Enclosure
Attachment 4
PG&E Letter DCL-11-104

Diablo Canyon Power Plant Process Protection System (PPS) Replacement System Quality Assurance Plan (SyQAP), Revision 0 (LAR Reference 52)

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

Process Protection System (PPS) Replacement
System Quality Assurance Plan (SyQAP)
Nuclear Safety Related

Rev 0

Prepared Sig.	Greg W Clark	Date	9/19/2011
Print Last Name	Clarkson	User ID	N/A
Reviewed Sig.	[signature]	Date	9/19/2011
Print Last Name	Heald	User ID	JWH3
Coord Sig/Org.	Edward Quinn	Date	9/22/11
Print Last Name	QUINN	User ID	N/A
Approval Sig.	[signature]	Date	9/27/11
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

1.1 Overview

The purpose of this System Quality Assurance Plan (SyQAP) is to establish the goals, processes, and responsibilities required to implement effective software quality management for the Process Protection Set (PPS) system software at Diablo Canyon Power Plant (DCPP), ensure any required software functions perform correctly, and that the required software functions conform to established technical requirements, conventions, rules, and standards. To achieve this goal, software development will proceed in a traceable, planned, and orderly manner. Throughout this document, the term software is used when referring to firmware and logic developed from software based developments systems. The objective of this plan is to:

- Define the software quality assurance activities to be performed during the lifecycle of the software;
- Describe the responsibilities and authorities for accomplishing the planned software quality assurance activities;
- Identify the required coordination of software quality assurance activities with other activities of the project;
- Identify the tools and the physical and human resources required for the execution of the plan;
- Ensure the software solutions necessary to implement the functional requirements, technical constraints, system development, configuration control, security, and software maintenance are accomplished in accordance with the approved methodology, supporting standards, and procedures;
- Ensure the products and services produced conform to applicable project requirements;
- Detect and eliminate design errors early in the software lifecycle; and
- Enhance the quality and reliability of PPS application software.

1.2 Applicability

PG&E procedure IDAP AD7.ID8 [2.1.3.1], Project Management which includes the Project Management Policies and Procedures, is the primary document describing the management processes and strategies for managing projects at Diablo Canyon Power Plant (DCPP). The Project Management Manual directs the overall project planning function and defines the organization, resources, and methodology for meeting project requirements. IDAP AD7.ID8 establishes measures for assuring that organizations performing activities affecting quality perform their responsibilities in a manner which results in safe nuclear power production. This SyQAP utilizes PG&E procedure IDAP CF2.ID9 [2.1.3.3], Software Quality Assurance Plan Development for software to be used in the PPS. The IDAP AD7.ID8 procedure describes the DCPP Quality program, policies, and procedures. The management approach, policies, and procedures described in this plan are derived from policies, procedures, codes and standards, and regulations applicable to the nuclear industry.

This plan applies specifically to the PPS at the Diablo Canyon Power Plant site. This software is Nuclear Safety-Related software requiring safety-related quality controls to meet SIL 4, as defined in IEEE 1012-1998 [2.1.2.24].

The plan covers the development lifecycle for SIL4 application software: requirements definition, detailed design, implementation, test, installation and checkout, operation, and maintenance. This software will be provided by two third-party suppliers who each have an approved 10CFR50 Appendix B Quality Assurance program [2.1.1.1]. This plan will umbrella the supplier's system development process. At a minimum the supplier's scope of supply will extend to the end of Factory Acceptance Testing (FAT). In

cases beyond the scope of the supplier, further work on the application software will be normally performed under the PG&E system quality assurance program.

This procedure is valid as of the date of final issue indicated on the title page. This procedure should be reviewed prior to making any changes to the PPS software.

1.3 Scope

This SyQAP applies to all software development and software maintenance activities, including those tasks performed by contractors and subcontractors. This SyQAP also applies to all applicable software lifecycle phases for the PPS not already covered under the suppliers' 10CFR50 Appendix B programs. This plan is intended for use by all project personnel to understand and perform the quality activities applicable to their responsibilities. Software Quality Assurance requires the project to identify quality activities for its currently planned work phase and related releases.

Software Quality Assurance for the project is planned along with other project tasks and initiatives. Implementation of and compliance with this SyQAP is the shared responsibility of all project personnel. Both project management and technical staff are thus integrated with and committed to the success of overall Software Quality Assurance.

The degree of rigor and effort is defined by the Software Integrity Level (SIL) and Software Categorization. Software SIL is defined in IEEE Std. 1012-1998 [2.1.2.24]. Nuclear Regulatory Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants [2.1.1.8], provides additional guidance that indicates that nuclear safety-related software should be assigned a SIL 4 rating.

In general, the SyQAP will place special emphasis on the software portion of the project. In addition the SyQAP will monitor, audit, and report on activities related to software safety to ensure no new safety hazards are introduced by the development process and on those activities related to configuration management. It will also provide traceability to verify that contractual requirements such as hardware requirements, the provision of specific system features, and other deliverables not directly related to the application software have been met. After successful completion of the Software Quality Assurance activities in this plan, the application software will meet the SIL-rating requirements for the software.

2. Reference Documents

2.1 Developmental References and Standards

2.1.1 U.S. Regulatory Guidance

2.1.1.1 Title 10 CFR, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power, Plants and Fuel Reprocessing Plants"

2.1.1.2 NUREG-0800 BTP 7-14, Branch Technical Position: Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, Revision 5, March 2007.

