Enclosure
Attachment 5
PG&E Letter DCL-11-104

Diablo Canyon Power Plant Units 1 & 2 Process Protection System Replacement System Verification and Validation Plan (SyVVP), Revision 0 (LAR Reference 53)

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

Process Protection System (PPS) Replacement
System Verification and Validation Plan (SyVVP)
Nuclear Safety Related

Rev 0

Prepared Sig.	Gregory W Clarkson	Date	10/06/2011
Print Last Name	Clarkson	User ID	NA
Reviewed Sig.		Date	10/06/2011
Print Last Name	Hefler	User ID	JWH3
Coord Sig/Org.	Earl L Quinn	Date	10/06/2011
Print Last Name	Quinn	User ID	NA
Approval Sig.		Date	10/06/2011
Print Last Name	Patterson	User ID	SBP1

ALTRAN SOLUTIONS

REVISION HISTORY

Revision Number	Affected Pages	Reason for Revision
0	All	Initial Issue

Table of Contents

1. Purpose

The purpose of this System Verification and Validation Plan (SyVVP) is to establish the goals, processes, and responsibilities required to implement effective system level verification and validation for the Process Protection System (PPS) Replacement Project at Diablo Canyon Power Plant (DCPP). This SyVVP provides a plan for specifying, evaluating, controlling, and maintaining the overall design for the PPS replacement at Diablo Canyon Power Plant.

The current Eagle 21 PPS is a digital microprocessor-based system. The proposed PPS replacement consists of the microprocessor-based Tricon Programmable Logic Controller (PLC) and the field programmable gate array (FPGA) based Advanced Logic System (ALS). The microprocessor-based Tricon PLC portion of the platform utilizes software to direct the PLC to perform its intended safety-related functions. The ALS portion of the platform is hardware logic-based and does not utilize software.

1.1 Scope

Software used in the Triconex portion of the PPS replacement is Nuclear Safety-Related and requires quality controls to meet SIL 4 as defined in IEEE-1012-1998 [2.1.2.25]. The Triconex product development process is specifically tailored to development of software used in designing and maintaining programmable logic devices (PLDs). The FPGA-based ALS does not utilize a microprocessor and does not execute software. However, the FPGA is configured using software tools; therefore a quality control procedure must be used in the development of the FPGA.

This SyVVP describes activities performed by the three responsible parties: PG&E, Invensys Operations Management (IOM), and Westinghouse/CS Innovations, LLC (CSI). The Triconex portion of the PPS replacement is provided by IOM. The ALS portion is provided by CSI.

Both suppliers have 10 CFR 50 Appendix B QA programs. Respective V&V activities are governed by the Triconex Nuclear Safety-Related Process Protection System Replacement DCPP Software V&V Plan (SVVP) [2.2.2.4], the ALS VV Plan [2.2.2.1], the ALS DCPP Management Plan [2.2.2.2], and the ALS DCPP Test Plan [2.2.2.3]. These plans have been reviewed and accepted by PG&E to ensure that the V&V effort is complete.

This SyVVP implements guidance described in IEEE Standard 1012-1998, Software Verification and Validation Plans [2.1.2.25] as relevant to the PPS Replacement Project.

1.2 Goals

PG&E will perform initial Concept phase development activities as described later in this SyVVP. The outputs of this phase will be utilized by the 10 CFR 50 Appendix B suppliers in accordance with their approved procedures to develop, implement, and test the respective systems. The supplier activities and products will be traceable to the PG&E design input documents. The 10 CFR 50 Appendix B suppliers will verify and validate their respective systems to ensure that all safety functions are traced to their requirements and are acceptable per their respective control procedures.

PG&E will review and accept the products of the 10 CFR 50 Appendix B supplier development and implementation V&V activities and will use the results to complete the overall PPS Replacement Project V&V activities. Upon completion of all V&V activities PG&E will issue a final System Verification and Validation Report (SyVVR).

2. Reference Documents

2.1 Developmental References and Standards

2.1.1 Regulatory Standards

2.1.1.1 U.S. Regulatory GuidanceNUREG-0800 BTP 7-14, Branch Technical Position: Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, Revision 5, March 2007.

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

2.1.1.3 NUREG/CR-6430, Software Safety Hazards Analysis, February 1996.

2.1.1.4 Regulatory Guide 1.118, Periodic Testing of Electric Power and Protection Systems, Revision 3, April 1995

2.1.1.5 Regulatory Guide 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Revision 3, July 2011.

2.1.1.6 Regulatory Guide 1.153, Criteria for Safety Systems, Revision 1, June 1996

2.1.1.7 Regulatory Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Revision 1, February 2004

2.1.1.8 Regulatory Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

2.1.1.9 Regulatory Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

2.1.1.10 Regulatory Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

2.1.1.11 Regulatory Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

2.1.1.12 Regulatory Guide 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, September 1997

2.1.1.13 Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Revision 1, November 2002

2.1.1.14 Interim Staff Guide DI&C-ISG-01, Cyber Security, Revision 0

2.1.1.15 Interim Staff Guide DI&C-ISG-02, Diversity and Defense-in-Depth Issues, Revision 2, June 2011

2.1.1.16 Interim Staff Guide DI&C-ISG-04, Highly Integrated Controls Rooms-Communications Issues (HICRc), Revision 1, March 2009

