Enclosure 3

UAP-HF-13243
Docket No. 52-021

Response to US-APWR DCD RAI No. 993-7027
(SRP 07-14 Branch Technical Position)

October 2013

(Non-Proprietary)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

10/9/2013

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**No.993-7027 Revision 0**
SRP SECTION:	**07-14 Branch Technical Position – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**07.01 – Instrumentation and Controls – Introduction** **07.09 – Data Communication Systems**
DATE OF RAI ISSUE:	**2/15/2013**

QUESTION NO. : 07-56

IEEE Std. 603-1991, Clause 5.3, Quality, states in part that "Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program." With respect to software quality, Regulatory Guide 1.152, Revision 3, Regulatory Position C.1, states that "Conformance with the requirements of IEEE Std. 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants."

The staff has questions with the US-APWR software development process conforming to the software quality guidance in Clause 5.3 of IEEE Std. 7-4.3.2-2003. The development for all safety software, such as the application software, basic software, and firmware, should contain similar life cycle development activities necessary to generate safety grade software (e.g., independent verification and validation, hazard analysis, requirements traceability, etc.). Despite the fact that the basic software has already been developed, important technical aspects of the processes used for its development are to be captured in the licensing basis documents (DCD or MHI TRs). The technical report (MUAP-07005-P, revision 8), *Safety System Digital Platform - MELTAC*, describes the basic software development process but it is not clear to the staff how MHI ensures that its vendor's safety software development process and the resulting software conforms to NRC regulation and guidance. The staff requests that MHI explain or describe its process to address this, and that there is an ITAAC to verify such process which should include the testing/demonstration of the required features of the safety software as well as independent verification and validation.

ANSWER:

As described in the US-APWR Software Program Manual (SPM) (MUAP-07017), the

Protection and Safety Monitoring System (PSMS) consists of application software and the MELTAC platform, which includes hardware and basic software. The US-APWR SPM describes the software quality assurance requirements for the PSMS.

MHI has already confirmed that the MELTAC basic software conforms to NRC regulations and guidance. This was done through MHI's assessment of MELCO's 10CFR50 Appendix B quality program. MHI will ensure MELCO maintains the current MELTAC software in accordance with the life cycle of their 10CFR50 Appendix B quality program. MHI will also ensure that MELCO develops any new software in accordance with the development commitments of their 10CFR50 Appendix B quality program. MHI's process to ensure MELCO adheres to these life cycle commitments is defined in the US-APWR SPM.

Testing/demonstration and independent V&V for MELTAC basic software will not be required to be conducted by MHI because these activities are conducted by MELCO in accordance with the "MELTAC Platform Basic Software Program Manual", which describes the software life cycle activities invoked by MELCO's 10CFR50 Appendix B quality program. For the current MELTAC basic software these activities have been reviewed and audited by MHI. MHI will conduct similar reviews and audits for any revised or new MELTAC basic software.

For consistency with RAI 995-7024, MHI will revise the US-APWR SPM (MUAP-07017) as follows:

1. References to the MELCO documents and MELCO as a sub-contractor will be removed.
2. A description will be added to state that, the US-APWR DCD's technical and process requirements will flow to MHI's vendors for procurements. This flow will be verified through the MHI vendor oversight process.
3. The software life cycle process for MELTAC basic software will be addressed in Section 6.0 of the MELTAC Technical Report (MUAP-07005) which will be attached in the response to RAI 995-7024 Revision 0, Question 07.01-45. The Section 6.0 will be referenced from the US-APWR SPM if needed.

In the current US-APWR SPM, the process of subcontractor management is described in Subsection 3.9.7.12 (Software Safety Plan) and Subsection 3.11.3.6 (Software Configuration Management Plan). These sections require that MHI ensures that MELCO's safety software maintenance process and the resulting software are controlled in accordance with the "MELTAC Platform Basic Software Program Manual".

The US-APWR SPM Subsections 3.9.7.12 and 3.11.3.6 will be revised to require that MHI will ensure that vendors' safety software development and maintenance process for any new products conforms to the software life cycle process for the MELTAC basic software described in Section 6.0 of MUAP-07005 which will be attached in the response to RAI 995-7024 Revision 0, Question 07.01-45 and meets the US-APWR DCD's technical and process requirements.

