****Requirement**

Requirements specifying the use of predeveloped software and systems (e.g., reused software and commercial off-the-shelf (COT) systems) should address the reliability of the safety system (e.g., by using predeveloped software functions that have been tested and are supported by operating experience).

<b>Analysis</b>
Security Related and Proprietary Information - Withheld Under 10CFR2.390
<b>Evaluation</b>
Compliance

**C.2.2.2 Development Activities**

<b>Requirement</b>
During the development of requirements, measures should be taken to ensure that the requirements development process and documentation are secure such that the system does not contain undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system.
<b>Analysis</b>
Security Related and Proprietary Information - Withheld Under 10CFR2.390
<b>Evaluation</b>
Compliance

**C.2.3 Design Phase**

**C.2.3.1 System Features**

**Staff Position 1**

<b>Requirement</b>
The safety system secure operational environment design features identified in the system requirements specification should be translated into specific design configuration items in the system design description.
The safety system secure operational environment design configuration items intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate predeveloped software into the safety system should address how the predeveloped software will not challenge the secure operational environment for the safety system.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

**Evaluation**

Compliance

**Staff Position 2**

**Requirement**

Physical and logical access control should be based on the results of the assessment

performed in the concepts phase of the lifecycle. The results of this assessment may identify the need for more complex access control measures, such as combination of knowledge (e.g., password), property (e.g., key and smart-card), or personal features (e.g., fingerprints), rather than just a password.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

**Evaluation**

Compliance

**C.2.3.2 Development Activities**

**Requirement**

The development should delineate the standards and procedures that will confirm with the applicable design controls to ensure that the system design products (hardware and software) do not contain undocumented code (e.g., back door coding), unwanted functions or applications, and any other coding that could adversely impact the reliable operation of the digital safety system.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

<div style="border: 1px solid black; padding: 5px; display: inline-block;">                 Security Related and Proprietary Information - Withheld Under 10CFR2.390             </div>
<b>Evaluation</b> Compliance

**C.2.4 Implementation Phase**

**C.2.4.1 System Features**

<b>Requirement</b> The developer should ensure that the transformation of the secure operational environment design configuration items from the system design specification is correct, accurate, and complete.
<b>Analysis</b> <div style="text-align: center; vertical-align: middle;"> <div style="border: 1px solid black; padding: 5px; display: inline-block;">                     Security Related and Proprietary Information - Withheld Under 10CFR2.390                 </div> </div>
<b>Evaluation</b> Compliance

**C.2.4.3 Development Activities**

**Staff Position 1**

<b>Requirement</b> The developer should implement secure operational environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alternations of the development system. The developer's standards and procedures should include testing, (such as scanning), as appropriate, to address undocumented code or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner.
---

The developer should account for hidden functions and vulnerable features embedded in the code, and their purpose and impact on the integrity and reliability of the safety system. These functions should be removed, or (as a minimum) addressed (e.g., as part of the failure modes and affects analysis of the application code) to prevent any unauthorized access or impact the reliability of the safety system.

#### Analysis

Security Related and Proprietary Information - Withheld Under 10CFR2.390

#### Evaluation

Compliance

### Staff Position 2

#### Requirement

COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for use in determining the complete set of system behavior inherent in a given operating system (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify such systems, the development activity should ensure that the features within the operating system do not compromise the required secure operational environment design features of the system in such each a manner that reliability of the digital safety system would be degraded.

#### Analysis

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Security Related and Proprietary Information - Withheld Under 10CFR2.390
--

**Evaluation**

N/A

**C.2.5 Test Phase****C.2.5.1 System Features****Requirement**

The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items. Therefore, secure operational environment design configuration items are just one element of the overall system validation. Each system secure operational environment design features should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access and/or the efforts of undesirable behavior of connected systems and does not degraded the safety system's reliability.

**Analysis**

Security Related and Proprietary Information - Withheld Under 10CFR2.390
--



- a. Design Control Document (DCD) for the US-APWR Section 7.9
- b. Safety I&C System Description and Design Process, MUAP-07004
- c. Safety System Digital Platform -MELTAC-, MUAP-07005
- d. MELTAC Platform Basic Software Program Manual, JEXU-1012-1132

The secure operational environment design for the PSMS application software for installation, checkout and acceptance testing, operation, maintenance, and retirement life cycle phases are outside the scope of this SPM.

**3. Secure Development and Operational Environment Assessment for Potential Unauthorized Changes of PSMS Application Software**

Left without a secure development and operational environment, the PSMS application software may be incorrectly changed by unauthorized activities of a user or developer. The potential unauthorized activities of the PSMS application software development, from the System Requirements Phase through the Test Phase, are as follows;

Security Related and Proprietary Information - Withheld Under 10CFR2.390

The following generic defenses against undesired PSMS application software changes is performed throughout each phase of the PSMS application software life cycle process as discussed in Section 3.1.4 of this SPM:

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Security Related and Proprietary Information - Withheld Under 10CFR2.390

In addition to the general secure development and operational environment design defenses described above, additional the secure development and operational environment measures for specific life cycle process of the PSMS application software are described below.