2.1.1.17 Interim Staff Guide DI&C-ISG-06, Licensing Process, Revision 1, January 2011

2.1.2 Industry Standards

2.1.2.1 Industry Codes and StandardsANSI/IEEE Std. 983-1986, IEEE Guide for Software Quality Assurance Planning

2.1.2.2 ANSIIISO/ASQ Q9001-2000, Quality management systems - Requirements

2.1.2.3 ANSI/ISO/ASQ Q9004-1-1994, Quality Management and Quality System Elements - Guidelines

2.1.2.4 ASME NQA-1-1994, 1997, Quality Assurance Requirements for Nuclear Facility Applications

2.1.2.5 EPRI TR-103291, Handbook of Verification and Validation for Digital Systems, Revision 1, December 1998

2.1.2.6 EPRI TR-108831, Requirements Engineering for Digital Upgrades

2.1.2.7 NEI 08-09, Revision 6, Cyber Security Plan for Nuclear Reactors

2.1.2.8 IEEE Std. 7-4.3.2-2003 IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Appendix D (Informative) Identification and Resolution of Hazards

2.1.2.9 IEEE Std. 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations

2.1.2.10 IEEE Std. 308-1971, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations

2.1.2.11 IEEE Std. 323-1974, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

2.1.2.12 IEEE Std. 338-1987, IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems

2.1.2.13 IEEE Std. 344-1987, Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

2.1.2.14 IEEE Std. 379-1977, IEEE Application of Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems

2.1.2.15 IEEE Std. 384-1981, IEEE Trial-Use Standard Criteria for Separation of Class 1E Equipment and Circuits

2.1.2.16 IEEE Std. 352-1987, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

2.1.2.17 IEEE Std. 497-2002, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

2.1.2.18 IEEE Std. 577-1976, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations

2.1.2.19 IEEE Std. 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

2.1.2.20 IEEE Std. 730-2002, Standard for Software Quality Assurance Plans

2.1.2.21 IEEE Std. 828-1998, Software Configuration Management Plans

2.1.2.22 IEEE Std. 829-1983, Standard for Software Test Documentation

2.1.2.23 IEEE Std. 830-1993, Recommended Practice for Software Requirements Specifications

2.1.2.24 IEEE Std. 1008-1987, IEEE Standard for Software Unit Testing

2.1.2.25 IEEE Std. 1012-1998, Standard for Software Verification and Validation

2.1.2.26 IEEE Std. 1016-1997, Recommended Practice for Software Design Descriptions

2.1.2.27 IEEE Std. 1028-1997 (reaffirmed 2002), Standard for Software Reviews

2.1.2.28 IEEE Std. 1042-1987, ANSI/IEEE Standard Guide to Software Configuration Management

2.1.2.29 IEEE Std. 1044-1997, IEEE Standard for Classification of Software Anomalies

2.1.2.30 IEEE Std. 1058.1-1991, IEEE Standard for Software Project Management Plans

2.1.2.31 IEEE Std. 1058-1998, IEEE Standard for Software Project Management Plans

2.1.2.32 IEEE Std. 1061-1998, IEEE Standard for a Software Quality Metrics Methodology

2.1.2.33 IEEE Std. 1063-1987, Standard for Software User Documentation

2.1.2.34 IEEE Std. 1074-1995, IEEE Standard for Developing Software Life Cycle Processes

2.1.2.35 IEEE Std. 1219-1998, Standard for Software Maintenance

2.1.2.36 IEEE Std. 1228-1994, IEEE Standard for Software Safety Plans

2.1.2.37 IEEE Std. 1233-1998, Guide for Developing System Requirements Specifications

2.1.2.38 IEEE Std. 1471-2000. Systems and Software Engineering – Recommended Practice for Architectural Description of Software-Intensive Systems

2.2 Control Procedures

2.2.1 PG&E Control Procedures

2.2.1.1 DCPP References and Procedures:PG&E Procedure, IDAP AD7.ID8, Project Management

2.2.1.2 PG&E Procedure, IDAP CF3.ID9, [Design Change (Package) Development

2.2.1.3 PG&E Procedure, IDAP CF2.ID9, Software Quality Assurance Plan Software Development

2.2.1.4 PG&E Procedure, IDAP CF2.ID2, Software Configuration Management for Computers & Software Used for Plant Operations and Operations Support

2.2.2 10 CFR 50 Appendix B Supplier Control Procedures

2.2.2.1 CS Innovations Document No. 6002-00003, "ALS VV Plan"

2.2.2.2 CS Innovations Document No. 6116-00000, "DCPP Management Plan"

2.2.2.3 CS Innovations Document No. 6116-00005, "DCPP Test Plan"

2.2.2.4 Triconex Document No. 993754-1-802, Nuclear Safety-Related Process Protection System Replacement DCPP Software V&V Plan (SVVP)

NOTE: The various 10 CFR 50 Appendix B software suppliers and the various regulatory agencies do not use the same terminology for software and software verification and validation. As mentioned in DI&C-ISG-06 Rev. 1 [2.1.1.17], an applicant may have different names for similar documents. Regardless of the titles of the documents submitted, the actual LAR should contain sufficient information to address the criteria discussed in the technical evaluation sections... This procedure does not specify that an approved software supplier meet this particular terminology, only that the intent of this procedure is followed and a high quality software product is generated for plant use.

NOTE 2: If any part of the software life cycle process is contracted to an approved supplier with a 10CFR50 Appendix B program, their SQA processes apply for their product, with PG&E auditing their program, and owner acceptance by PG&E.