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

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

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

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

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

2.1.1.8 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

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

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

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

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

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

2.1.1.14 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

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

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

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

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

2.1.2 Industry Codes and Standards

2.1.2.1 ANSI/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 NEI 08-09, Revision 6, Cyber Security Plan for Nuclear Reactors

2.1.2.7 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1.3 DCPP References and Procedures:

2.1.3.1 PG&E Procedure, IDAP AD7.ID8, Project Management

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

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

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

2.1.3.5 PG&E Form 69-20164, Work Group Specific Training Record

2.1.3.6 PG&E Procedure, AD10.ID1, Storage and Control of Quality Assurance Records

NOTE: The various 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 [2.1.1.18], 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.

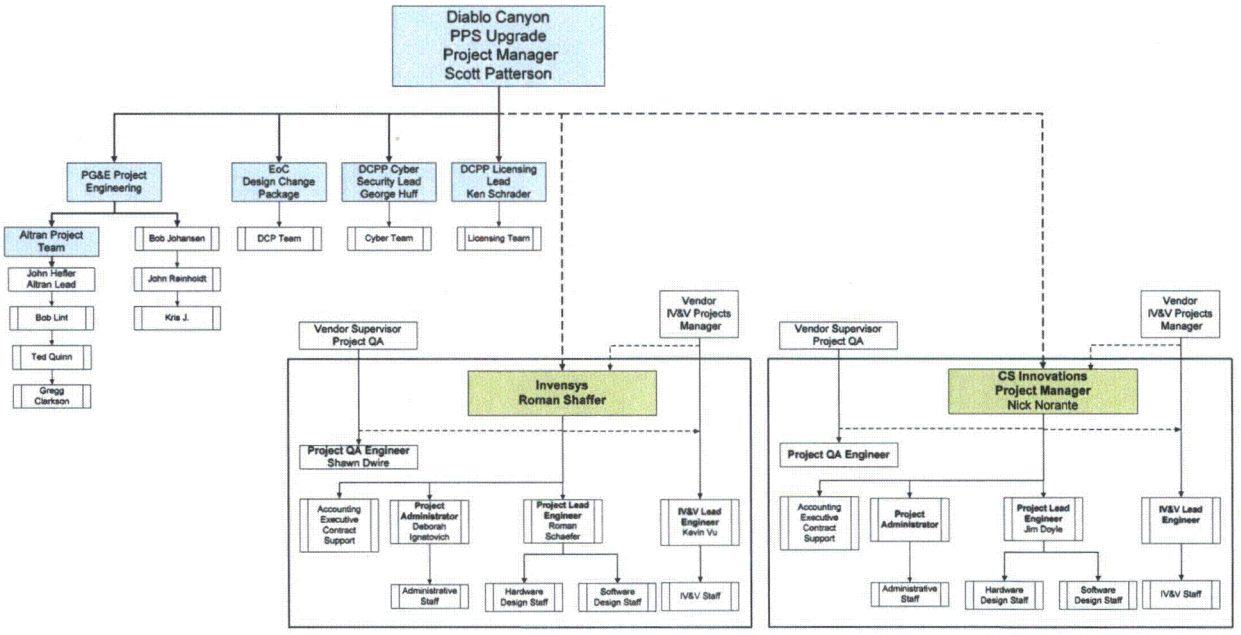
3. Management

3.1 Organization

Different organizational units, their responsibilities and relationships with regard to Quality are discussed in this SyQAP. The basic organizational structure that influences software quality is shown in Figure 3-1.

Quality Management for each of the 10CFR50 Appendix B suppliers will be independent of the project management organization. The basic tenet of Quality Management is to make all employees responsible for the quality of their work. This means quality management is the responsibility not only of management, but also of all project personnel who perform work for, and provide services and products for the project.

Figure 3-1 PPS Project Organization



It is expected of each 10CFR50 Appendix B supplier that the Project Manager is responsible for the development, integration and testing of the application software. The software development tasks are originated and supervised by the Responsible Engineer or directly by the Project Manager (or his designee) who leads the engineering team, and reports to the Design Authority. The PG&E Project Team determines the functional requirements of the software while the 10CFR50 Appendix B supplier designs the application software with the aid of engineering and software development tools.

The 10CFR50 Appendix B supplier will have different test personnel than those personnel involved in the design effort. Test personnel design the test plan and test cases, and perform the software testing. This organizational design is intended to promote objectivity, and improve the process of problem resolution and verification.

The respective 10CFR50 Appendix B supplier's integration team loads the completed software or logic onto the hardware platform, and performs integration testing, including Factory Acceptance Testing. This team is also staffed with individuals who did not participate in the software design effort.

The 10CFR50 Appendix B supplier's Nuclear Oversight Department, or equivalent, is responsible for the performance of the reviews, audit, and inspections of the software supplier. V&V Engineers will perform the activities prescribed in this plan. Additionally, V&V personnel have been tasked with verifying that the project meets nuclear and functional safety requirements per the Failure Modes and Effects Analysis, and Reliability Analysis. V&V personnel also ensure that no new software hazards are introduced throughout the software lifecycle. Overall responsibility for project safety is the responsibility of the Project Manager.

For this project, the Lead Verification Engineer performs the role of the Software Quality Assurance Manager and Project Safety Officer.