### 3.1 Defense against Unauthorized Changes in Requirements Phase

Security Related and Proprietary Information - Withheld Under 10CFR2.390

The SysRS and related documents are checked by the VVT which is specified by this SPM. Therefore, the insertion of undesired requirements that introduce the secure development and operational environment vulnerabilities would be detected and corrected. The VVT review assures that the PSMS application software secure development and operational environment requirements are correctly included and unauthorized functionality is not included. The VVT participants, review scope, and review findings are documented as required by the SVVP in Section 3.10 which are specified by this SPM. The SysRS for the PSMS application software

and related documents are versioned and released as required by the Software Configuration Management Plan (SCMP) which are specified by Section 3.11 of this SPM.

The secure development and operational environment measures that ensure the System Requirements Phase output products are protected from unauthorized alteration after the IV&V and final approval are described in the following Table 3.1.

**Table 3.1: Secure Development and Operational environment Measures of the Requirements Phase Software and Documents Development/Storage Environment**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

The secure development and operational environment design assessment conducted through the IV&V of the System Requirements Phase output products, confirms the System Requirement Phase output products adequately reflect the secure development and operational environment design features of the Plant Requirements Phase, and that no unintended functions have been added.

**3.2 Defense against Unauthorized Changes in Design Phase**

The SysDD is developed during this phase, in accordance with the SDP and SSP, based on the SysRS which is output of the System Requirements Phase, and provides the necessary system, functional requirements, detail functions and logics, software specifications and hardware specifications and software and hardware interface requirements.

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Multiple SysDD are prepared for the various functions of the PSMS (e.g., RPS, ESFAS, SLS, etc.). When each SysDD is completed by the DT, the VVT, as indicated in Section 2.2 of this SPM, shall verify each SysDD. The VVT review shall ensure that all PSMS application software requirements identified in the SysRS are properly reflected in the SysDD. In addition, the VVT shall ensure there are no additional functions that are not traceable to the SysRS. Verification of the SysDD shall be performed in accordance with Section 3.10 of this SPM.

The SysDD and related documents are checked by the VVT which is specified by this SPM. Therefore, the insertion of undesired designs introducing the secure development and operational environment vulnerabilities would be detected and corrected. The VVT review assures that the secure development and operational environment requirements are correctly included and unauthorized functionality is not included. The IV&V review assures that the functionality specified by the SysRS and related documents are included and built into the SysDD and related documents. The VVT participants, review scope, and review findings are documented as required by the SVVP which are specified by this SPM. The SysDD and related documents are versioned and released as required by the SCMP which are specified by Section 3.11 of this SPM.

The secure development and operational environment measures that ensure the Design Phase output products are protected from unauthorized alteration after the IV&V and final approval are described in Table 3.1 and 3.3.

The secure development and operational environment design assessment conducted through the IV&V of the Design Phase output products, confirms the Design Phase output products adequately reflect the secure development and operational environment design features of the System Requirements Phase and that no unintended functions have been added.

### 3.3 Defense against Unauthorized Changes in Implementation Phase

The PSMS application software is implemented on each target safety system in the PSMS hardware during this phase, in accordance with the SDP and SSP. Input from the SysRS and the SysDD provides the necessary information to implement the PSMS application software.

The DT shall be responsible for developing, maintaining and updating the PSMS application software, in accordance with the design documented in the SysRS and the SysDD, and design process defined in this SPM.

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Software units generated during this phase are tested by the VVT in accordance with the STP and the SVVP which are specified in Sections 3.12 and 3.10 of this SPM, respectively.

The PSMS application software is checked by the VVT which is specified by this SPM. Therefore, the insertion of undesired designs introducing secure development and operational environment vulnerabilities would be detected and corrected. The VVT review assures that the secure development and operational environment requirements are correctly included and unauthorized functionality is not included. The VV review assures that the functionality specified by the SysDD and related documents are included and built into the application software documents. The VVT participants, review scope, and review findings are documented as required by the SVVP which are specified by this SPM. The PSMS application software is versioned and released as required by the SCMP which are specified by Section 3.11 of this SPM.

Security Related and Proprietary Information - Withheld Under 10CFR2.390

**Table 3.3: Secure Development and Operational Environment Measures of the Post-Design Phase Software Development/Storage Environment**

Security Related and Proprietary Information - Withheld Under 10CFR2.390

The VVT participants, review scope, and review findings are documented as required and specified by the SVVP in Section 3.10 of this SPM. The PSMS application software and related documents are versioned and released as required by the SCMP which are specified by Section 3.11 of this SPM.

Security Related and Proprietary Information - Withheld Under 10CFR2.390

The integration personnel shall confirm the following points to evaluate the integration results;

Security Related and Proprietary Information - Withheld Under 10CFR2.390

The secure development and operational environment design assessment conducted through IV&V of the Implementation Phase output products, confirms the Implementation Phase output products adequately reflect the secure development and operational environment design features of the Design Phase, and that not unintended functions have been added.