3. Definitions

Acceptance	Official recognition that a product (usually hardware or software configuration item) meets contractual and project requirements.
Acceptance Test	A Formal test conducted in an operational environment to determine whether or not the system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system.
Accuracy	The degree of freedom from error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output.
Anomaly	Any condition that deviates from the expected based on requirements, specifications, design, documents, user documents, standards, etc.
Application Software	Software designed to fulfill specific needs of a user; for example, software for navigation, or process control.
Approval	Official recognition of product validity.
Architecture	The organizational structure of a system or component.
Baseline	• A specification or product that has been formally reviewed and agreed upon, and thereafter serves as the basis for further development. It is changed only through formal change-control procedures • A complete and documented set of design requirements and system components (hardware and software) placed under configuration control that identifies the applicable version/revision level of each of these requirement documents and system components. • Work products (e.g., document and/or software) that have been officially approved or accepted and used to judge the acceptability of a system, Subsystem, or configuration item. (A baseline is subject to configuration control and is updated to reflect approved changes to the configuration item throughout its life cycle.)
Build	Intermediate version of a system or configuration item that provides a demonstrable subset of capabilities needed to meet requirements allocated to the system or configuration item.
Completeness	Those attributes of the planning documents, implementation process documents and design outputs that provide full implementation of the functions required of the software. The functions that the software is required to perform are derived from the general functional requirements of the safety system and the assignment of functional requirements to the software in the overall system design.
Component Testing	Testing conducted to verify the correct implementation of the design and compliance with program requirements for one software element (e.g., function block) or a collection of software elements

Correctness	The degree to which a design output is free from faults in its Specification, design, and implementation. There is considerable overlap between correctness properties and properties of other characteristics such as accuracy and completeness.
Conceptual Phase	Encompasses those activities that are necessary to produce the basic design and functional requirements for the project or system. The conceptual phase identifies the idea or need for a software application including feasibility studies. It establishes the scope, basic design criteria, required effort, cost, functionality, and classification of the software.
Configuration	Form, fit, and functions of a system or configuration item as defined in baseline documentation.
Configuration Audit	In the context of an audit for delivery of a product, a configuration audit includes both a functional configuration audit and a physical configuration audit.
Configuration Item	• An aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process. The collection of configuration items should encompass all data, code, drawings, and other information that is used to configure, maintain, or define the operation or configuration of the designated equipment and the project application. • Developed or purchased item, controlled, accepted, and maintained separately from other items. (A configuration item can be composed of hardware or software or, for major configuration items, an aggregation of both.)
Configuration Management	A discipline that involves identifying, controlling, and tracking the configuration of a system or product.
Corrective Action	Corrective action is taken to eliminate the causes of an existing nonconformity, defect, or other undesirable situation in order to prevent recurrence.
Criticality	A subjective description of the intended use and application of the system. Software criticality properties may include safety, security, complexity, reliability, performance, or other characteristics.
Criticality Analysis	A structured evaluation of the software characteristics (e.g., safety, security, complexity, performance) for severity of impact of system failure, system degradation, or failure to meet software requirements or system objectives.
Deliverable	A work product or service given to the client for review and acceptance. It frequently has contractual implications.

Design Phase	Encompasses those activities that are necessary to produce the Software Design Description for the project or system. The primary activity is encoding the application information and function definitions of the Software Requirements Specification into function diagrams. Design Descriptions are the translation of the Requirements Specification into the design and development of the software.
Factory Acceptance Testing (FAT)	Final customer-witnessed or customer–performed testing at supplier's site which demonstrates that the designed system meets the purchaser's functional and performance requirements and/or industry and regulatory requirements.
Firmware	Computer programs and data loaded in a class of memory that cannot be dynamically modified by the computer during processing, e.g., EPROM.
Functional Requirement	Requirement on the I&C system from point of view of the process function. The functional requirements usually are given in the form of written descriptions (customer functional specifications) and information flow diagrams.
Functional Testing	Tests whether the functions of the I&C system fulfill the software requirements. In the case of safety-related I&C equipment these tests are performed by simulating the measurement signals that prevail during normal or accident conditions in order to check that protective actions are initiated correctly.
Functionality	The operations, which must be carried out by the software. Functions generally transform input information into output information. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.
Hardware	Physical equipment (components) that typically provide a specific function and is assembled with other equipment to create a system; certain components host the various types of Software or Firmware
Hazards Analysis	A systematic qualitative or quantitative evaluation of software for undesirable outcomes resulting from the development or operation of a system. These outcomes may include injury, illness, death, mission failure, economic loss, property loss, environmental loss, or adverse social impact. This evaluation may include screening or analysis methods to categorize, eliminate, reduce, or mitigate hazards.
I&C Function	The formal specification of the functional behavior of the I&C equipment, as derived from the functional requirements. I&C functions are specified and described in the SRS, as information flow diagrams and data tables, and form the basis for automatic software generation in application software development.

