Enclosure
Attachment 4
PG&E Letter DCL-12-050

**PG&E Document "SCM 36-01, Revision 0,
Diablo Canyon Power Plant Units 1 & 2
Process Protection System (PPS) Replacement
Software Configuration Management Plan (SCMP)"**

Pacific Gas & Electric Company
Diablo Canyon Power Plant
Units 1 & 2

Process Protection System (PPS) Replacement
Software Configuration Management Plan (SCMP)
Nuclear Safety Related

SCM 36-01

Rev 0

Prepared Sig.		Date	5/9/2012
Print Last Name	Hebert	User ID	WHH3
Reviewed Sig.		Date	05/09/2012
Print Last Name	LINT	User ID	RALA
Coord Sig/Org.		Date	5/09/2012
Print Last Name	Schrader	User ID	KJSE
Approval Sig.		Date	5/9/2012
Print Last Name	Patterson	User ID	SBP1

ALTRAN SOLUTIONS

REVISION HISTORY

Revision Number	Release Date	Affected Pages	Reason for Revision
0		All	Initial Issue

TABLE OF CONTENTS

TABLE OF FIGURES

This page left blank by intent

1 Introduction

1.1 Purpose

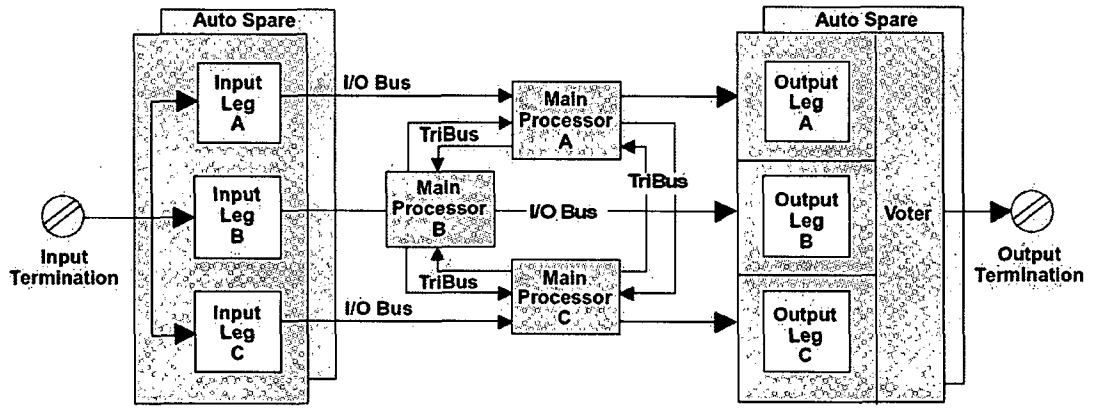
1.1.1 The purpose of this Configuration Management Plan is to establish and document a process of change control and software configuration management for the replacement Process Protection System (PPS), from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility (PITF) and for the remainder of its life cycle following installation at DCPP. This procedure is equally applicable at the PITF as at DCPP.

1.1.2 The Process Protection System (PPS) monitors plant parameters, compares them against setpoints and provides signals to the Solid State Protection System (SSPS) if the setpoints are exceeded. The SSPS evaluates the signals and performs Reactor Trip System (RTS) and Engineered Safety Feature Actuation (ESFAS) functions to mitigate the event that is in progress.

1.1.3 The replacement PPS replaces the Westinghouse Eagle 21 process protection sets currently housed in Protection Racks 1 – 16. Replacement architecture is illustrated in Figure 1-3.

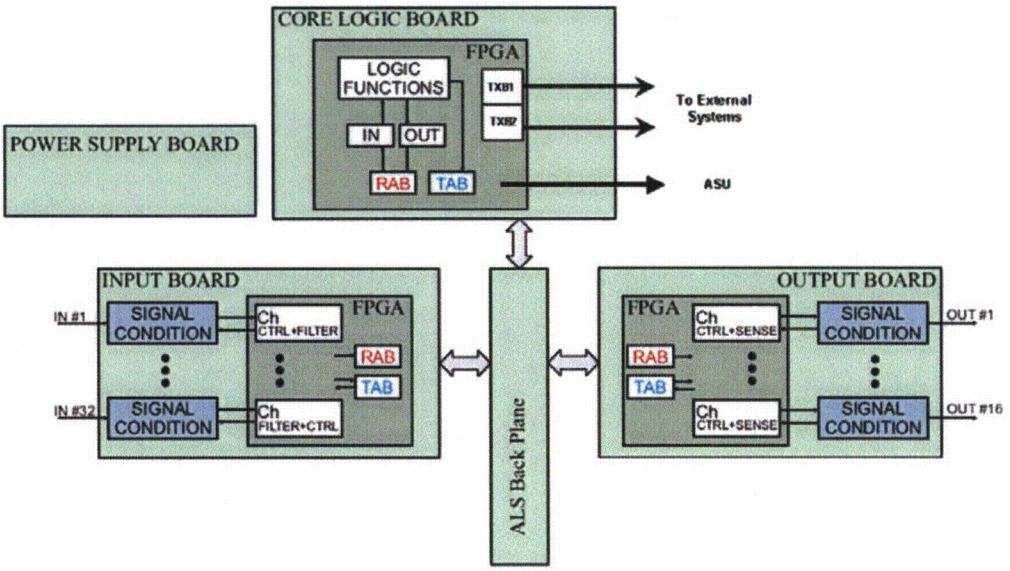
1.1.4 Replacement PPS protective functions will be implemented in four (4) redundant protection sets, each using a software-based Triconex Tricon processor [Figure 1-1] to mitigate events where the NRC-approved PPS Replacement Diversity and Defense in Depth Evaluation [28] determined that diverse and independent automatic mitigating functions are available to mitigate the effects of postulated Common Cause Failure (CCF) concurrent with FSAR Chapter 15 events

Figure 1-1 Tricon Triple Modular Redundant Architecture



1.1.5 For the events where the evaluation determined that diverse and independent automatic mitigating functions were not available and mitigation otherwise would require manual action, automatic protective functions will be performed in a diverse safety-related Westinghouse CS Innovations, LLC Advanced Logic System (ALS) [Figure 1-2]. Refer to the approved PPS Replacement Diversity and Defense in Depth Topical Report [28] for additional information regarding replacement diversity and defense in depth.

Figure 1-2 Generic ALS FPGA Architecture



1.2 Scope

1.2.1 This Plan is required by CF2 [2] and is implemented by CF2.ID2 [3]. Further guidance is contained in SCM 99-1 [21]. This Plan covers configuration control of the system software and defines individuals and organizations responsible for various aspects of the Plan's implementation.

1.2.2 The PPS is identified as a Class "A" computer system as defined in Paragraph 3.3.2 of CF2.ID2 [3] and is listed in CF2.ID2 Attachment 1 as a Class "A" system. A Class "A" computer is defined as a real-time process control or monitoring system used directly to make operational or maintenance decisions.

1.2.3 This document specifies the software configuration management (SCM) activities that are to be done, how they are to be done, who is responsible for doing specific activities, when they are to happen, and what resources are required. It provides general instruction for developing and maintaining configuration control of replacement PPS hardware, firmware, software, interfaces and documentation. This document establishes the basis for a uniform and concise standard of practice for the software configuration management process, based in part on IEEE Standard 828. This document will be updated as needed.

1.2.4 This Plan covers (1) the operating system firmware and the application programs of the Tricon PLC-based PPS subsystem; and (2) the FPGA and NVRAM configuration of the

ALS FPGA-based PPS subsystem. The plan includes the Diablo Canyon specific implementation database; i.e., tunable constants.