3.2 10CFR50 Appendix B Supplier Tasks

Below is a sequence of the tasks which describes the general development process PG&E expects the 10 CFR50 Appendix B [2.1.1.1] suppliers to follow. The specific development process employed by the 10CFR50 Appendix B vendors may vary. PG&E will use this SyQAP as a guide for the owner review and approval of the outputs of the development process employed by the 10CFR50 Appendix B vendor.

The tasks describe a complete program, from the requirements definition phase through the integration and testing phase of the software life cycle. Reviews and audits will be performed as described in Section 6. Software lifecycles are defined per BTP 7-14 [2.1.1.2] using the guidance in IEEE Std. 1074 [2.1.2.33]; Tasks meet the minimum requirements contained in RG 1.168 [2.1.1.8] and IEEE 1012-1998 [2.1.2.24]Table 2:

3.2.1 Project Initiation and Planning Phase Tasks

The Planning phase confirms that the system to be acquired is what is actually needed, and that it will be in compliance with the licensing basis of the plant. This phase also produces procedures for managing the interface with the supplier, and for managing changes to requirements. A verified and accepted contract is a product of this phase.

Tasks performed in this phase include:

Verify that system requirements (from Request for Proposal or tender, and contract) are consistent and conform to the current licensing basis;

- Verify that procedures are documented for managing requirement changes and for identifying the management hierarchy to address problems;
- Verify procedures for interface and cooperation among the parties are documented, including ownership, warranty, copyright, and confidentiality; and
- Verify that acceptance criteria and procedures are documented in accordance with requirements.
- Plan the interface between the V&V effort and the supplier.
- Review the supplier development plans and schedules to coordinate the V&V effort with development activities.
- Establish procedures to exchange V&V data and results with the development effort.
- The Project Manager should coordinate the plan with the supplier.
- Incorporate the project software integrity level scheme into the planning process.

A documented process for managing requirements changes and procedures for handling the interface among the parties signifies the end of this phase. The contract verification report will be used as an input to the preliminary Requirements Traceability Matrix.

3.2.2 Conceptual Design Phase Tasks

The Conceptual design phase defines the scope of the V&V effort. The initial V&V Plan, SyQAP, and FRS are products of this phase. Tasks performed in this phase are:

- Review the draft Functional Requirements Specification (FRS) (Concept Documentation Analysis);
- Verify SIL Classification(s), criticality, and software category per IEEE 1012 (Criticality Analysis);
- Draft and issue project System V&V Plan (SyVVP);
- Review the System Quality Assurance Plan (SyQAP);
- Provide input to the project master schedule;
- Analyze system hazards, security, and risks;
- Verify the correctness, accuracy, and completeness of the allocation of the requirements to hardware, software, and user interfaces in the conceptual design;
- Baseline the system so that subsequent changes can be assessed to determine new hazards and impact of project risk;
- Develop the preliminary Requirements Traceability Matrix (RTM);
- Review other management plans if available. These may include the Software Development Plan, Software Installation Plan, Software Integration Plan, Software Safety Plan, and Software Test Plan. These plans may be developed and reviewed in later phases just before they are needed.

The responsibilities of the V&V engineer are to publish the project Software V&V Plan (SVVP) and the V&V Summary Report documenting V&V activities and Task Reports for this phase. The draft RTM could be developed by the V&V team. At a minimum, the V&V engineer is responsible for ensuring that the RTM possesses the attributes needed to support V&V traceability analysis and associated metrics. The RTM will also be used to document traceability to contractual requirements such as hardware requirements, the confirm implementation of specific system features, and confirm compliance with other deliverables not directly related to the application software. In addition, the V&V engineer verifies the Requirements Allocation Analysis against user needs to verify correct, accurate, and complete allocation of requirements to hardware, software, and human operators.

An approved Functional Requirements Specification (FRS), Software V&V Plan, and Software Configuration Management Plan signify the end of the Conceptual Design Phase. A Preliminary Failure Modes and Effects Analysis (FMEA) may be started in this phase.

3.2.3 Requirements Phase V&V Tasks

In this phase, a Software Requirements Specification (SRS) will be prepared by the design team for each applicable software product using the guidance of IEEE Std. 830 [2.1.2.22]. The SRS will be developed based on the functional requirement specification and the system interface requirements specification, each of which must be approved by the customer prior to beginning.

The output of this task is the approved Software Requirement Specification (SRS). Tasks performed in this phase are:

- Review the Preliminary FMEA if applicable;
- Update the Requirements Traceability Matrix (RTM) completed in the Project Initiation and Conceptual Phase. The matrix typically will be in the form of a table. Since it will undergo frequent

change, it will be stored on safe, but readily retrievable computer storage media. Requirements Management planning is contained within the RTM document;

- Perform a Software Requirements Traceability Analysis by tracing the requirements between the FRS and the SRS. It is expected that requirements be traceable forward from the FRS to the SRS and backwards from the SRS to the FRS;
- Perform a Software Requirements Evaluation by evaluating that the SRS is correct, consistent, complete, accurate, readable, traceable and testable. The requirements will be checked for testability for purposes of validation testing. This ensures that the SRS adequately defines the software requirements necessary to perform the intended function;
- Assess software safety by reviewing that the safety requirements are correctly addressed. The purpose of this task is to ensure no new hazards have been introduced, ensure that software elements that can affect safety have been identified, and to ensure evidence exists that other elements do not affect safety;
- Perform a Software Requirements Interface Analysis by reviewing that requirements for interfaces to hardware, user, operator, and other software are correct, consistent, complete, accurate, traceable and testable;
- Verify that the configuration management process is complete and adequate (Configuration Management Assessment);
- Assess if there are any changes required to the Criticality Analysis;
- Perform a baseline change assessment to assess any changes to risk or security analyses; Issue the Baseline Review Report (BRR);
- Review or develop System V&V test plans;
- Coordinate resolutions of discrepancies with project management, design team personnel, and quality management;
- Produce the Software Requirements Review (SRR) Report

An approved Software Requirements Specification (SRS), satisfactory resolution of discrepancies, and an approved Software Requirements Review (SRR) Report containing the appropriate Task Reports and Anomaly Reports signify the end of the requirements phase. The SRS will be approved by prior to proceeding to the Design Phase.