Implementation Phase	Encompasses those activities that are necessary to generate the code from the completed function diagrams or source code and load it onto the processors. This includes documenting the steps and matching specific checksums for identity checking.
Independence	Organization whose personnel maintain independence from a Technical, Managerial, and Financial perspective: • Technical Independence is defined as personnel who are not involved in the development of the software. • Managerial Independence is defined as an organization separate from the development and program management organizations. Managerial independence also means that the independent organization selects the segments of the software and the system to analyze and test, choose techniques, defines testing schedule, and selects the specific technical issues and problems to act upon. The independent organization effort must be allowed to submit to program management the testing results, anomalies, and findings without restrictions or adverse pressure, direct or indirect, from the development group. • Financial Independence is defined as an organization that is financially independent from the development organization. This independence prevents situations where independent activities cannot be completed because funds have been diverted or adverse financial pressures or influences have been exerted by the development organization.
Independent Design Review	A detailed line by line technical verification of a document by a competent individual other than the preparer. The independence and technical competence of the reviewer is certified by the cognizant technical manager. This is performed by the design group personnel, is not part of the software verification and validation process, and may also be referred to as Independent Review.
Inspection	Evaluation technique in which intermediate development products are examined in detail by a person or group other than the author to detect technical deficiencies or violations of standards.
Integration Testing	An orderly progression of testing in which software elements, hardware elements or both are combined and tested until the entire system has been integrated. The final set of testing, completed successfully, before the FAT which demonstrates that the system (integrated hardware and software) is ready for FAT.
Integrity Level	The assigned integer value from 0 to 4 that indicates the degree of verification and validation that is applied to the system during the development life cycle, subsequent to an evaluation of a combination of the criticality of the system function to the owner's mission, and the importance and likelihood of a system failure. For larger systems, this level may be applied to specific subsystems or sub-modules.

Interface	A shared boundary across which information is passed. A Hardware or Software component that connects two or more other components for passing information from one to the other.
Interface Control	• Identification of all functional and physical characteristics relevant to the interfacing of two or more Configuration Items provided by one or more organizations • Ensuring that proposed changes to these characteristics are evaluated and approved prior to implementation.
Lessons Learned	Lessons learned are guidance that enhance the practitioner's understanding of a process, clarify a process' applicability to a particular application, provide guidance for special cases, highlight issues, or convey supplier advice. The lessons learned come from a variety of sources including, but not limited to, operation experience, experiences in the use of tools and techniques, and published best practices from other organizations.
Malicious Software	Software code that is intended to breakdown or bypass security barriers; or software code that is intended to adversely impact proper system performance or function.
May	An expression of possibility, a permissive choice to act or not, as distinguished from shall, which is a requirement or action that must be performed.
Measure	A measure is any quantitative group. Examples of measures are estimated cost, actual cost, ratio of actual to estimated cost, number of defects, defect density, mean time between failures, average length of support call, and number of peer reviews performed.
Peer Review	An examination of a product by the creators' peers to identify defects and areas where changes are needed. It uses the capabilities of independent reviewers, individually or in a group, to identify the improvements needed in a product and to agree on which improvements should be made.
Product Review	An examination of a product to identify errors before the product is formally passed forward in the development process.
Project Manager	Individual responsible to coordinate all aspects of the assigned project(s). Primary customer interface responsible for coordinating implementation of the project, quality control, customer invoicing and tracking project performance against as- sold estimates.
Quality	Degree to which a system or configuration item satisfies its requirements.
Quality Management	Consists of the management responsibilities and actions that determine and implement quality policies. It includes obtaining the commitment of the organization, marshaling resources, and ensuring that quality management processes are used and supported effectively.

Release	A build that will be delivered to the customer. A release may include an integrated set of builds.
Reliability	The degree to, which a software system or component operates without failure. This definition does not consider the consequences of failure, only the existence of failure.
Requirements Phase	Encompasses those activities that are necessary to produce the Software Requirements Specification (SRS) for the project or system. These are the primary software design activities wherein customer requirements are identified and described, and documented in a manner necessary for the specification of function diagrams. The Requirements Specification is the building block for the development, procurement, and maintenance of software and data. As such it is important the Requirements Specification is created considering all the requirements for the software/data.
Requirements Traceability	The process of verifying that each specified requirement for a system has been implemented into the design, that all aspects of the design have their bases in the specification requirements (forwards and backwards traceability, respectively), and that testing produces results compatible with the specified requirements. The completed steps of the verification process are typically recorded in a Requirements Traceability Matrix (RTM). This usually takes the form of a table that lists requirements and the corresponding sections of documents that indicate how the particular requirement is satisfied.
Requirements Traceability Matrix (RTM)	A Requirements Matrix provides a method that can be used to trace and document that requirements have been met. It provides a complete view of requirements to be tested, and traces specific requirements through all phases of development to verify that the requirement was met. Additionally, the RTM formally documents the process and provides documented evidence that can be useful in auditing that safety requirements and licensing commitments were met.
Review	An expert analysis and evaluation of the results of a task, a step, or a phase. It is implemented either globally, or in detail on random samples (e.g., in the case of code inspection).
Safety	Those properties and characteristics of the software system that directly affect or interact with system safety considerations. The safety characteristic is primarily concerned with the effect of the software on system hazards and the measures taken to control those hazards.
Security	The ability to prevent unauthorized, undesired, and unsafe intrusions. Security is a safety concern insofar as such intrusions can affect the safety-related functions of the software.
Shall	"Shall" denotes a requirement or action that must be performed.
Should	"Should" denotes a requirement or action that would be beneficial to SUPPLIER or OWNER but is not mandatory within the PPS scope of work.