1.2.5 The Tricon operating system comprises firmware that resides in the Tricon PPS subsystem processors. The Tricon firmware is controlled and maintained solely by Triconex and any changes/upgrades to the systems must be initiated through Invensys Operations Management (IOM). The Tricon application program is developed by Triconex under their 10 CFR 50 Appendix B [1] QA program. Changes to the Tricon application program must be initiated through IOM.

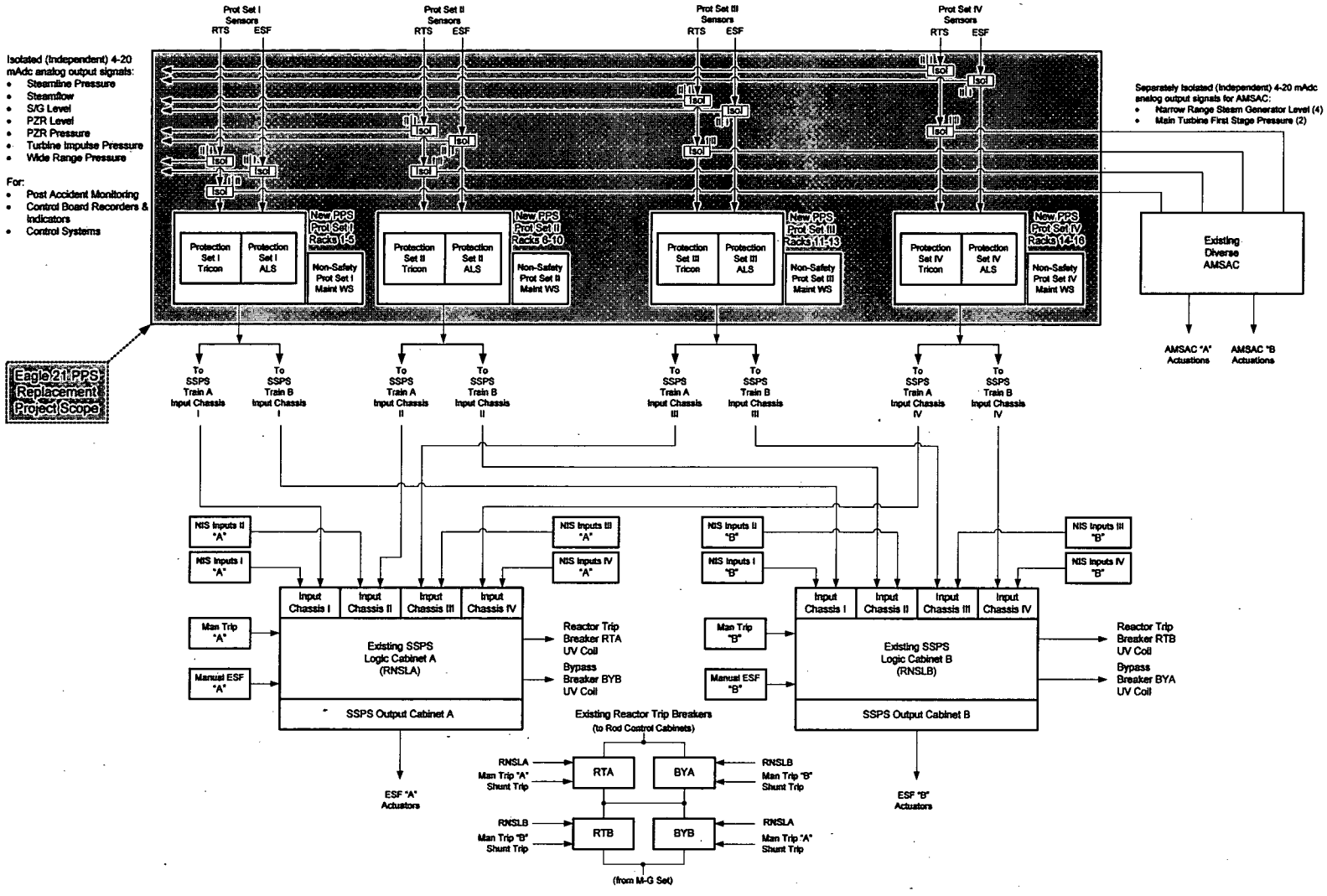
1.2.6 The FPGA-based ALS does not utilize software in the usual sense. The specific application is permanently "burned in" to the FPGA devices to create the PPS logic. The PPA ALS configuration is controlled and maintained solely by Westinghouse/CSI and any changes or upgrades to the system must be initiated by Westinghouse/CSI.

1.2.7 The Diablo Canyon specific implementation database resides in battery-backed memory in the Tricon and in non-volatile random access memory (NVRAM) in the ALS. The database consists of setpoints, tuning constants, gains, offsets, time delays, etc. The database is entered and updated in the respective PPS subsystems per approved plant procedures.

1.2.8 Each ALS board has two sets of NVRAM. The first NVRAM set contains data such as setpoints and tuning constants that can be altered by the technician using the ALS Service Unit (ASU). The second NVRAM set contains the configuration for the particular ALS board. The configuration NVRAM can be changed only by removing the subject board from the ALS chassis and inserting it into a special test fixture. The test texture will be used to configure the ALS boards for a specific protection set.

1.2.9 Self-diagnostics are performed by the Tricon Main Processors and by the ALS Core Logic Boards.

Figure 1-3 PPS Replacement Architecture



1.3 Glossary

1.3.1 Definitions

The following definitions apply to this document:

Term	Definition
Acceptance Criteria:	Indicators used to determine the success or failure of the SCM activity.
Baseline	A set of hardware, firmware, software components and supporting documentation that is subject to change management and is upgraded, maintained, tested, statused and obsolesced as a unit. The collection of configuration items (CI), that have been formally reviewed and agreed upon, then serves as the basis for further development, and can be changed only through the formal change control process. Once a work product has been completed, approved and logged as part of an official baseline, it cannot be changed without appropriate level of approval.
Configuration Control	Configuration control is a formal process for which a change to the specification of a CI is systematically proposed, evaluated, approved or disapproved, and implemented. Configuration control is the means of ensuring that system baselines are accurate and known throughout the lifecycle of the system.
Configuration Management (CM)	A formal engineering discipline that provides the methods and tools to identify and control the system throughout its development and use. An integrated process that identifies existing plant design and licensing requirements and controls changes to ensure that the plant is configured, maintained, operated and managed in a manner that is consistent with the design bases and licensing commitments.
Design Change Vehicle	Changes to the DCPP configuration shall be made via an appropriate design change vehicle per CF4.ID1 [12]. Design changes, requests, and vehicles are described in detail in CF4.ID1
Firmware	Firmware is the combination of a hardware device and computer date or instructions that reside as read-only software on that device.
Functional Change	Any software change which affects the functionality of the PPS. Generally these changes require a change in design basis and/or system requirements documentation.