The processes to confirm compliance to the US-APWR Software Program Manual, which ensure that MELCO both maintains the current MELTAC basic software and develops new basic software in accordance with the software life cycle process for the MELTAC basic software, are addressed in existing ITAAC Table 2.5.1-6 #24 relating to the PSMS software lifecycle process.

In addition, to be consistent with RAI 995-7024, any references to the MELCO documents (e.g., JEXU, JSX, N- and Q- documents) will be deleted from the US-APWR SPM.

Impact on DCD
There is no impact on the DCD.

Impact on R-COLA
There is no impact on the R-COLA.

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Report
MUAP-07017 will be revised as shown in Attachment-1.

~~MELCO~~	~~Mitsubishi Electric Corporation~~	DCD_07-56
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	

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~~the digital platform (i.e., 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.~~ The MELTAC Platform is supplied by MELCO, an approved supplier of the safety related digital I&C platform of the MHI US-APWR design as described in DCD Section 1.4.. ~~However, t~~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~~ the basic software is developed and controlled by ~~the MELTAC Platform Basic Software Program Manual (Reference 24)~~this SPM. The basic software shall be specified, procured and received in accordance with the MHI quality management system and controlled under MHI's configuration control as a safety-related item. 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. DCD_07.01-35 DCD_07-56

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.

(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".~~ DCD_07-56

1.4 Definitions

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

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.

~~As described in Section 1.2, the MELTAC Platform including basic software is supplied by MELCO. However,~~ MHI is responsible for specifying the system requirements to develop all PSMS software and confirming that all as-built PSMS software~~, including basic software supplied by MELCO,~~ meets these requirements. Mitsubishi Nuclear Energy Systems (MNES) shall provide the procurement specification to MHI ~~and MELCO~~ which address the subcontractor control specified in this SPM. DCD_ 07-56 DCD_ 07.01-35

Figure 2.2-1 describes the typical organization structure from the plant requirement phase to the installation phase. The organization after the operation and maintenance phase may be changed; however, regardless of the organization changes made, the independence of the VVT from the DT, and the independent reporting relationship for the QA organization shall always be maintained. DCD_ 07-14 BTP-49

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).

DCD_ 07-56

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

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 ~~S~~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).~~

DCD_07.01-30

DCD_07-56

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. | DCD_ 07.01-30

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).~~ | DCD_ 07-56
- The PSMS application software is ~~fully~~ qualified by Independent V&V activities as described in Section 3.10 "SVVP" of this SPM. | DCD_ 07-14 BTP-43
- 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. | DCD_ 07-14 BTP-43
- 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. | DCD_ 07.01-30
- 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 SMP 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).

Subcontractors and suppliers shall be managed in accordance with Section 7 "Control of purchased material, equipment, and services" of Topical Report PQD-HD-1995 "Quality Assurance Program Description" (Reference 27). | DCD_ 07-14 BTP-45

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.
- The MELTAC platform, including the life cycle process for the basic software, is described in MUAP-07005 (Reference 2) ~~and the MELTAC Platform Basic Software Program Manual (Reference 24)~~. The DT and the VVT shall each ensure that the basic software is delivered in accordance with this SPM. DCD_07-56 DCD_07-14 BTP-46
- The DT shall identify the activities being performed by ~~MELCO~~MHI sub-vendor and ensure that these activities are conducted in accordance with this SPM. DCD_07-56 DCD_07-14 BTP-46

3.1.4 Security

Security controls shall be implemented in the application software environment throughout

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

[

]

DCD_ 07.01-30

DCD_ 07.01-30

DCD_ 07-56

DCD_07-14 BTP-46

DCD_07-56

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

DCD_
07-14
BTP-44

DCD_
07-56

DCD_
07-56

DCD_
07-14
BTP-44

DCD_ 07-14 BTP-44

DCD_ 07-14 BTP-44

DCD_ 07-56

DCD_ 07-56

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. As shown in Table 3.2-1 to 3.2-4 and Figure 3.2-1, ~~T~~ the lifecycle activities for the PSMS application software which are organized in a waterfall model include no activity to use prototyping.