3.2.4 Design Phase V&V Tasks

In this phase, the design team will prepare the Software Design Description (SDD) for each applicable software product using the guidance of IEEE Std. 1016 [2.1.2.25]. The SDD will be developed based on the software requirement specification and the software and hardware architecture. The SDD consists of two parts: the software and hardware architectural description and the Software Detailed Design. The Hardware Requirements Specification (HRS), Interface Requirements Specification (IRS) and Software Requirements Specification (SRS) should be approved by the customer prior to beginning the design phase to minimize project risk.

The output of this task is the approved SDD. Software Test Plan(s) (STP) will be generated by the design team to evaluate system performance. A three-pronged approach is used for testing:

(1) Component (Software Unit) Testing,

(2) Integration Testing, and

(3) Factory Acceptance Testing (FAT)

Software Test Plans conform to the requirements of IEEE Std. 829 [2.1.2.21] and IEEE Std. 1008 [2.1.2.23]. Software Test Plans will be reviewed by V&V. A separate Factory Acceptance Test Plan will be developed.

Tasks performed in this phase are:

- Perform a Software Design Traceability Analysis by tracing the requirements between the SRS and the SDD. It is expected that requirements be traceable forward from the SRS to the SDD and backwards from the SDD to the SRS. The results are recorded in the updated RTM;
- Perform a Software Design Evaluation. The SDD will be evaluated for correctness, consistency, completeness, accuracy, readability, and testability. The design will be evaluated for compliance with established standards, practices and conventions. Design quality will be assessed;
- Perform a Software Design Interface Analysis by reviewing that the software design interfaces to hardware, user, operator, and other software are correct, consistent, complete, accurate, and testable;
- Assess software safety to ensure no new software hazards have been introduced by the design;
- Assess if there are any changes required to the Criticality Analysis;
- Perform a baseline change assessment to assess any changes to risk or security analyses; Issue the Baseline Review Report (BRR);
- Develop Software Test Plan(s) (Component and Integration) related to software and the FAT Plan to ensure system test criteria will show compliance with all functional requirements in a system environment, performance at hardware, software and user interfaces, and performance at boundaries under stress conditions;
- Review Component, Integration, System, and Acceptance Test Designs as applicable.
- Produce the Software Design Review Report;
- Coordinate resolutions of discrepancies with project management, design team personnel, and Quality Management.

An approved Software Design Description (SDD), satisfactory resolution of discrepancies, approved Test Plan(s) and Design(s), and an approved Software Design Review Report signify the end of the design phase. These activities are required to be completed prior to proceeding to the Implementation Phase.

3.2.5 Implementation Phase V&V (Unit/Component Testing)

During this phase the executable code is produced and tested. Depending upon the target system, source code may be developed by the design team/programmers, or automatic code generators may produce the executable code. In either case, the functions described in the SRS are developed in the coding environment to programming standards. The correct implementation of the SRS is validated during function tests with the software development and simulation tools, and during testing on the test/development system. The RTM will generally have no entries for this phase. Also during this phase, software unit testing is performed by the design team.

Tasks performed in this phase are:

- Observe the building and compiling processes; A source code generation evaluation is performed to verify that the source code compiles without and builds without errors;
- Perform a Software Implementation Traceability Analysis to ensure that the correct versions and revisions of function diagrams were used to assemble the code for each subsystem;

- Verify that the procedure(s) used for software generation and download were followed and that the proper versions of code generators have been used;
- Examine the software for completeness to ensure that only qualified system software components have been used and that the software was successfully loaded onto the system;
- Review Software Unit Test results;
- Produce the Software Implementation Review Report;
- Coordinate resolutions of discrepancies with project management, design team personnel, and quality management;

Perform a baseline change assessment to assess any changes to risk or security analyses; Issue the Baseline Review Report (BRR);

Approved FAT Test Procedures, satisfactory resolution of discrepancies, and an approved Software Implementation Review Report signify the end of the implementation phase and readiness to proceed to the Integration Phase.

3.2.6 Integration Phase V&V Tasks

Integration Testing is a separate software Lifecycle activity per NUREG-0800 BTP 7-14 [2.1.1.2] and can be mapped to IEEE 1012-1998 [2.1.2.24]. s a continuation of the Implementation Phase. The Software is integrated with the hardware and integration testing is performed in accordance with the test procedures per IEEE Std. 829 [2.1.2.21]. Integration test execution results are analyzed to determine if the system implements the requirements and design and that the software components function correctly together.