Term	Definition
Organization	A description of the organization responsible for SCM activities. A description of the boundaries and interfaces between the SCM organization and other company organizations. A description of the reporting channels.
Oversight	A process or function used to oversee work, such as the Quality Assurance program.
Plant Computer System	A computer system including microprocessor digital systems used to perform functions important to safe and reliable plant operation.
Record-keeping	Identification of SCM records required 1) to document the work performed, 2) to demonstrate that the purpose has been achieved, and 3) to store, handle, retain and ship documentation. Record structures should be provided. Procedures should exist for protecting configuration items. A tracking system should exist for managing configuration items so that the revision history of each configuration item may be retrieved and so that the latest revision of each configuration item may be easily identified. Procedures should exist for backup and disaster recovery.
Responsibilities	A definition of the duties assigned to the responsible organization(s) covered by the SCMP, and of the individuals within the organization(s). Specification of the person or group responsible for the successful completion of each SCM task. Definition of the duties of change authorities, such as ITRs and CDRs. Specification of the entity with the authority to release any hardware, software, data or documents for operation.
Risks	The method used to identify, assess and manage risks that may interfere with achieving the purpose of the SCMP.
Schedule	The time order of events necessary to achieve the purpose of the SCMP, given either as absolute dates, ranges of dates, or offsets from other dates.
Security	The methods used to protect the information created by or reviewed by the organization covered by the SCMP from inadvertent or malicious alteration. The ability to prevent unauthorized, undesired and unsafe intrusions, and verify that cyber security features are maintained under configuration control.

Term	Definition
Software Design Description (SDD)	The SDD describes the major components for software design, including internal interfaces and controlled databases.
Software Design Review	The formal process of reviewing, confirming, or substantiating the technical adequacy of a software design or modification to an established standard.
Software Life Cycle	The complete life cycle of the software modules including requirements, design, implementation, test, installation, and operation and maintenance. This SCMP emphasizes the operation and maintenance phase of the software life cycle.
Software Quality Assurance Plan	A Plan which identifies SQA requirements and defines all reviews and approvals for each computer system and/or application and specifies the manner in which modifications will be made and documented.
Software Requirements Specification (SRS)	The SRS discusses the system's functional requirements, including functions, performances, design constraints, attributes, etc., of the software and the external interfaces.
Software	Computer programs, procedures, rules, and associated documentation and data pertaining to the operation of a computer system and/or application. The definition of software shall also include data files containing programmer-specified constants, flags, and setpoints. This includes programs that generate displays of plant system configuration, technical specification applicability, and similar items relied upon by operators and technical personnel to operate the plant.

1.3.2 Abbreviations and Acronyms

Term	Definition
ALS	Advanced Logic System
AS	Application Sponsor
ASU	ALS Service Unit
CCF	Common Cause Failure
CCP	Configuration Change Package
CDR	Critical Digital Review
CI	Configuration Item
COTS	Commercial Off-the-Shelf

CSA	Configuration Status Accounting
CSI	CS Innovations, Inc.
DCP	Design Change Package
DCPP	Diablo Canyon Power Plant
DLAP	Department Level Administrative Procedure
EPROM	Electrically Programmable Read Only Memory
FCA	Functional Configuration Audit
FPGA	Field Programmable Gate Array
FRS	Functional Requirements Specification
I&C	Instrumentation and Control
ICE	Instrument & Controls Engineering
IDAP	Interdepartmental Administrative Procedure
IOM	Invensys Operations Management
IOS	Input Output System
IRS	Interface Requirements Specification
ITR	Independent Technical Review
LAN	Local Area Network
LBIE	Licensing Basis Impact Evaluation
MWS	Maintenance Workstation
NVRAM	Non-Volatile Random Access Memory
PCA	Physical Configuration Audit
PD	Program Directive
PDN	Plant Data Network
PG&E	Pacific Gas & Electric Company
PITF	Project Integration and Test Facility
PLC	Programmable Logic Controller
PLS	Precautions, Limitations, and Setpoints
PMT	Post Modification Testing
PPS	Process Protection System
SC	Software Coordinator
RMS	Records Management System
SCM	Software Configuration Management
SCMP	Software Configuration Management Plan
SCP	Software Change Package
SDD	Software Design Description

SQA	Software Quality Assurance
SRS	Software Requirements Specification
SQAP	Software Quality Assurance Plan
V&V	Verification & Validation

1.4 References

1. Title 10 Code of Federal Regulations Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power, Plants and Fuel Reprocessing Plants"
2. PG&E CF2 Computer Hardware, Software, and Database Control
3. PG&E CF2.ID2 Configuration Management for Computers and Software Used for Plant Operations and Operations Support
4. PG&E CF2.ID9 Software Quality Assurance Plan for Software Development
5. PG&E CF2.ID10 Administrative Controls for Access and Interface with Plant Digital Systems and Components
6. PG&E CF2.ID11 Cyber Security Assessment of Critical Digital Assets
7. PG&E CF3, Design Control Program Directive
8. PG&E CF3.ID9, Design Change Development
9. PG&E CF3.ID16, Specifications
10. PG&E CF3.ID13, Replacement Parts Evaluation and CITE
11. PG&E CF4, Modification Control Program Directive
12. PG&E CF4.ID1, Modification Request and Authorization
13. PG&E CF4.ID3, Modification Implementation
14. PG&E CF6.ID1 Setpoint Control Program
15. PG&E OM7.ID1 Problem Identification and Resolution – Action Requests
16. PG&E TS3.ID2 Licensing Basis Impact Evaluations
17. PG&E AD7.DC8, Work Control
18. PG&E AD10.ID1 Storage and Control of Quality Assurance Records
19. NEI 01-01: Nuclear Energy Institute, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1: A Revision of EPRI TR-120348 to Reflect Changes to the 10 CFR 50.59 Rule"
20. NEI-08-09, Rev 6, Nuclear Energy Institute, "Cyber Security Plan for Nuclear Reactors"
21. PG&E SCM 99-1, SCM Plan for I&C Digital Assets
22. PG&E SQA 99-5 Software Quality Assurance Plan for I&C Digital Assets
23. PG&E 663195-44, Process Protection System (PPS) Replacement Functional Requirements Specification (FRS)
24. PG&E PPS Interface Requirements Specification (IRS)
25. PG&E 10115-J-NPG, Controller Transfer Functions Design Input Specification

26. CS Innovations 6116-00011 Diablo Canyon PPS ALS System Design Specification
27. PG&E 663229-47, Precautions, Limitations, and Setpoints
28. U.S. Nuclear Regulatory Commission, Letter "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, "Process Protection System Replacement Diversity & Defense-In-Depth Assessment" (TAC Nos. ME4094 and ME4095)," April 19, 2011 (ADAMS Accession No. ML110480845)
29. U.S. Nuclear Regulatory Commission, Letter to PG&E, "Diablo Canyon Power Plant, Units Nos. 1 and 2 – Issuance of Amendments RE: Approval of Cyber Security Plan (TAC Nos. ME4290 and ME4291), July 15, 2011, including approved Cyber Security Plan
30. PG&E SC-I-36-M, "Eagle 21 Tunable Constants"
31. PG&E Diablo Canyon Power Plant Technical Specifications
32. Tricon PPS Replacement Software Requirements Specification (SRS)
    a) Triconex Document No. 993754-11-809, "Process Protection System Replacement DCPP Software Requirements Specification Protection Set I"
    b) Triconex Document No. 993754-12-809, "Process Protection System Replacement DCPP Software Requirements Specification Protection Set II"
    c) Triconex Document No. 993754-13-809, "Process Protection System Replacement DCPP Software Requirements Specification Protection Set III"
    d) Triconex Document No. 993754-14-809, "Process Protection System Replacement DCPP Software Requirements Specification Protection Set IV"
33. Triconex PPS Replacement Software Design Description (SDD)
    a) Triconex Document No. 993754-11-810, "Process Protection System Replacement DCPP Software Design Description Protection Set I"
    b) Triconex Document No. 993754-12-810, "Process Protection System Replacement DCPP Software Design Description Protection Set II"
    c) Triconex Document No. 993754-13-810, "Process Protection System Replacement DCPP Software Design Description Protection Set III"
    d) Triconex Document No. 993754-14-810, "Process Protection System Replacement DCPP Software Design Description Protection Set IV"

2 Software Configuration Management

The objective of managing configuration control is to assure the reliability of nuclear generation equipment. Controlling configuration requires controlling change; i.e., all changes shall be auditable and authorized, and that all unauthorized changes shall be investigated.