### 3.4 Defense against Unauthorized Changes in Test Phase

Test reports contain a summary of the test results and attachments with all detailed results, and the configuration of the test environment. Unauthorized changes of test results, or not reporting adverse findings documented in the test logs, are excluded by reviews performed by the VVT in accordance with the SVVP in Section 3.10 of this SPM.

Security Related and Proprietary Information - Withheld Under 10CFR2.390

### 3.5 PSMS Design Features to Minimize Application Software Secure Development and Operational Environment Vulnerabilities

The PSMS has multiple defensive layers and secure development and operational environment features to minimize the potential for unauthorized changes of the PSMS application software and thereby protect the system from secure development and operational environment vulnerabilities.

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Security Related and Proprietary Information - Withheld Under 10CFR2.390

Security Related and Proprietary Information - Withheld Under 10CFR2.390

#### 4. Conclusion

The PSMS application software exhibits different degrees of susceptibility to unauthorized changes by a user or developer at different phases of the PSMS application software life cycle process. The analysis in the previous sections addressed life cycle phases, from the System Requirements Phase to the Test Phase, to a detail commensurate with the potential for unauthorized changes by a user or developer, and to a level of detail appropriate for the each life cycle phase. The measures imposed by the PSMS engineering procedures assure that all countermeasures against unauthorized changes at any time in the PSMS application software development life cycle are adequately addressed.

The secure development and operational environment design assessments conducted through IV&V for each subsequent PSMS application software life cycle process confirm that the secure development and operational environment related design features are progressing through the development process, in accordance with this SPM. In addition, these secure development and operational environment design assessments ensure unintended functions have not been introduced at any point in the PSMS application software life cycle process.

---

## Appendix D Software Program Manual for Augmented Quality Systems

### 1. Scope

The basic and application software of the PSMS is classified as Class 1E as defined in IEEE Std 603-1991, and the basic and application software is classified as software integrity level 4 in accordance with Chapter 1 of RG 1.168 Rev. 1. The PSMS application software complies with this US-APWR Software Program Manual.

The Plant Control and Monitoring System (PCMS) is classified as a non-safety related system, but several subsystems and components in the PCMS have specific regulatory requirements. Therefore, these PCMS subsystems and components are classified as augmented quality. The System Quality Group Classifications are described in DCD Section 3 "Design of Structures, Systems, Components, and Equipment." The PCMS subsystems and components classified as augmented quality are categorized as Equipment Class 5, whereby they must meet selected QA requirements of 10 CFR 50 Appendix B as described in Section 3.2.2.5 of the DCD.

The equipment classes of all systems are listed in Table 3.2-2 of DCD Chapter 3, and the systems which are categorized as Equipment Class 5 require the augmented quality classification. The actual scopes of the augmented quality systems and the applied regulatory requirements for each system are described in Table 7.1.5 of DCD Chapter 7.

### 2. Software Life Cycle Requirements

The software life cycle processes of the PCMS application software selected for the augmented quality systems are listed in Table D-1.

#### 2.1 Basic Software

For the hardware and basic software of the augmented quality PCMS subsystems and components, the pertinent QA requirements of 10 CFR 50, Appendix B as described in Section 3.2.2.5 of the DCD are required in the same manner as other Equipment Class 5 SSCs, such as structures, structural components, non digital I&C and electrical components.

The augmented quality program for the selected PCMS subsystem and component application software, which includes integration and final validation testing, encompasses the basic software and hardware. Therefore a unique basic software and hardware augmented quality program is not required.

#### 2.2 Application Software

For the application software of the augmented quality PCMS subsystems and components, the software life cycle control requirements which are specified by this US-APWR Software Program Manual are applied as described in Table D-1.

**Table D-1: Applicability of US-APWR SPM to Application Software of PCMS functions with augmented quality**

Software Plans	Applicability
Software Management Plan (SMP)	A
Software Development Plan (SDP)	A
Software Quality Assurance Plan (SQAP)	N/A <sup>(1)</sup>
Software Integration Plan (SIntP)	A
Software Installation Plan (SInstP)	A
Software Maintenance Plan (SMaintP)	A
Software Training Plan (STrngP)	A
Software Operations Plan (SOP)	A
Software Safety Plan (SSP)	N/A
Software Verification and Validation Plan (SVVP)	A <sup>(2)</sup>
Software Configuration Management Plan (SCMP)	A
Software Test Plan (STP)	A
Output Documents	A <sup>(3)</sup>
Appendix C	A

Note: A-applicable N/A-not applicable

- (1) Based on QA requirements for Equipment Class 5 Systems in Section 3.2.2.5 of the DCD.
- (2) All V&V activities are conducted. However activities may be conducted by the Design Team or the V&V Team, and V&V independence is not required.
- (3) Documents provided by VVT are not applicable.