DCD_ 07-14 BTP-46

- NUREG/CR-6101 (Reference 26)
- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.153 Rev. 1 (Reference 30)
- Section C of RG 1.172 (Reference 21)

DCD_ 07-14 BTP-45

DCD_ 07-14 BTP-45

- Section C of RG 1.173 (Reference 22)

3.2.10 Basic Software

DCD_07-14 BTP-46

The SDP ~~requirements~~ for the basic software are described in Section ~~3.2~~6.0 of ~~the MELTAC Platform Basic Software Program Manual (Reference 24)~~MUAP-07005.

DCD_07-56

- IEEE Std 730-1998 ~~2002~~ (Reference 8) which is referenced by IEEE Std 7-4.3.2-2003 (Reference 5) DCD_07-14 BTP-47
- Section 3.1.2 of NUREG/CR-6101 (Reference 26).
- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.68 Rev. 1 (Reference 18)
- Section C of RG 1.173 Rev. 0 (Reference 22) DCD_07-14 BTP-45
- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.68 Rev. 1 (Reference 18)
- Section C of RG 1.173 Rev. 0 (Reference 22)

3.3.9 Supplier Control

DCD_07-14 BTP-47 DCD_07-56

All of the PSMS application software is provided by MHI. There are no other suppliers of PSMS application software. However, the basic software is supplied by ~~MELCO~~MHI sub-vendor, and the SQAP requirements for the basic software are described in Section ~~3.3~~6.0 of ~~the Basic Software Program Manual (Reference 24)~~MUAP-07005. ~~MELCO~~MHI sub-vendor shall be controlled as an approved supplier of safety-related items and services, subject to the provisions of 10 CFR 50 Appendix B and 10 CFR 21.

condition is determined by the ~~Licensee~~ engineering organization 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 of the engineering organization as described in Chapter 17 of the facility FSAR. DCD_07-14 BTP-49

The ~~Licensee~~ engineering organization shall also ~~determine~~ evaluate operability of affected Systems, Structures and Components in accordance with the facility Technical Specifications. DCD_07-14 BTP-49

(2) ~~MHI~~Design Team (DT) DCD_07-14 BTP-49

In response to the ~~Licensee~~ engineering organization report provided in Step (1), ~~MHI~~ the DT 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~~ The DT shall ~~assign~~ have 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). DCD_07-14 BTP-49 DCD_07-14 BTP-49

3.6.6.2 Activity: Fault Correction

The DT shall collect and analyze the operational failure data to be provided by the ~~Licensee~~engineering organization, which may include design engineers, system engineers, maintenance engineers, or training engineers, as described in Section 3.6.6.1. DCD_07-14 BTP-49

(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).~~ DCD_07-56

(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 V&V T 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).~~ DCD_07-56

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 ~~P~~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~~ to comply with 10 CFR 50 Appendix B ~~QAP~~. Therefore, there is no maintenance of commercial dedication activities applicable to the PSMS.

DCD_07.01-30

DCD_07-56

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).
- Section C of RG 1.173 Rev. 0 (Reference 22)

DCD_07-14 BTP-45

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 plant personnel for each US-APWR plant. These include MHI technical personnel and management as well as the potential for the ~~customer's~~plant personnel to be qualified to install, operate and maintain the software. Training is therefore essential for ~~technical~~ plant personnel ~~both for MHI and customer~~. This StrngP provides ~~customer~~plant personnel training for the MELTAC platform and the application software of the PSMS. DCD_07-14 BTP-50

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~~. DCD_07-14 BTP-50

(2) ~~Customers~~Plant Personnel DCD_07-14 BTP-50

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~~ 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~~plant personnel. DCD_07-14 BTP-50

~~(3) MHI/MELCO Training Department~~ DCD_07-14 BTP-50

~~MHI~~The DT shall provide ~~customer~~ plant personnel training for the application software using the training materials described in Section 3.7.4.1.1~~. MELCO shall provide customerplant personnel training~~and for the MELTAC ~~P~~platform as described in Section 3.7.4.1.2. DCD_07-56