2.1 Organization

2.1.1 System Coordinator (SC)

The person responsible for the technical aspects of providing and maintaining the digital assets and system components. The SC is normally a member of the Digital Systems Engineering Group.

2.1.2 Application Sponsor (AS)

The person who represents the system users for a particular application and who maintains administrative control of the application. Normally, this is a representative from I&C Engineering (ICE). The AS is responsible for initiating and reviewing changes to the system.

2.1.3 System Team

The permanent PPS System Team is comprised of the following members:

- Application Sponsor (Design System Engineer)
- System Coordinator
- Maintenance Engineer(s), as appropriate
- Operations

Other, temporary, members may be required to provide additional expertise for specific projects or problems.

2.2 Responsibilities

2.2.1 Technical Oversight

The SC shall be responsible for the technical aspects of development and maintenance of the system and its associated peripherals and software. The SC shall be qualified to perform a LBIE screen-related technical review of system change requests and packages, in accordance with TS3.ID2 [16].

The SC is responsible for the technical aspects of how system development and maintenance affect the Simulator system.

The SC normally takes on the role of AS for applications installed on the system per plant design for changes that do not result in a change to the Functional Requirements Specification (FRS) of the application [23].

The AS shall be responsible for implementing and updating this SCMP and the SQAP, overseeing development of and approving any required documentation, establishing

access controls, approving configuration changes, and ensuring other related administrative tasks are performed.

Specifically, the System Coordinator is responsible for:

- Software design and modification
- Control of software documentation
- Evaluating the impact of hardware changes on system software.
- Ensuring modifications maintain the design bases of the PPS.

The Application Sponsor is responsible for:

- Development of SQA procedures
- Coordination of SQA required activities
- Self-assessments of SQA implementation
- Evaluating any maintenance or other activities that may lead to hardware or software changes
- Evaluating all new software releases from the vendor to determine if and when the software will be installed
- Evaluating, coordinating, implementation and documenting of software change requests by other plant departments
- Classifying software changes per the levels defined in Section 3.2.2.

The System Team facilitates effective overall management of the PPS. System Team responsibilities include overall direction and management to ensure the PPS is operating properly and fulfilling its requirements. System Team responsibilities include:

- Evaluation of PPS problems or failures
- Analysis of impact of industry events
- Monitoring material condition and problems within the system
- Supporting major audit activities
- Addressing nonconformances within the system
- Assisting prioritization of system work backlog
- Operability Evaluations
- System Walkdowns

The SC and the System Team are responsible for classifying changes per Section 3.2.2.

2.2.2 Functional Changes

The AS shall be responsible for implementing functional changes; i.e., changes that require modification to the FRS [23], IRS [24], or Controller Transfer Function Specification [25] as described in Section 3.2.2.

The AS shall have Qualification ENGDRI per Section 5.1 of CF3.ID9 [8]. Functional changes shall be documented with a Design Change Package (DCP) of sufficient detail to ensure baseline configuration is ascertainable at any time. Approved functional changes shall be installed in conformance with existing DCPP design change procedures.

2.2.3 Configuration Control

The SC shall maintain configuration control. Application software and configuration (firmware, FPGA, NVRAM) modifications shall be performed by or under the direction of the SC and shall be documented with a Software Change Package (SCP) or Configuration Change Package (CCP) of sufficient detail to ensure baseline configuration is ascertainable at any time. Refer to SQA 99-5 [22] for further detail and instructions for developing SCP and CCP documentation.

Offsite vendors and other support personnel shall comply with this SCMP or a similarly approved plan when providing outsourced services on the system.

2.2.4 Problem Identification

Software, hardware and configuration problems with the system shall be reported and documented per OM7.ID1 [15]. Software and/or configuration problems should normally be reported via a PROG PDCM Notification (a notification task may be utilized off an existing notification). Hardware related problems should be an EQPR AANS Notification.

2.3 Risks

2.3.1 Deploying Changes

Testing and setup of configuration and software changes shall be performed on an asset that is not in service; i.e., the maintenance training system provided for this purpose. Comprehensive regression testing on an off-line development test platform shall be performed to the extent appropriate to the complexity of the change.

2.3.2 Contingency Planning

In the event of emergencies, system failures or disaster, recovery of each component vital to the system shall be facilitated. Software/Configuration backups shall be made at the discretion of the SC based on the frequency at which critical data and configurations are changing.

2.3.3 Media Control

Valid backups shall be available to support recovery of any software-based portion of the PPS; that is, the Tricon and Maintenance Workstation (MWS). The ALS is FPGA-based and does not employ software. Installation media, license keys, backups, logical network diagrams and configuration information shall be stored in a safe location, such as Source Safe.

The Digital Systems Engineering SourceSafe is the repository for all committed project software. The repository contains the following typical file types[1]:

- Executables
- Source code
- PLC and HMI program code
- IOS Kernel
- Setup and configuration files
- Database files
- Input files for software testing, verification testing and validation testing
- Test Case data files used for validation testing
- Scripts and post-processing utilities used for software testing

Where magnetic or optical media are used for storage of essential PPS files, the media shall be labeled and maintained by the SC such that the current version is readily identifiable. To provide redundancy and data integrity, copies of media should be created and stored in physically separate locations, as appropriate.

The SC shall document and maintain local copies of restoration procedures for backup and disaster recovery.

2.4 Security

2.4.1 Physical Security

Access to digital assets, system components, software libraries, portable devices, and removable media shall be restricted to necessary personnel.

2.4.2 Cyber Security

User authentication and access to edit configuration, software and data shall be controlled by the SC per CF2.ID10 [5] and CF2.ID11 [6]. Passwords and/or restricted user privileges shall be used to maintain access control and activity accountability. The SC may periodically change passwords or account capabilities.

Access control to the maintenance workstation shall be consistent with NEI 08-09 A.1 [20]. The use of the maintenance workstation will require a key that is obtained from operations personnel in the plant control room. The maintenance workstation is contained in the plant vital area and can only be reached by personnel with vital area access. Use of the maintenance workstation will be password protected.

The PPS will be isolated from the DCPP Plant Data Network (PDN) by means of a network appliance that allows one way communication from the PPS to the DCPP PDN only. The PDN itself will be isolated from the DCPP Business LAN using a deterministic

[1] This is a list of typical file types that reside in the SourceSafe. The PPS may not use all file types listed.

unidirectional network appliance in accordance with Paragraph 4.3 of the NRC-approved DCPP Cyber Security Plan [29].

3 SCM Activities

3.1 Configuration Identification

Configuration identification is the process of identifying and describing system elements in terms of its common and site-specific component parts, to include all hardware, firmware, software and associated documentation.

3.1.1 Configuration Items (CIs)

CIs are an aggregation of reasonably mature hardware, software, Commercial Off-the-Shelf (COTS) or database components that combine together to perform a specific function or functions. Each CI is designated for configuration management control.

3.1.1.1 COTS Hardware

COTS hardware products are identified by vendor names, part numbers, serial numbers, and drawing numbers.

3.1.1.2 COTS Software

COTS software products are identified by vendor names, part numbers, version/revision numbers, serial numbers, installed locations, and any applicable installation parameters.

Configuration files developed for COTS software shall be maintained and controlled by the SC.

3.1.1.3 Databases

Databases are defined by both their schema and their contents. The database schema is managed and controlled as software. The database contents are managed and controlled as configured articles, which can be categorized either as static parameters or dynamic data generated by the system. Static database parameters are controlled. The contents of dynamic database files are not controlled.