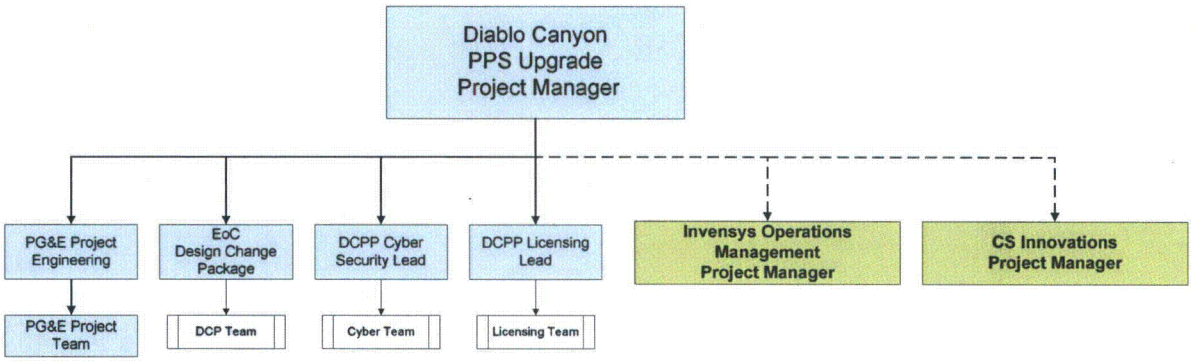
Software	The programs, procedures and any associated documentation pertaining to the operation of a data processing or computing system. Software is an intellectual creation, independent of the medium on which it is stored. Software includes firmware and logic developed from software based developments systems.
Software Component	Software components are a constituent element of a software system. For application software, this usually means the modules, sub-modules, or I&C functions as described in the SRS. A specific collection of Software Components is assembled to form a System Component.
Software Lifecycle	The period of time that starts when a software product is conceived and ends when the software product is no longer available for routine use. Includes the following phases: preliminary engineering (conceptual), requirements, detailed design, implementation, integration, testing, installation and checkout, operations & maintenance, and sometimes a retirement phase.
Software Requirements	Software requirements are those that must be met by the software to satisfy a contract, standard, specification, procedure, or user need. The set of all software requirements form the basis for subsequent development of the software. Requirements include, but are not limited to: identification of needed software functions, the inputs, processes, and outputs required for each function, the design constraints and attributes of the software, performance requirements, interface requirements, and development standards. Each requirement is defined such that its achievement can be verified and validated objectively.
Software Tool	A computer program used in the development, testing, analysis, or maintenance of a program or its documentation. Examples include comparator, cross-reference generator, decompiler, driver, editor, flowcharter, monitor, test case generator, and timing analyzer.
Surveillance	A formal review of a process implementation against a documented standard or process. Surveillance is a planned activity that focuses on a project or a functional area.
System	The hardware and software required for solving a complex task. It consists of several subsystems or components which have different performance characteristics but which are suitable for use together to accomplish the required functions.
System Component	System components are the equivalent of a subsystem that can be used separately and performs a self-contained function. They consist of one or more modules, which are suitable for use together in an overall system. In the documentation, emphasis is placed on functionality, communication relationships, sequences, inputs/outputs and common resources.
System Test	System tests are used to determine whether the specified system characteristics of equipment (behavior on failure, behavior on start-up, testability, etc.) have been implemented. These types of test are performed without regard to the specific I&C function.

Task Iteration	The repeat of a V&V task which occurs as a result of identification of an anomaly, its resolution, and the verification by the V&V team that the resolution is complete.
Test	Sequence of events designed to verify that a system or configuration item satisfies requirements or to identify differences between expected and actual results.
Test Phase	Encompasses those activities that are necessary during the application software production process to assemble and integrate the complete system, and to perform required testing. These are the primary software design activities wherein system performance is checked and documented to ensure the required functions are correctly and completely implemented.
Timing	The ability of the software system to achieve its timing objectives within the hardware constraints imposed by the computing system being used.
Traceability	The degree to which each element of one life cycle product can be traced forward to one or more elements of a successor life cycle product, and can be traced backwards to one or more elements of a predecessor life cycle product. Traceability is central to the production of complex systems to ensure all requirements are implemented, checked and tested.
Unit	Smallest replaceable element in a configuration item also referred to as a configuration unit (CU). For software, a unit is typically a subroutine; for hardware, a unit may be a board that is fabricated as a separate item.
Validation	The evaluation of a product at the end of the development process to ensure the product complies with previously specified software requirements. This process is usually performed by testing. Validation involves evaluating the overall system and software behavior under conditions representative of its intended use.
Verification	The process of determining whether or not the products of a given development phase fulfill the requirements imposed at the start of the phase. Verification includes detailed review and testing at each phase and determines whether the project is ready to proceed to the next phase.
Verification and Validation	The systematic program of review and testing activities performed through the software lifecycle to ensure that the software satisfies its intended use and user needs. V&V activities are performed by persons who are different and independent from those who accomplish the design and integration.
Verifiability	The degree to, which a software planning document, implementation process document or design output is stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses, reviews, or tests to determine whether those criteria have been met.
Will	"Will" means that an action or activity can be assumed to be completed by the subject of the sentence whether the subject is SUPPLIER, OWNER or others.

4. Organization

Different organizational units, their responsibilities and relationships with regard to Verification and Validation are discussed in this SyVVP. The basic organizational structure for the PPS Replacement System project is shown in Figure 4-1.