Tasks performed in this phase are:

- Confirm that the software shown in the SDD is loaded into the system processors, and that the correct software was loaded onto the system;
- Develop Factory Acceptance Test (FAT) procedures and verify each functional requirement is tested;
- Review the Final FMEA to ensure that testing of failures where practical is included in test procedures;
- Evaluate the quality of user manuals;
- Assess software safety to ensure no new software hazards have been introduced by implementation activities;
- Assess if there are any changes required to the Criticality Analysis;
- Perform a baseline change assessment to assess any changes to risk or security analyses; Issue the Baseline Review Report (BRR);
- Review Integration test results;
- Perform requirements tracing between the FAT procedures and the SDD. The relationships between the V&V test plan(s), software designs, tests, and test procedures are analyzed for correctness and completeness;
- Assess software safety to ensure no new software hazards have been introduced by the integration activities;
- Produce a V&V Summary Report for the Integration Phase Activities;
- Coordinate resolutions of discrepancies with project management, design team personnel and quality management.

At the conclusion of the Integration Phase, the System Integration Review Report will confirm that the configuration of the system is complete and ready for FAT testing, and that there are no unresolved discrepancies or safety problems. Requirements tracing from the SDD to FAT test procedures should be completed in this phase to reduce the risk of an incomplete FAT test.

3.2.7 Test Phase V&V Tasks

System tests are performed in accordance with the FAT test procedures. Tests are analyzed to determine if the system implements the requirements and design and that the software components function correctly together. Test results are analyzed to determine if the software satisfies system objectives. Tests pass or fail based on the acceptance criteria stipulated in the SRS and on specific requirements found in the RTM.

Tasks performed in this phase are:

- Complete requirements tracing if not already completed in the integration phase to verify a valid relationship between test plans, procedures, and designs;
- Witness the FAT test and verify the tests validate that software correctly implements the requirements and that the expected results conform to the requirements;
- Identify discrepancies between actual and expected results;
- Produce the final verified and approved RTM;
- Produce a V&V Summary Report of the Test Phase Activities;
- Coordinate resolutions of discrepancies with project management, design team personnel, and quality management;
- Determine the extent of regression testing.

Approved FAT Test results as approved by the Project Manager and Customer Representative, satisfactory resolution of all discrepancies, and an approved Software Validation Report signify that the system meets it requirements and is ready for delivery to the customer. Each of the 10CFR50 Appendix B suppliers will provide a certificate of conformance at the completion and PG&E acceptance of the FAT results.

3.2.8 Final V&V Tasks

The final V&V tasks include issuing the Final V&V Report, 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.

Following approval of the final V&V Report, a certificate or letter of conformance will be issued certifying the system meets the SIL requirements.

Finally a configuration audit is performed to ensure all deliverables have either been previously shipped or are included for shipment to the customer.

3.3 PG&E Tasks

Below is a sequence of tasks which generally describes the process for PG&E after the final acceptance of the 10CFR50 Appendix B supplier FAT.

3.3.1 The Installation and Checkout Phase

The Installation and Checkout phase is when the developed system is first assembled in the Project Integration and Test (PIT) for pre-installation staging and checkout. Performance of the site acceptance test (SAT), per PG&E plant procedure, is conducted in the PIT. The developed system is then installed in the final target environment/location and performance of the design verification testing (DVT) per PG&E plant procedure is conducted. Depending on the complexity of the project, either the supplier or PG&E will perform system installation and checkout. Ultimately, PG&E will be responsible for acceptance of the results of the SAT and DVT. The Installation and Checkout V&V activity addresses software installation and software acceptance support.

Tasks performed in this phase:

- Audit the installation configuration to verify that all software products required to correctly install and operate the software are present in the installation package. Validate that all site-dependent parameters or conditions to verify supplied values are correct.
- Installation Checkout by V&V; Conduct analyses or tests to verify that the installed software corresponds to the software subjected to V&V. Verify that the software code and databases initialize, execute, and terminate as specified. In the transition from one version of software to the next, the V&V effort will validate that the software can be removed from the system without affecting the functionality of the remaining system components. The V&V effort will verify the requirements for continuous operation and service during transition, including user notification.
- Verify that the installation procedures and installation environment does not introduce new hazards; Update the hazard analysis;
- Review and update risk analysis using prior task reports; Provide recommendations to eliminate, reduce, or mitigate the risks; and
- Generate the V&V Final Report – Depending upon project scope, either PG&E or the supplier will be responsible for developing this report; Summarize in the V&V final report the V&V activities, tasks and results, including status and disposition of anomalies.
- Provide an assessment of the overall software quality and provide recommendations.

Outputs of this phase are the Operations Manual, the Installation Configuration Tables, Training Manuals, Maintenance Manuals, an Installation Safety Analysis, a V&V Installation Analysis and Test Report, and a CM Installation Report

3.3.2 Operation Phase V&V Tasks

The operation process covers the operation of the developed and installed system by PG&E in the target environment/location, and operational support by the system supplier. PG&E will have primary responsibility for V&V activities during this phase (unless contracted out to a software supplier with an approved and audited 10CFR50 Appendix B quality program). The objectives of Operation V&V tasks are to evaluate new constraints in the system, assess proposed changes and their impact on the software, and evaluate operating procedures for correctness and usability.

Tasks performed in this phase:

- Evaluate new constraints (e.g., operational requirements, platform characteristics, operating environment) on the system or software requirements to verify the applicability of the SVVP; Software changes are maintenance activities (see Section 3.2.10 Maintenance Phase, below).
- Assess proposed changes (e.g., modifications, enhancements, or additions) to determine the effect of the changes on the system. Determine the extent to which V&V tasks would be iterated.
- Verify that the operating procedures are consistent with the user documentation and conform to the system requirements.