3.1.2 Baselines

A baseline is a logical grouping of configuration items that constitute the system. Baselines provide a fixed reference to specify the configuration items at a particular milestone event or point in time.

The PPS baseline is the operating system, firmware, applications software, FPGA configuration, and database(s) prepared by the vendors (IOM and Westinghouse/CSI) which define the system at specific milestones; i.e., at the time it is shipped, installed, and maintained in the plant.

The baseline establishes an approved standard upon which subsequent work can be made. After the initial PPS baseline is established, changes to the baseline can only be performed through a formal change request process.

The PPS database listing of all tunable constants will be maintained in PPS Scaling Calculation SC-I-36-M [30]. The current values of parameters updated by surveillance tests are obtained from, and documented by, the respective surveillance test procedure.

3.1.3 Backup and Disaster Recovery Libraries

The Digital Systems Engineering SourceSafe is the repository for all committed project software.

Digital assets use magnetic and optical media for storage of files. Media shall be labeled and maintained by the SC such that the current version is readily identifiable. To provide redundancy and data integrity, copies of media should be created and stored in physically separate locations, as appropriate.

The SC shall document and maintain local copies of restoration procedures for backup and disaster recovery.

3.1.4 Configuration Identification Documents

Configuration identification documents support the configuration and development of a CI. These technical documents are used to establish baselines at specific milestones throughout the lifecycle of the system.

3.1.4.1 Technical Documentation

Types of technical documentation include:

- Functional and technical specifications (FRS, IRS, SRS, SDD, etc.)
- Drawings and parts lists
- Technical manuals (Users Manual, System Maintenance Manual, etc.)
- Management plans and procedures (SCMP, SQAP, etc.)

3.1.4.2 Software Configuration Manuals

System-specific SCM information for the PPS shall be captured in the following SCM Manuals:

a. The Tricon baseline configuration shall be captured and recorded in a specific Tricon SCM Manual that shall be prepared per the guidance of Section 6.0 of SCM 99-1 [21].
b. The ALS baseline configuration shall be captured and recorded in a specific ALS SCM Manual that shall be prepared per the guidance of Section 6.0 of SCM 99-1.
c. The Maintenance Workstation (MWS) baseline configuration shall be captured and recorded in a specific Tricon SCM Manual that shall be prepared per the guidance of Section 6.0 of SCM 99-1.

Information to be captured in the SCM Manual shall include the detailed system baseline configuration, and specific installation and disaster recovery instructions for that system, in compliance with configuration identification and management expectations in Sections 3.1 and 3.2 of this document. Guidance for preparation of SCM Manuals is provided in SCM 99-1 [21].

3.2 Configuration Control

Configuration control is a formal process for which a change to the specification of a CI is systematically proposed, evaluated, approved or disapproved, and implemented. Configuration control is the means of ensuring that system baselines are accurate and known throughout the lifecycle of the system.

3.2.1 Requesting Changes

All PPS modification requests shall be initiated and tracked per plant procedures or CF4.ID1 [12], as judged appropriate by the SC and AS for the level of modification.

3.2.2 Evaluating Changes (Classification of Modifications)

This Plan recognizes that modifications will be made to the System over its lifecycle. It is expected that the modifications will vary in scope and complexity. It is necessary, therefore, to assign a level to the various types of modifications. The SC shall be responsible for assigning the levels to the modifications. These levels are defined in the following paragraphs.

As defined below, Level 1 changes are minor software/configuration changes that do not modify system functionality. Change package documentation, per CF2.ID2 [3], shall be generated for Level 1 minor software/configuration changes. The software change process is detailed in the Digital Systems Engineering SQA Plan for I&C Digital Assets [22].

Level 2 and Level 3 modifications are major software changes that require a 10 CFR 50.59 evaluation. An in-depth potential software failure analysis shall be performed, per NEI 01-01 [19] guidance, to determine whether the proposed software change meets the evaluation criteria or poses potential consequences and risks that are significantly different than previously associated with the software. If the analysis shows that any of the 10 CFR 50.59 criteria are not met, the licensee must submit a license amendment request to the NRC and needs to receive approval prior to implementation.

An approved Change Package is required prior to implementing any changes that modify the documented system baseline. The Change Package documentation shall describe the issue being addressed by the change, the primary component(s) affected by the change and a brief summary of the approved changes.

An SAP Notification and Order shall be utilized as the work authorization, per AD7.DC8 "Work Control" [17]. Modification information is recorded in the requesting SAP Notification. The implementation of the change is documented in the associated Change Package and SAP Order. All records generated per this procedure shall be entered in the Record Management System (RMS) and handled as "Quality Records" per AD10.ID1 [18].

3.2.2.1 Level 1 Modification

Level 1 modifications to the DCPP PPS database are controlled by plant procedures. In general, such changes are parameter updates that are the result of surveillance tests or maintenance procedures, and specifically exclude any parameters controlled by the Technical Specifications, the Precautions, Limitations, and Setpoints (PLS) document [27], Engineering-Controlled Setpoints, or other plant design bases. These parameters include, but are not limited to the following:

1. NR and WR RTD coefficients and IRTD
2. PZR Vapor Temp RTD Coefficients and IRTD
3. NI current IBIAS
4. NR RTD Scan Status
5. OTDT and OPDT Turbine Runback Settings (within PLS Limits is a Level 1 change)
6. OTDT and OPDT Tuning Constants Full Load Loop DT (DELTA T0) and Full Load Tavg (TAVG0 FULL OTSP, TAVG1 FULL OPSP)
7. Streaming Factors (S1 STREAMING, S2 STREAMING, S3 STREAMING)
8. Hot and Cold Leg Deviation Check Setting (DELTAH RSA, DELTAC RSA)
9. Reactor Power Distribution Factor (SCAL FLUX CALIB)
10. Threshold for Application of Streaming Factors (PLOW BIAS CAL THR)
11. Steam Pressure Density Compensation Constants (a STM DENSITY COMP, b STM DENSITY COMP, STEAM DENSITY REF)
12. Trip Time Delay (TTD) Power Limit (TTD POWER HI LIMIT) (within Tech Spec Limits is a Level 1 change), and Full Power Delta-T (DELTA T0)
13. Comparator Deadbands
14. Streaming Factor Calc Lag (TAU8 STREAM LAG)
15. RCS Flow ranges (mx+b)
16. Steam Flow ranges (mx+b)
17. Calibration gains and offsets (Determined during Surveillance Test)
18. Steam flow cutoff threshold (SF DP LOW THRESHOLD)

Level 1 changes shall be made per the applicable plant procedure or program, and documented in SC-I-36-M [30] with the exception of calibration gains and offsets.

3.2.2.2 Level 2 Modification

A Level 2 modification to the System database software affects the Technical Specifications, the PLS, or other plant design bases. Level 2 modifications require a design change vehicle per CF4.ID1 [12] unless another procedure takes precedence.

A design change vehicle per CF4.ID1 [12] is required for any modification to the PPS which will result in a revision to approved Drawings, design classification, functional requirements, installation specifications, test procedures, supplier drawings or approved instruction manuals, and any other baseline documents, except for Level 1 modifications as discussed above.

Level 2 modifications shall be made per CF4.ID1 [12], CF4.ID3 [13], and CF3.ID9 [8], unless the System Team agrees upon another, more appropriate design change vehicle.

3.2.2.3 Level 3 Modification

A Level 3 modification installs revised PPS firmware, application software or FPGA release, which may in turn affect the database software or PPS configuration.