Figure 4-1 PPS Project Organization



4.1 PG&E Roles & Responsibilities

Detailed PG&E roles and responsibilities are defined in control procedures listed in Section 2.2.

The PG&E Project Manager has the ultimate responsibility, authority, and accountability for all aspects of the project. Responsibilities include quality of design, timely integration with site schedules, supplier quality management/oversight, quality field implementation, and successful post-installation testing. The Project Manager is also responsible to recommend re-evaluation of the project if he detects changes in the project that alter the decision to proceed.

The PG&E Project Manager shares the responsibility for meeting the software quality goals and objectives of the project and for the implementation of software quality management throughout the project.

The PG&E Project Manager will:

- Release the system level V&V plan and reports
- Review progress of the SyVVP and V&V program
- Approve corrective actions, scope changes and resource allocations.
- Coordinate the disposition of discrepancy reports generated in the course of verification and validation.

The Engineer of Choice (EoC) Design Change Package Team is responsible for the design change process utilized by DCPP for the design and implementation of modifications to controlled Structures, Systems, and Components. The Engineer of Choice (EoC) Design Change PackageTeam is also responsible for establishing quality goals and objectives for their organization consistent with those of the project.

The PG&E Project Engineering Team conducts and ensures quality-related inter-group coordination for design and engineering between software and hardware design activities. Project engineering is responsible for identifying the processes and corresponding standards and procedures to guide project

performance. The project engineering team is further responsible for ensuring work activities are performed in compliance with these standards and procedures.

4.2 10 CFR 50 Appendix B Supplier Roles and Responsibilities

Detailed roles and responsibilities for each of the 10CFR50 Appendix B suppliers are provided in the respective 10CFR50 Appendix B supplier control procedures listed in Section 2.2.2.

The 10 CFR 50 Appendix B Supplier Project Manager (PM) is responsible for providing direction in implementation of the V&V activities to ensure that they are performed per the respective control procedures listed in Section 2.2.2. The Project manager is responsible for overall project safety in the respective organization.

The 10CFR50 Appendix B supplier produces documentation and is responsible for the performance of the reviews, audits, and inspections as described in the control documents. PG&E will review the documents and products produced and witness testing activities. PG&E will accept the documeents and reports after the 10 CFR 50 Appendix B suppliers resolve anomalies and PG&E comments.

5. V&V Processes

The PG&E SyVVP and 10CFR50 Appendix B supplier SVVP describe documents, hardware and software V&V tools, techniques, methods, and operating and test environment to be used in the respective V&V process.

During the Project Initiation and Planning activities the lifecycle documentation needed to support the LAR was identified, and is shown in **Figure 5-1**. Additional detail regarding each of the illustrated documents will be provided in the System Quality Assurance Plan (SyQAP) and System Verification and Validation Plan (SyVVP).

5.1 PG&E V&V Tasks

5.1.1 Concept Phase V&V

During the Concept phase, the system architecture is selected, and system requirements are allocated to hardware, software, and user interface components. The outputs of the Concept phase, shown in **Figure 5-1** are:

1. Conceptual Design Document (CDD)
2. Functional Requirements Specification (FRS - includes Function Block Diagrams)
3. Interface Requirements Specification (IRS - includes Input/Output List)

Development of concept documentation and allocation of resources was performed for the PPS Replacement Project per PG&E procedure CF2.ID9 [2.2.1.3], which includes verification of the Concept phase documents through a signature process involving all stakeholders. There are no specific V&V products of this phase.

PG&E considers the CDD to be a descriptive document, not a design input document. Taceability by the 10 CFR 50 Appendix B suppliers from the CDD to the FRS and IRS is not required.

5.1.2 Installation and Checkout Phase V&V

The Installation and Checkout phase begins after PG&E has reviewed and accepted all development phase documentation and V&V reports, including the 10 CFR 50 Appendix B supplier Software (or System) V&V Report (SVVR), that have been prepared per the control documents listed in Section 2.2.2.

5.1.2.1 Project Integration

The 10 CFR 50 Appendix B supplier FAT will verify that the respective systems correctly process all safety-related and non-safety-related analog and discrete inputs and outputs. The FAT will verify that all safety functions specified in the PG&E design documents (FRS and IRS) perform in accordance with specified requirements. The FAT will also verify operation of the non-safety-related Maintenance Workstation (MWS) functions associated with each platform per specified requirements.

However, the 10 CFR 50 Appendix B suppliers will implement their respective systems in different facilities with different physical locations, and without access to external PG&E non-safety-related systems, such as the Plant Process Computer Gateway. Necessarily, the FAT will not include end-to-end tests of functions that involve such dependencies. The completed systems will be assembled in the PG&E Project Integration and Test (PIT) facility for pre-installation staging and checkout of the integrated system.

The ALS processes Reactor Coolant System and Pressurizer Vapor Space temperatures and provides scaled analog 4-20 mA signals corresponding to Engineering Units to the Tricon. The ALS FAT will verify that the ALS processes the temperature signals correctly and produces properly scaled 4-20 mA analog outputs per specified requirements. The Tricon FAT will verify that all safety functions utilizing the 4-20 mA analog signals perform per specified requirements using simulated signals. The SAT will test the integrated PPS replacement system using the transmission of live 4-20 mA analog Reactor Coolant System temperatures from the ALS to the Tricon.