- Verify that the operating procedures and operational environment does not introduce new hazards; Update the hazard analysis.
- Review and update risk analysis using prior task reports; Provide recommendations to eliminate, reduce, or mitigate the risks.

3.3.3 Maintenance Phase V&V Tasks

The maintenance process is activated when the software product undergoes modifications to code and associated documentation caused by a problem or a need for improvement or adaptation. The Maintenance V&V activity addresses modifications (e.g., enhancements, additions, and deletions), migration, or retirement of the software during the operation process.

Modifications of the software will be treated as development processes and will be verified and validated in accordance with development process described in the previous sections. Software integrity level assignments will be assessed during the maintenance process. The software integrity level assignments will be revised as appropriate to reflect the requirements of the maintenance process. For SIL3 systems, revising the software integrity level to the SIL4 may require updating the relevant planning documents, or generating new planning documents, as appropriate. For SIL4 software that is being downgraded to SIL3, the implications on compliance with the site's current licensing basis as well as compliance with regulatory requirements must be evaluated and document prior to initiating the maintenance activity. System modifications may be derived from requirements specified to correct software errors (e.g., corrective), to adapt to a changed operating environment (e.g., adaptive), or to respond to additional user requests or enhancements (e.g., perfective).

The Maintenance V&V activity covers modifications (e.g., corrective, adaptive, and perfective), migration, and retirement of software. Migration of software is the movement of software to a new operational environment. The retirement of software is the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system.

The Maintenance V&V activity addresses problem and modification analysis, modification implementation, maintenance review/acceptance, migration, and software retirement. The objectives of V&V are to assess proposed changes and their impact on the software, evaluate anomalies that are discovered during operation, assess migration requirements, assess retirement requirements, and re-perform V&V tasks.

Tasks performed in this phase:

- Revise the SyVVP to comply with approved changes. When the development documentation required by this plan is not available, generate a new SyVVP;
- Assess proposed changes (i.e., modifications, enhancements, or additions) to determine the effect of the changes on the system. Determine the extent to which V&V tasks would be iterated.
- Evaluate the effect of software operation anomalies.
- Perform a criticality analysis to determine the software integrity levels for proposed modifications. Validate the integrity levels assigned during development; address any inconsistencies, particularly if the SIL level is downgraded. For V&V planning purposes, the highest software integrity level assigned to the software will be the software system integrity level.
- Assess whether the software requirements and implementation address 1) specific migration requirements, 2) migration tools, 3) conversion of software products and data, 4) software archiving, 5) support for the prior environment, and 6) user notification.

- For software retirement, assess whether the installation package addresses: 1) software support, 2) impact on existing systems and databases, 3) software archiving, 4) transition to a new software product, and 5) user notification.
- Verify that software modifications correctly implement the critical requirements and introduce no new hazards; Update the hazard analysis.
- Review and update risk analysis using prior task reports; Provide recommendations to eliminate, reduce, or mitigate the risks.
- Perform V&V tasks, as needed, to ensure that 1) planned changes are implemented correctly; 2) documentation is complete and current; and 3) changes do not cause unacceptable or unintended system behaviors.

3.4 PG&E Roles & Responsibilities

The different roles and responsibilities for Software Quality Assurance as they relate to this SyQAP are discussed below:

3.4.1 PG&E Project Manager

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 project manager will:

- Release the system level V&V plan and reports
- Establish cost controls
- Enter the plan activities into the master project schedule.
- Review progress of the SyQAP and V&V program
- Evaluate any reported deviations or anomalies for their potential risk and impacts to project cost and schedule.
- Approve corrective actions, scope changes and resource allocations.
- Coordinate the disposition of discrepancy reports generated in the course of verification and validation.

3.4.2 Engineer of Choice (EoC) Design Change Package Team

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 Package Team is also responsible for establishing quality goals and objectives for their organization consistent with those of the project.

3.4.3 PG&E Project Engineering Team

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.

3.5 10CFR50 Appendix B Supplier Roles & Responsibilities

The section below is a general description of the 10CFR50 Appendix B supplier's roles and responsibilities. Detailed roles and responsibilities for each of the 10CFR50 Appendix B suppliers are provided in the respective 10CFR50 Appendix B supplier SQAP.

3.5.1 Supervisor Project QA

The Supervisor Project QA is responsible for monitoring implementation of the quality program throughout the project and supports all levels of management. The Supervisor Project QA monitors project activities to ensure compliance with the policies reflected in this program manual and the related standards and procedures throughout all system phases and maintenance activities.

Supervisor Project QA supports the Project overseeing implementation of the SQAP program. Responsibilities in this capacity include:

- Review the project-specific V&V plan and reports
- Ensure the SQAP addresses the quality goals and priorities of the project and client organization, and satisfies all organization requirements and expectations
- Ensure the SQAP is put under configuration management (CM) control and made available to all affected groups and individuals
- Ensure audits of activities for compliance with the SQAP and other applicable requirements
- Establish processes and procedures to perform SQAP activities
- Report findings to project management, and identify corrective actions related to the product and process verifications.

3.5.2 Project Manager (PM)

The Project Manager (PM) is responsible for providing direction in implementation of the SQAP program defined by this SQAP and for ensuring adequate resources are allocated to accomplish the implementation. The 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 project manager will:

- Release the project-specific V&V plan and reports
- Establish cost controls
- Enter the plan activities into the master project schedule.
- Review progress of the SQAP and V&V program
- Evaluate any reported deviations or anomalies for their potential risk and impacts to project cost and schedule.