It is imperative that any such modification be evaluated for Licensing Basis Impact per TS3.ID2 [16]. Should the manufacturer recommend a firmware or FPGA upgrade, the System Team shall coordinate the evaluation of the new releases per CF4.ID1 [12]. A determination shall be made as to whether or not to install the new firmware or FPGA release per CF4.ID1.

Level 3 modifications shall be made per CF4.ID1 [12], CF4.ID3 [13], and CF3.ID9 [8]. PPS firmware or FPGA may be replaced with identical firmware or FPGA without a design change. Such replacement may be necessary due to EPROM or FPGA failure, electronic circuit board replacement, or for other maintenance-related reasons. Replacement EPROMs or FPGA shall be obtained from the manufacturer.

If replacement of an ALS board requires configuration of NVRAM on the board, the board may be replaced without a design change provided that the replacement board NVRAM is configured identically to the NVRAM of the board being replaced. This applies to both sets of NVRAM on the ALS board.

3.2.3 Approving or Disapproving Changes

The System Coordinator shall evaluate proposed changes and recommend approval or disapproval to DCPP management via approved procedures.

3.2.4 Implementing Changes

3.2.4.1 The SC shall determine when the modification will be installed (outage or during plant operation). The SC shall be responsible for coordinating performance of the work with the Work Planning Center. The System Team may elect to have a vendor representative install modifications depending on the complexity. If so, the SC will be the responsible work supervisor.

3.2.4.2 The SC will coordinate the implementation of the software changes. A temporary plant procedure may be used to implement, verify, and test the software changes. For minor changes, order instructions may be used to implement software changes provided that all changes are verified by a second qualified individual.

3.2.4.3 PPS application program and FPGA changes are subject to verification and validation (V&V) per manufacturer's procedures. The manufacturers are responsible for preparing the necessary Verification and Validation Test Plan, and the V&V Test Report upon completion of V&V activities in accordance with their 10 CFR 50 Appendix B [1] software development procedures.

3.2.4.4 Level 1 and Level 2 changes shall be implemented using appropriate plant procedures with verification by a second qualified individual that the changes are consistent with the design.

3.2.4.5 The SC shall evaluate whether the software changes impact the Simulator. If so, the Learning Services Simulator Group shall be notified by SAP Task, as appropriate.

3.2.4.6 An approved Change Package is required prior to implementing any changes that modify the documented system baseline. The Change Package documentation shall describe the issue being addressed by the change, the primary component(s) affected by the change and a brief summary of the approved changes.

3.2.4.7 A SAP Notification and Order shall be utilized as the work authorization, per AD7.DC8 "Work Control" [17]. Modification information is recorded in the requesting SAP Notification. The implementation of the change is documented in the associated Change Package and SAP Order. All records generated per this procedure shall be entered in the Record Management System (RMS) and handled as "Quality Records" per AD10.ID1 [18].

3.2.5 Document Identification and Control

3.2.5.1 Document identification and control consists of placing all project documentation and drawings in a central location and maintaining a record of changes to those files. The NPG Library is the repository of project documents. The DCPP/HBPP Drawing Library is the repository of project drawings. These repositories maintain a record of the document version number when a specific file was last changed.

3.2.5.2 Documentation shall be generated for all firmware, software, and FPGA configuration changes that modify the functionality of the system, as required per procedure CF2.ID9 [4], and Program Directives [7] and CF4 [11]. The functionality of the PPS is defined in the FRS [23], IRS [24], and the Controller Transfer Function Specification [25],

3.2.5.3 Software Change Package (SCP) documentation is developed by the SC responsible for the software. The SCP tracks completion of all tasks required to transition from one baseline to another. The SC shall update the SCM records with the revised CI baseline. See SQA 99-5 [22] for further detail and instructions for developing SCP documentation.

3.2.5.4 Configuration Change Package (CCP) documentation is developed by the SC responsible for maintaining system hardware configuration. This is used solely for changes in the configuration of equipment and not to initiate changes to compiled software. The CCP details the requirements of the change, scope, specifications, testing and implementation. The SC may update the SCM records with the revised configuration baseline, as appropriate. See SQA 99-5 [22] for further detail and instructions for developing CCP documentation.

3.2.5.5 The current location of the document repository is http://dcpp142/idmws/home.asp. All library users are allowed read access to the repository. Only the project SC, AS or their designees may commit changes to files retained in the repository.

3.2.6 Interface Control

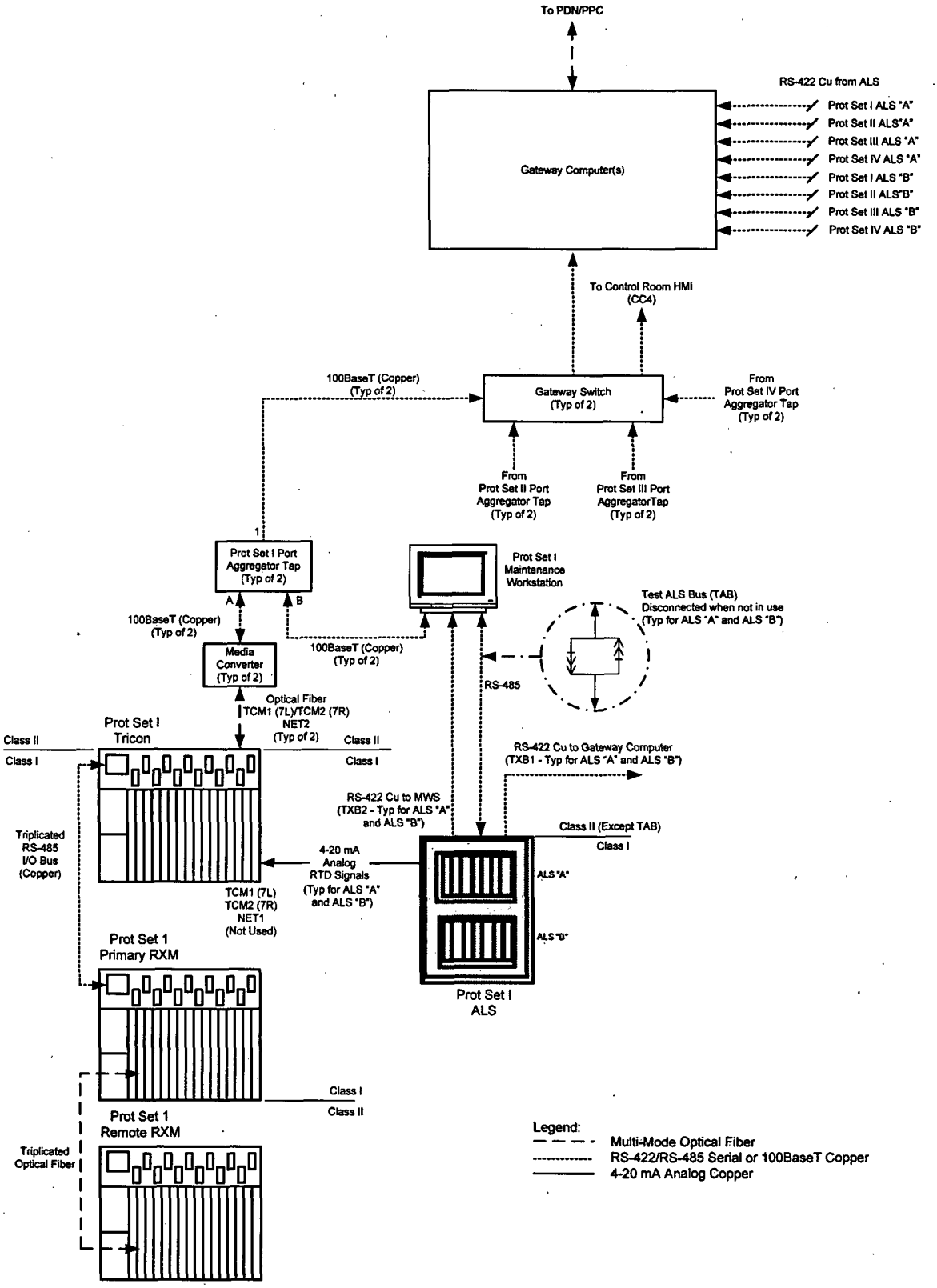
Figure 3-1 provides a simplified illustration of PPS communications with external plant systems.