5.1.2.2 Site Acceptance Test

The PG&E Site Acceptance Testing (SAT) will test the fully integrated system prior to installation. The SAT does not retest safety functions. All specified safety functions will be tested in the 10 CFR 50 Appendix B supplier FAT. As described above, the SAT will test the transmission of live analog data from the ALS to the Tricon and will also include V&V of the non-safety-related communication interfaces with the MWS and external systems as specified in the IRS.

Tasks performed in this phase:

- Audit the installation configuration to verify that all products required to integrate the system have been delivered by the 10 CFR 50 Appendix B suppliers and that all ancillary components are available.
  - For the software based Tricon portion of the PPS replacement, verify that the installed software corresponds to the software subjected to V&V. Verify that the system initializes, execute, and terminates as specified. Verify the requirements for continuous operation and service, including user notification of errors.
  - For the hardware based ALS portion of the PPS replacement, verify that the installed FPGA logic corresponds to the logic subjected to V&V. Verify that the system initializes, executes, and terminates as specified. Verify the requirements for continuous operation and service, including user notification of errors.
- Validate that all site-dependent parameters or conditions to verify supplied values are correct.
- Conduct the SAT per approved PG&E plant procedure.

5.1.2.3 Installation and Design Verification Test

The Design Verification Test (DVT) is performed on the system once it is fully installed in the final target environment and location. The DVT is performed per PG&E plant procedure CF3.ID9 [2.2.1.2]. PG&E is responsible for acceptance of the results of the SAT and DVT.

Tasks performed in this phase:

- Audit the installation configuration to verify that all software products required to correctly install and operate the completed system are present in the installation package.
- Validate that all site-dependent parameters or conditions to verify supplied values are correct.
- Conduct the DVT per approved PG&E plant procedure.
- Verify that the installation procedures and installation environment do not introduce new hazards; Update the hazard analysis;
- Generate the V&V Final Report

  PG&E will review and accept the products of the Appendix B supplier development and implementation V&V activities and will use the results to ensure that the overall PPS Replacement Project V&V activities are complete. Upon completion of all V&V activities, tasks, and results, including status and disposition of anomalies, PG&E will issue a final System Verification and Validation Report (SyVVR).

5.1.2.4 Traceability Analysis

PG&E will prepare a Requirements Traceability Matrix (RTM) to document the verification and validation of specified requirements that were not included in the respective 10 CFR 50 Appendix B supplier V&V scope.

5.1.2.5 Outputs of this phase are:

- Site Acceptance Test Report
- V&V Installation Analysis
- Design Verification Test Report.
- RTM for items not in 10 CFR 50 Appendix B supplier V&V scope.
- SyVVR