- Approve corrective actions, scope changes and resource allocations.
- Coordinate the disposition of discrepancy reports generated in the course of verification and validation.

3.5.3 Project Lead Engineer

The focus of the Project Lead Engineer is to conduct and ensure quality-related inter-group coordination for design and engineering between software and hardware design activities. The Project Lead Engineer is responsible for identifying the processes and corresponding standards and procedures to guide project performance. The Project Lead Engineer is further responsible for ensuring work activities are performed in compliance with these standards and procedures.

3.5.4 Design Team

The Design Team interfaces with SQA regularly to review the status of software quality activities and to address any quality-related issues identified by SQA. The Design Team is responsible for establishing quality goals and objectives for their organization consistent with those of the project.

3.5.5 Testing/Integration Team

The Testing/Integration Team is responsible for integration and Factory Acceptance Testing (FAT). The Testing/Integration Team develops test plans and reports for systems integration and test activities, defines requirements for, develops, and implements test plans for systems integration and FAT. The Testing/Integration Team may include members of the Design Team.

3.5.6 Lead Verification Engineer (SQA Manager)

The Lead Verification Engineer is responsible to implement the Software Quality Assurance Program as defined in the Software Quality Assurance Plan (SQAP) for the project. The Lead Verification Engineer also manages resources to perform V&V activities, ensures the independence of V&V personnel, and approves the SVVP and V&V reports. The Appendix B software supplier is expected to have a separate QA organization and the Lead Verification Engineer will review and approve all test plans and V&V reports. Purchase Orders will be written so the SQA Organization is not constrained by either budget or schedule in the performance of their duties.

3.5.7 Verification & Validation (V&V) Staff

Verification & Validation (V&V) Staff will maintain technical independence, managerial independence, and financial independence. The V&V Staff are responsible to perform V&V audits and inspections per approved V&V Plans, create or verify the traceability of customer and functional requirements using a Requirements Traceability Matrix, review Software Test Plans, verify independently that all items of safety software have been correctly identified and included appropriately in the design documents, review test procedures as applicable, and produce Software V&V Reports in accordance with V&V Procedures. In addition V&V is responsible to evaluate the activities in each software Lifecycle phase to ensure the activities performed do not introduce new software hazards. Finally V&V will perform audits of configuration management. Project needs may dictate that V&V personnel will develop all software test plans, the FAT plan, and FAT procedures as well as supervise testing of the developed system.

3.5.8 Project QA Engineer or Equivalent

The Project QA Engineer is responsible to ensure that nuclear and functional safety objectives are met in accordance with IEEE 1012 [2.1.2.24].

4. Documentation

The NRC has issued Interim Staff Guidance (ISG) in digital instrumentation and control DI&C-ISG-06 [2.1.1.18] that describes the licensing process that may be used in the review of License Amendment Request (LAR) associated with digital I&C system modifications.

DI&C-ISG-06, Enclosure B, lists documents that are typically submitted by the licensee in support of a submittal during Phases 1 and 2 of review. The Phase 1 documents that are associated with this project are summarized in a separate attachment to the LAR. A list of Phase 2 documents associated with this project will be provided 12 months prior to the requested LAR approval date.

The documentation discussed below is a summary of the documents to be provided by PG&E and the 10CFR50 Appendix B supplier(s). As stated above, specific documents associated with this project are listed in separate lists provided with the LAR and Phase 2 submittal enclosure.

4.1 Overview of PG&E Documents

The following is a summary of the documents to be provided by PG&E.

4.1.1 Conceptual Design Document (CDD)

The CDD will provide a high level description of the overall system to be implemented by the DCPP PPS upgrade project.

4.1.2 Functional Requirements Specification (FRS)

The FRS will provide a general description of what PG&E expects the system to do. All known customer requirements will be documented. The FRS should state the specific customer requirements as clearly and consistently as possible. It will describe the operations the user wants to perform with the software and define all the constraints that the customer wishes to impose upon any solution. The FRS will describe the external interfaces to the system. IEEE Std. 1233 [2.1.2.36] can be used for guidance in regards to the content, table of contents and details that should be included in the FRS. The FRS is a deliverable from PG&E.

4.1.3 Interface Requirements Specification (IRS)

The IRS will provide a general description of how PG&E expects the separate deliverables from each of the 10CFR50 Appendix B suppliers to interface with one another. Specifically, the IRS will provide:

(1) Requirements for the interfaces between external field devices such as process transmitters and the 10CFR50 Appendix B suppliers' equipment;

(2) Electrical and communication interfaces between the 10CFR50 Appendix B suppliers equipment and their associated peripheral devices; and

(3) Other interfacing Diablo Canyon Power Plant (DCPP) systems such as the Plant Process Computer (PPC), Main Annunciator System (MAS), Safety Parameter Display System (SPDS) and the Safety-Related 120 Vac and 125 Vdc Power Systems.

4.1.4 System Verification & Validation Plan (SyVVP)

The System Verification and Validation Plan (SyVVP) for the overall system life cycle will be prepared according to IEEE Std. 1012 [2.1.2.24]. PG&E will review and approve 10CFR50 Appendix B supplier life cycle outputs providing independent V&V activities including review, evaluation, analysis, and inspection. It will include both an assessment of the development process, and independent testing of the software and logic products within the Site Acceptance Test (SAT).