~~The customer shall develop and maintain training procedures, and shall train and qualify their personnel, including~~ Plant personnel, including operators, I&C engineers shall be trained and I&C technicians in accordance with the training program described in the facility FSAR. DCD_07.01-30 DCD_07-14 BTP-50

3.7.3 Measurement

Training effectiveness shall be measured in accordance with the ~~customer~~ plant personnel training program as described in the facility FSAR. DCD_07-14 BTP-50

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~~plant personnel, 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 plant personnel~~customer~~ as described in the SMaintP (Section 3.6 of this SPM). Training materials shall contain the following information as a minimum: DCD_07-14 BTP-50 DCD_07-14 BTP-50

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 for the Plant Personnel DCD_07-14 BTP-50

~~MHI shall train customer~~ The trainers using for the plant personnel shall be trained the Systematic Approach to Training methods developed by the National Academy for Training (INPO), using the materials developed in Step (1), above. DCD_07-14 BTP-50

(3) Implement the Training Program

~~Customer~~ The trainers for the plant personnel qualified in accordance with the facility FSAR shall implement the training of ~~customer~~ the plant personnel, including operators, I&C engineers and I&C technicians, in accordance with this STrngP, using the training materials provided in Step (1), above. DCD_07-14 BTP-50

3.7.4.1.2 Training for the MELTAC Platform

[ ] DCD_07-56 DCD_07-14 BTP-50

DCD_ 07.01-30

DCD_ 07-56

DCD_ 07-56

DCD_ 07.01-30

DCD_ 07.01-30

DCD_ 07.01-29

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 Ttechnical rReport JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual", which is referenced by this SPM~~ in Section 6.0 of MUAP-07005 "Safety System Digital Platform –MELTAC-". The Design Team (DT) shall create the PSMS application software and associated system configuration in accordance with the critical safety requirements. DCD_07-56

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

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 ~~t~~Technical ~~r~~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 ~~t~~Technical ~~r~~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. DCD_07.01-30 DCD_07-14 BTP-43

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 ~~t~~Technical ~~r~~Report MUAP-07005 "Safety System Digital Platform –MELTAC- " and other related ~~t~~Technical ~~r~~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. DCD_07-14 BTP-43

(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 tTechnical rReport JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual (Bbasic SPM)"~~Section 6.0 of MUAP-07005 "Safety System Digital Platform –MELTAC-" 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 ~~B~~basic SPM. DCD_07-56 DCD_07-56

DCD_07-14 BTP-51
DCD_07-56

DCD_07-56

DCD_07-56

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.~~

DCD_07.01-35

The DT shall ensure that the basic software is developed and maintained in accordance with ~~the "MELTAC Platform Basic Software Program Manual" (JEXU-1012-1132)~~Section 6.0 of MUAP-07005 "Safety System Digital Platform –MELTAC-", and meets the technical and quality requirements specified in the MUAP-07005 Table 0-1. The DT shall determine if the output of the basic software SSP adversely impacts on the SSA activities described in this SPM.

DCD_07-56

The DT shall initiate the corrective actions as needed. ~~If the corrective action requires a change to the basic software SSP or the basic software itself, the DT shall notify MELCO.~~

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

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 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 and other, connected components such as sensors and reactor trip breakers. The MELTAC platform hazard analysis described in ~~the~~ Appendix E of the MELTAC Technical Report (~~JEXU-1011-1002~~MUAP-07005)~~technical report JEXU-1015-1009 "MELTAC Platform Basic Software Safety Report",~~ establishes the preliminary hazards analysis ~~for the PSMS~~ for the MELTAC platform. This analysis confirms that the MELTAC platform can prevent hazardous systems states due to any conditions within the platform, including software and hardware, and ~~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. The system level preliminary hazard analysis for the entire PSMS, including the overall system configuration, the redundancies and the components (process and actuating devices) except the MELTAC platform, are described through Section 3.9.8.1.2 to 3.9.8.1.5.

DCD_ 07.01-39

DCD_ 07-56

DCD_ 07.01-39

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 ~~t~~Technical ~~r~~Report MUAP-09021 "Response Time of Safety I&C System".