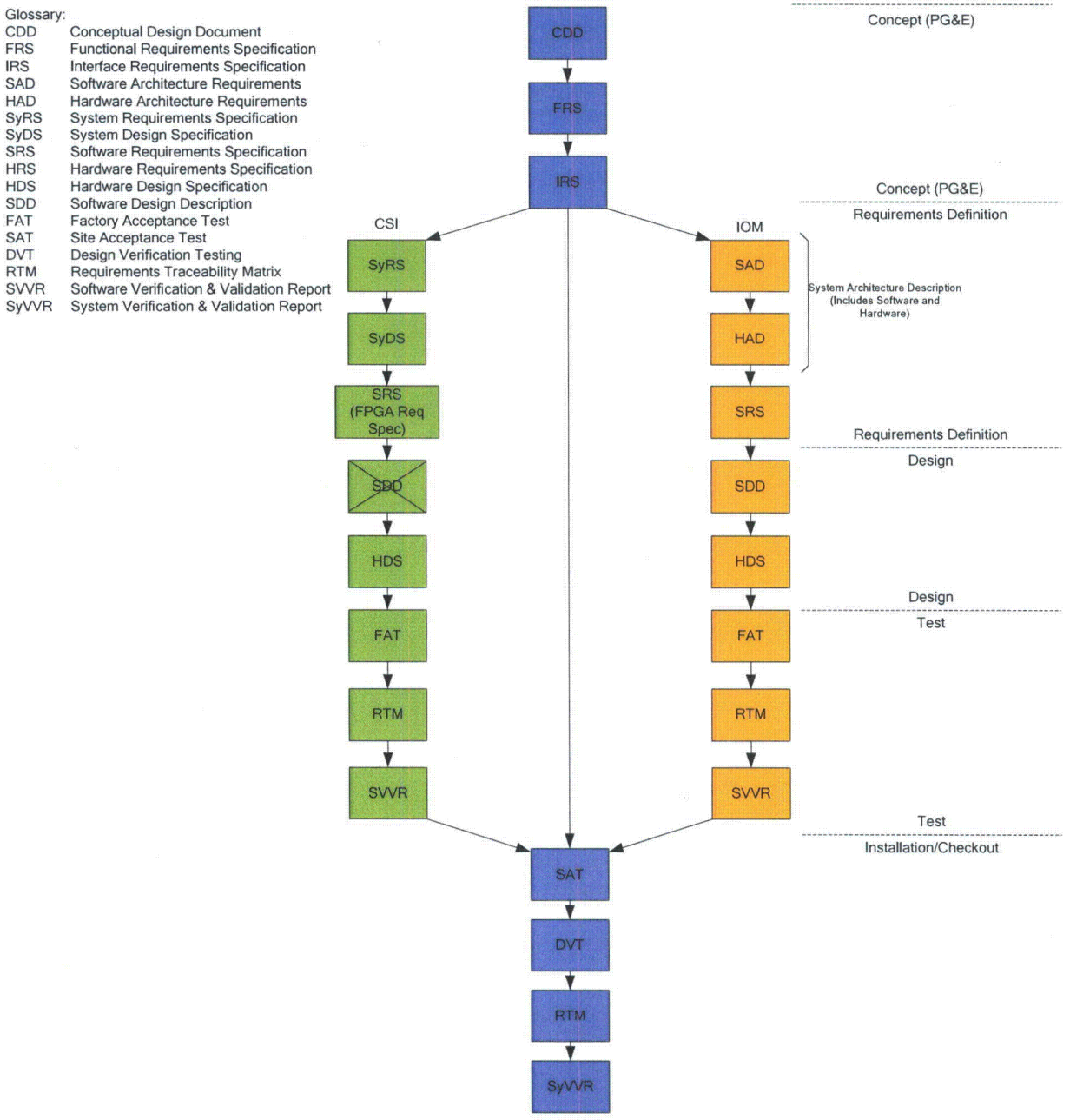
5.1.3 Operation Phase V&V Tasks

Not in the scope of this SyVVP; governed by other approved DCPP procedures

5.1.4 Maintenance Phase V&V Tasks

Not in the scope of this SyVVP; governed by other approved DCPP procedures

Figure 5-1 PPS Replacement Project Lifecycle Document Flow



5.2 10CFR50 Appendix B Supplier Tasks

Respective V&V activities are governed by the Triconex Nuclear Safety-Related Process Protection System Replacement DCPP Software V&V Plan (SVVP) [2.2.2.4], the ALS VV Plan [2.2.2.1], the ALS DCPP Management Plan [2.2.2.2], and the ALS DCPP Test Plan [2.2.2.3]. These plans have been reviewed and accepted by PG&E to ensure that the V&V effort is complete.

During requirements definition, design and implementation activities, the 10 CFR 50 Appendix B suppliers will issue reports for the results of V&V activities. PG&E will review and accept the reports after comments and any anomalies have been resolved according to the 10 CFR 50 Appendix B supplier procedures.

The 10 CFR 50 Appendix B suppliers will prepare traceability documentation and analyses for the starting from the FRS and IRS and continuing through Factory Acceptance Testing (FAT) per their respective control procedures. The 10 CFR 50 Appendix B suppliers will verify and validate their respective systems to ensure that all safety functions are traced to their requirements and perform per the specified requirements in accordance with the respective control procedures. This process ensures that all safety requirements specified in the FRS and IRS are properly implemented and tested at the FAT.

The 10 CFR 50 Appendix B suppliers will issue a final V&V Report,(SVVR) which summarizes all life cycle V&V tasks and the task results. It will also summarize the discrepancies and their resolution found during the V&V evaluation. The report will give an assessment of overall software quality and provide any recommendations. The SVVR will be prepared per the respective control procedures.

6. V&V Reporting Requirements

V&V reporting shall consist of Task Reports, V&V Activity Summary Reports, Anomaly Reports, and the V&V Final Report. Task report(s), V&V activity summary report(s), and anomaly report(s) are provided as feedback to the software development process regarding the technical quality of each software product and process.

Task Reports shall document V&V task results and status, and shall be in a format appropriate for technical disclosure. Task Report requirements are defined in the respective 10 CFR 50 Appendix B supplier control procedure.

An Activity Summary Report shall summarize the results of V&V tasks performed for each of the V&V activities. V&V Activity Summary Report requirements are defined in the respective 10 CFR 50 Appendix B supplier control procedure,

An Anomaly Report shall document the identification and resolution of all anomalies detected by the V&V effort. Anomaly reporting and resolution requirements are defined in the respective PG&E and 10CFR 50 Appendix B supplier control procedures.

The V&V Final Report, consisting of the System V&V Report (SyVVR), will be issued by PG&E at the end of the installation and checkout phase. The V&V Final Report will include the following, as a minimum:

a. Summary of all life cycle V&V activities within PG&E and 10 CFR 50 Appendix B supplier scope
b. Summary of anomalies and resolutions
c. Assessment of overall software quality
d. A copy of or reference to all completed V&V documents and reports

7. V&V Administrative Requirements

Anomaly Resolution and Reporting shall be performed per the respective PG&E and 10CFR 50 Appendix B supplier control procedures.

Task iteration evaluation and disposition shall be performed in accordance with the PG&E and 10CFR50 Appendix B supplier control procedures.

V&V Task Reports shall be generated to document the results of regression testing per the PG&E and 10CFR50 Appendix B supplier control procedures.

The procedures and criteria used to deviate from this SyVVP are defined as follows. The information required for disposition of deviations shall include task identification, rationale, and potential effect on software quality. The authority responsible for approving deviations is the PG&E Project Manager. Approval shall be documented in a Change Notice or equivalent formal PG&E document, and shall be incorporated into the SyVVP as a revision at the first practical opportunity.

Control Procedures: Refer to Section 2.2.1 (PG&E) and Section 2.2.2 (10 CFR 50 Appendix B suppliers)

Standards, Practices and Conventions: Refer to Section 2.1.

8. V&V Documentation Requirements

V&V documentation shall be prepared in accordance with the PG&E and 10 CFR 50 Appendix B supplier control procedures.