Data products that flow between systems are subject to configuration management. The SC of the source of the data (output) and the SC of each receiving system (input) are equally responsible for ensuring the continuity of the interface.

Interface management is captured in the Triconex SRS [32] and the ALS System Design Specification [26] as well as the replacement PPS Interface Requirements Specification (IRS) [24] document.

Changes to an interface must be coordinated and agreed to by the SCs of all systems participating in that interface, whether provider or end user.

Figure 3-1 PPS Communications (Simplified)



3.2.7 Testing

3.2.7.1 Post Modification Testing

a. For Level 1 modifications, the applicable plant procedure should include appropriate documentation of steps performed. Changes are documented by a performer and verified by a second qualified individual that changes have been entered correctly, and successful completion of the appropriate surveillance or maintenance test, if required.
b. For Level 2 modifications, the PMT requirements of CF3.ID9 [8] are sufficient. Determination of PMT requirements shall include an evaluation of impact on Technical Specifications, PLS, or other plant design bases. All applicable surveillance tests shall be completed successfully.
c. For Level 3 modifications, guidance shall be obtained from the manufacturers and such guidance shall be included in the PMT requirements for the DCP.
d. Following a like-for-like EPROM, FPGA, or NVRAM replacement, PMT shall include the performance of at least one surveillance test on a channel affected by the replacement. PMT shall also include verification that the database is consistent with the controlled database in SC-I-36-M [30].

3.2.7.2 Surveillance Testing

Prior to being placed in service and declared OPERABLE and at all times thereafter when required to be OPERABLE, the PPS shall pass all applicable surveillance tests required to meet Technical Specifications [31].

3.2.8 Code Control

3.2.8.1 Triconex Code Control

The Triconex PPS subsystem operating system, firmware, and PPS application source code is strictly under IOM control. PG&E cannot make any changes to the operating system, firmware, or application source code. The Tricon application source code is documented in accordance with the Tricon SRS [32] and SDD [33], which are provided to PG&E for review and approval.

3.2.8.2 ALS Code Control

The ALS PPS subsystem FPGA configuration is strictly under Westinghouse/CSI control. PG&E cannot make any changes to the FPGA configuration. The FPGA configuration is provided in the ALS System Design Specification [26].

3.2.9 Disaster Recovery

Maintaining the PPS database in SC-I-36-M [30] and spare parts availability discussed in Section 3.2.12.3 ensure that means exist to recover software, data and documentation after it has been damaged (e.g., fire, loss of power, earthquake, etc.). The object is to quickly and efficiently recreate the baseline that was present just prior to the loss.

3.2.10 Problem Reporting and Corrective Action

All identified problems and their corrective action shall be tracked to completion using a notification. The System Team shall follow the requirements contained in OM7.ID1 [15].

3.2.11 Supplier Control

3.2.11.1 The Tricon and ALS hardware, software, FPGA and future releases are produced in accordance with the respective manufacturer 10 CFR 50 Appendix B [1] QA program.

3.2.11.2 The evaluation, purchase and installation of PPS hardware and firmware releases after those shipped with the system shall be the responsibility of the SC.

3.2.12 PPS Configuration Management

3.2.12.1 PPS Hardware and Firmware/Operating System Configuration

a. The Tricon baseline configuration shall be captured and recorded in a specific Tricon SCM Manual that shall be prepared per the guidance of Section 6.0 of SCM 99-1 [21].
b. The ALS baseline configuration shall be captured and recorded in a specific ALS SCM Manual that shall be prepared per the guidance of Section 6.0 of SCM 99-1.
c. The Maintenance Workstation (MWS) baseline configuration shall be captured and recorded in a specific Tricon SCM Manual that shall be prepared per the guidance of Section 6.0 of SCM 99-1.

3.2.12.2 PPS Database

The current PPS database listing of all tunable constants shall be maintained by the SC in SC-I-36-M [30].

3.2.12.3 Spare Parts

The System Coordinator shall be responsible for ensuring that a supply of spare parts is available in the warehouse at all times. The SC shall coordinate with the DCPP Materials Department to ensure that the proper stock codes are assigned to replacement parts.

3.2.12.4 Replacement Parts Evaluation

Replacement PPS components which are different from those shipped with the system would normally be considered to be Level 2 modifications. As described in Section 3.2.2.2, such Level 2 modifications require a Design Change Vehicle to be prepared per CF4.ID1 [12]. If the replacement parts meet the following criteria, use of the Replacement Parts Evaluation process per CF3.ID13 [10] is an acceptable design change vehicle:

a. The replacement parts are equivalent to the original in form, fit, and function; and
b. The replacement parts do not affect PPS safety function; and
c. The replacement parts do not modify the PPS application program or FPGA or DCPP specific database.

3.2.12.5 System Hardware Modifications

a. The SC shall be responsible at all times to ensure that changes to the physical characteristics and installed configuration of the PPS are accurately documented, as discussed in previous sections of this procedure.

b. If modifications are required due to replacement parts, and are equivalent to the original configuration in form, fit, and function, the RPE process may provide an acceptable design change vehicle. See Section 3.2.12.4.

3.3 Configuration Status Accounting

Configuration Status Accounting (CSA) is a means by which enhancements/changes and new versions/revisions of configuration items are identified, recorded and tracked. Configuration status accounting activities collect data that can be used to measure various aspects of program effectiveness and to assess product completeness and quality.

A CSA system is already established with existing Program Directives (PDs), Inter-Departmental Administrative Procedures (IDAPs) and Department-Level Administrative Procedures (DLAPs). The status of proposed changes will be progressively tracked through approval and implementation in Change Package documentation. These records provide traceability between Configuration Item versions and associated documentation.

3.3.1 Software Release Process

Every approved new software release shall be tagged with a specific version number and committed to the Digital Systems Engineering SourceSafe repository. Revisions will be tagged with an incremented version number.

3.3.2 SCM Metrics Reports

The purpose of SCM metrics is to measure SCM and system status and performance. Data from metrics may also be used to understand problems and inefficiencies in processes, and to provide insight for making necessary corrections and improvements.

The types of metrics reports that portray system health and status include the following:

- Baseline Elements / Device Inventory / Software Version Levels
- Change Request Reporting / Aging / Trends
- Change Process Compliance
- Change Rate / Change Variance / Changes by Severity
- Changed Elements (CIs) / Detailed Changes / Frequently Changed Elements
- CI Compliance History

3.4 Configuration Auditing

Configuration auditing ensures that the technical and administrative integrity of the system is being maintained throughout the lifecycle of the system. Configuration management self-assessments and internal reviews will be conducted annually, at a minimum, to determine to what extent the actual hardware, firmware, software and documentation reflect the required physical and functional characteristics of the system. These activities are formal examinations of the as-built system compared to the as-required system.

The SC shall participate in all baseline assessments and reviews, report any resulting discrepancies, and track any advised corrective actions. Compliance is demonstrated by audit results. The SC may conduct audits at defined project milestones, such as new product

releases and phase upgrades. The SC may also periodically conduct targeted spot check audits, as initiated by complaint or event.