DCD_ 07.01-30

The ~~t~~Technical ~~r~~Report MUAP-09021 provides response time allocations. It demonstrates that, with those allocations, the response time requirements in Chapter 15 can be met.

DCD_ 07.01-30

3.9.8.1.3 Criticality Analysis

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~~basic ~~SPM (JEXU-1012-1132), which is referenced by this SPM~~ in Section 6.0 of MUAP-07005 "Safety System Digital Platform –MELTAC-".

DCD_ 07.01-30

DCD_ 07.01-30

DCD_ 07-56

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

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

[ ]

DCD_07-14
BTP-44
DCD_07-56

(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)

(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

[ ] DCD_07-56

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).

3.11.3.2.4 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)~~Section 6.0 of MUAP-07005 "Safety System Digital Platform –MELTAC-"). DCD_07-56

(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.~~ The basic software shall be controlled to ensure that it is developed and maintained in accordance with ~~the "MELTAC Platform Basic Software Manual" (JEXU-1012-1132) (Reference 24)~~ Section 6.0 of MUAP-07005 "Safety System Digital Platform –MELTAC-" and the correct version of the basic software is used in the PSMS application software lifecycle.

DCD_ 07.01-35

DCD_ 07-56

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. The DTM and the DT has the overall responsibility for maintaining the SCMP.

DCD_ 07-14 BTP-53

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

DCD_07-56

(3) System V&V Test

(4) Acceptance V&V Test

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".~~Deleted DCD_07-56

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 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~~security as described in this Technical Report, MUAP-07017 "US-APWR Software Program Manual", and the following related documents; DCD_07-14 BTP-55

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~~ DCD_07-56

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. The secure development and operational environment for the design, production and maintenance of the MELTAC platform basic software is described in ~~Technical Report, JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual (Reference 24)"~~ Section 6.1.6 of MUAP-07005 "Safety System Digital Platform –MELTAC-". The conformance to ~~describes compliance to~~ the secure development and operational environment requirements of RG 1.152, Rev. ~~2~~3 for ~~future changes to~~ the basic software is also described in ~~JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual (Reference 24)".~~Appendix G of MUAP-07005 "Safety System Digital Platform –MELTAC-". DCD_07-14 BTP-55 DCD_07-56

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

Security-Related Information – Withheld Under 10 CFR 2.390	DCD_ 07-56 DCD_ 07-14 BTP-55
Evaluation	
Compliance	

C.2.3.2 Development Activities

Requirement	
During the design phase, ~~The development~~ measures should ~~delineate the standards and procedures that will confirm with the applicable design controls security policies 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 malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted and undocumented functions or applicationsother coding that could adversely impact the reliable operation of the digital safety system~~ be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.	DCD_ 07-14 BTP-55
Analysis	
Security-Related Information – Withheld Under 10 CFR 2.390	DCD_ 07-14 BTP-55

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~~ developer should ensure that the features within the operating system do not compromise the required ~~secure operational environment~~ design features of the secure operational environment so as to degrade ~~system in such each a manner that~~ reliability of the digital safety system ~~would be degraded~~.
Analysis
Security-Related Information – Withheld Under 10 CFR 2.390
Evaluation
N/A

DCD_ 07-14 BTP-55

DCD_ 07-14 BTP-55

DCD_ 07-56

DCD_ 07.01-30

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 for the secure operational environment are just one element of the overall system validation. Each system ~~secure operational environment~~ design features of the secure operational environment 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 Information – Withheld Under 10 CFR 2.390

DCD_ 07-14 BTP-55

DCD_ 07-14 BTP-55

DCD_ 07-56

Security-Related Information – Withheld Under 10 CFR 2.390
Evaluation
Compliance

DCD_07.01-30

C.2.6 Summary

The scope of the PSMS application software secure development and operational environment responsibilities include the Plant Requirements Phase through the Test Phase, as described in RG 1.152, rev.3. The combination of the information in the following documents and this document (MUAP-07017) fully address the software and data secure development and operational environment issues associated with the PSMS application software;

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~~

DCD_07-56

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 Information – Withheld Under 10 CFR 2.390

DCD_
07-56

Security-Related Information – Withheld Under 10 CFR 2.390