3.4.1 Functional Configuration Audit (FCA)

Per Section 3.5.1 of SCM 99-1 [21], the FCA verifies that the performance of the installed PPS meets the approved requirements specifications. This formal audit is required at the end of all testing just before deployment into a production environment. Test results may serve as validation of functional compliance.

The Surveillance Testing that is performed periodically on the PPS to ensure that it is performing the safety functions mandated by Technical Specifications together with Post Modification Testing per Section 3.2.7.1 are equivalent to the FCA described above. A formal FCA need not be performed.

3.4.2 Physical Configuration Audit (PCA)

The PCA verifies that the actual configuration of the installed PPS matches the documented PPS configuration design. The resulting report of this formal audit may be used to establish the baseline.

The SCM Manuals required by Sections 3.1.4.2 and 3.2.12.1 contain the documented PPS configuration. The SCM Manuals should be audited periodically, to compare the as-built PPS configuration to the documented configuration as described in Section 3.4, above. Discrepancies should be resolved by updating the SCM Manual or correcting the configuration per approved procedures.

3.4.3 Audit Reports

Audit findings detailing the compliance posture of the system are reported to management and communicated to appropriate system team members. Audited items that are not in compliance with the configuration management standards within the SCM Plan are tracked in SAP until they are resolved. Once all discrepancies have been resolved, the audit will be closed.

Audit records shall be retained for at least three calendar years.

4 SCM Schedules

Configuration management activities will occur iteratively throughout the product lifecycle for each system increment and release.

4.1 Project Milestones

- Initial production delivery to operations
- Phased upgrades
- Repairs/Replacement
- Obsolescence/Decommission

4.2 Audit Acceptance Criteria

- SCM policies, procedures and practices are being followed

- Approved changes to hardware, software and documentation are properly implemented
- The as-built documentation of each CI agrees with the as deployed configuration, or that adequate records of differences are available at all times.
- The as-built configuration compares directly with the documented configuration identification represented by the detailed CI specifications.
- Test results verify that each product meets its specified performance requirements to the extent determinable by testing.
- The as-built configuration being installed compares with the final tested configuration. Any differences between the audited configuration and the final tested configuration are documented.
- When not verified by test, the compatibility of products with interfacing products or equipment is established by comparison of documentation with the interface specifications which apply.
- COTS software products are included in formal audit as integral parts of the system baseline.
- A post-audit report is written outlining the specific items audited, audit findings, and corrective actions to be taken. All action items are tracked to closure.

5 SCM Resources

5.1 Software Tools

The following tools are used to manage system configurations at DCPP:

- Microsoft Visual SourceSafe - Archive, retrieval and release of source code, configuration files, backups, disaster recovery files
- Triconex TriStation 1131 Developer's Workbench

The manufacturers may utilize other tools during application development. Such tools are not documented in this Plan because they are not used by PG&E.

5.1.1 Vendor Products

Per CF3.ID16 [9], vendor products selected for implementation must show evidence through test results that they meet functional and physical requirements. Additionally, all vendor products must show a history of reliability, availability and supportability, as required by the project.

The vendor will supply a plan specifying how license agreements, leased products, warranties and vendor support will be transferred to adequately provide for continued maintenance and support of all vendor products throughout the lifecycle of the system. Problems associated with COTS software products are recorded, dispositioned, and corrected with vendor assistance as required.

5.1.1.1 Unmodified COTS Software

Unmodified COTS software is delivered with the vendor's standard documentation package, including historical change data. COTS software upgrades initiated by the vendor are reviewed for acceptability by the responsible SC before they are implemented.

Media and licenses for unmodified COTS software are physically stored in the computer program library. Unmodified COTS software is released by the SC to users in accordance with the provisions of the licensing agreement.

5.1.1.2 Vendor-Modified COTS Software

In some cases, the COTS software vendor is contracted to incorporate changes into COTS software in accordance with Project specifications. COTS software modified by the vendor is delivered with addendum documentation describing the changes from the off-the-shelf product.

Media and licenses for COTS software modified by the vendor are physically stored in the computer program library. Vendor-modified COTS software is released by the SC to users in accordance with the provisions of the licensing agreement.

5.1.1.3 Project-Modified COTS Software

In some cases, the Project will secure the license to modify COTS software and obtain rights to the source code to permit the responsible development organization to modify the COTS software. Project-modified COTS software is maintained by the SC and documented by addendum documentation as necessary to define the changes from the off-the-shelf product.

Media and licenses are physically stored in the computer program library. Project-modified COTS software is released by the SC to users in accordance with the provisions of the licensing agreement.

5.2 Equipment and Techniques

5.2.1 Development/Operating Environments

The Learning Services Simulator Group maintains a training simulator environment and the Digital Systems Engineering Group maintains a development test lab. Software for the training simulator is controlled by the training section. Software for the development test lab is controlled by the SC.

The SC shall distribute copies of all hardware and software modification packages to the training section for their information and use. There are no procedural controls on the software for the Training Unit. Configuration of the Training Unit software will be the responsibility of the training section.

5.2.2 Supporting Infrastructure

The Diablo Canyon file server has a partitioned area on the S-drive reserved for use by Engineering Services.

Electronic documentation and drawing libraries are hosted in the DCPP/HBPP Drawing Library.

Change request notifications and orders are hosted in SAP.

The system software library is hosted on the Digital Systems Engineering Group's SourceSafe server

5.3 Personnel and Training

SCM training requirements shall be per CF2.ID2 [3].

The system coordinator shall ensure that all individuals who will be using the system software have received the level of training necessary to perform the required task. This will include cognizant engineers and technicians.

6 SCM Plan Maintenance

SCMP maintenance is necessary to document software configuration management activities throughout the software lifecycle. If any requirements defined in this document are changed, those changes shall be updated in the SCMP as needed.

Reviews of the SCM Manual shall occur periodically throughout the software lifecycle. At a minimum, an update shall occur concurrently with every major product change. As part of the document review process, a physical walkdown of the system shall be performed to verify and validate the accuracy of the baseline configuration.

All changes to the SCMP and SCM Manuals shall be disseminated to the appropriate user community in a timely manner.

6.1 Oversight

The SC is responsible for monitoring compliance and ensuring that changes and updates are reflected in this Plan and the SCM Manuals as required.

ATTACHMENT 1: SCM Manual Outline

This outline is intended as a guideline. The SCM Manual may be tailored to accommodate the needs of the specific system as long as the content is in compliance with the requirements of this document. Distinctions between Unit 1 and Unit 2 shall be clearly indicated. Refer to SCM-23-01-SR as an example of a completed SCM Manual.

1. System Overview

- Block diagram of basic architecture, such as:
  - Communications
  - External Interfaces
- Drawings and/or photos of physical cabinets/system panels
- Identification of safety-related vs. non-safety-related components
- Applicability to Unit 1 and/or Unit 2

2. Reference Documents

- Requirement Specifications
- Design Specifications
- Applicable ECG & Tech Specs
- Drawings
- User Manuals

3. Hardware Configuration Baseline

- Module model numbers
- Chassis slot positions
- Switch settings
- Network/Communications settings

4. I/O Configuration Baseline

- I/O type, module, slot, channel
- Signal range
- Scaling

5. Software Configuration Baseline

- OS and Application filenames, version, patch levels
- Operation parameters

6. Installation Instructions

- OS services enabled/disabled
- Application custom settings
- Network/Communications setup

7. Disaster Recovery Instructions

- Time-ordered sequence of steps