In accordance with the system verification & validation plan, the overall plan for the verification and validation of the system is described. All methods, criteria, and tasks are listed, including required inputs and outputs.

4.1.5 Site Acceptance Test (SAT) Plan

The SAT Test Plan will prescribe the scope, approach, resources, and schedule of the testing activities. It identifies the items to be tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. The SAT Plan describes the formal acceptance testing approach, methodology, and acceptance criteria that will enable PG&E to accept the system for implementation in the plant. Test plans, test cases, and test procedures are developed in accordance with IEEE Std. 829 [2.1.2.21]. See Section 7 for further details about testing.

4.1.6 Requirements Traceability Matrix (RTM)

The RTM will be used to demonstrate traceability for each function through all phases of the system development. Regulatory guidance requires traceability analysis only for software requirements. However, formal requirements management is considered to be a good business practice toward development of a high-quality digital system. Therefore, it is recommended that the RTM cover hardware, software, and interface requirements of the digital system to the extent practical.

A RTM is created to demonstrate that all requirements have been successfully implemented in the design and tested in the testing program. Both forward and reverse paths must exist to be able to trace each design requirement to and from the SAT. During the RTM development there may be some requirements that cannot be validated by testing. For these, techniques such as analysis or reviews can be used and noted in the RTM. More information can be found in the EPRI V&V handbook (TR-103291).

4.1.7 System Verification and Validation (SyVVR) Final Report

The System Verification and Validation Final Report summarize all results of the execution of the SyVVP. It lists all deficiencies found; provides the results of reviews, audits and tests.

4.2 Overview of 10CFR50 Appendix B Supplier Documents

The section below is a general description of the 10CFR50 Appendix B supplier's documents. A detailed listing and description of the documents supplied by each of the 10CFR50 Appendix B suppliers is provided in the respective 10CFR50 Appendix B supplier SQAP.

4.2.1 System Requirements Specification (SyRS)

The System Requirements Specification (SyRS), which includes the I/O list and memory mapping between devices, describes the external input/output as well as input and output between modules of the new system architecture so hardware and software designs can proceed independently. Hardware and Software Design will consistently apply naming conventions to avoid confusion.

4.2.2 Software Verification & Validation Plan (SVVP)

The Software Verification and Validation Plan (SVVP) for the software life cycle will be prepared according to IEEE Std. 1012 [2.1.2.24]. Independent V&V activities include review, evaluation, analysis, and inspection. It will include both an assessment of the development process, and independent testing of the software products as necessary.

In accordance with the software verification & validation plan, the overall plan for the verification and validation of the software is described. All methods, criteria, and tasks are listed, including required inputs and outputs.

The V&V plan will describe the methods for verifying that the generated software implements design as expressed in the SDD and the requirements of the SRS, and validating that the code, when executed, complies with the expected results of the Software Test Plan(s) (STP).

The V&V plan will describe test plans and test cases to validate the capabilities and correct operation of any third party software, including the operating system and communications protocols, if required.

4.2.3 Software Configuration Management Plan (SCMP)

The software configuration management plan (SCMP) will be published to document configuration management activities applicable to the portion of the software life cycle covered by the SQAP. The SCMP will conform to the requirements of IEEE Std. 828 [2.1.2.20]. The configuration management activities required by the SCMP will be audited; the audit may be performed by QA, V&V, or by a team composed of both.

4.2.4 Software Safety Plan

The Software Safety Plan provides a systematic approach for identifying hazards and reducing software risks and defines the safety goals that are expected to be achieved by adhering to the plan. The plan follows and complies with BTP-7-14 [2.1.1.2] and the concepts of IEEE 1228 [2.1.2.35] but does not fully comply with IEEE 1228. The NRC has not endorsed IEEE 1228. The design of the SRS, SDD and code is potentially subject to constraints arising from the safety analysis. Supplier organizations are expected to provide documentation on their organization, requirements coupled with the performance of the FMEA, response time analysis and FAR to ensure that there are no safety hazards.

4.2.5 Baseline Review Report

The Baseline Review Report (BRR) documents the results of the Baseline Change Assessment (BCA) performed at the end of each lifecycle phase. The BCA is an evaluation of proposed software changes (e.g., anomaly corrections and requirement changes) for potential effects on previously completed V&V tasks. Plan iteration of affected tasks or initiate new tasks to address software baseline changes or iterative development processes. The BCA verifies and validates that the change(s) is (are) consistent with system requirements and does (do) not adversely affect requirements directly or indirectly. An adverse effect is a change that could create new system hazards and risks or affect previously resolved hazards and risks adversely.

4.2.6 Software Requirements Specification (SRS)

The SRS describes all functions accomplished using software that have to be specified during the software development. It is based on the reviewed and released Functional Requirements Specification (FRS). The SRS contains all information, necessary for the specification of function diagrams such as: function descriptions, performance criteria, signal interfaces, ID codes, hardware assignments and design constraints. Each function within the SRS is uniquely identified, such that its achievement is capable of being objectively verified and validated. The SRS follows the guidance in IEEE Std. 830[2.1.2.22] to the extent practical. The SRS is subject to the Software Requirements Review.

4.2.7 Requirements Traceability Matrix

The Requirements Traceability Matrix (RTM) will be used to demonstrate traceability for each function through all phases of the software development. Regulatory guidance requires traceability analysis only for software requirements. However, formal requirements management is considered to be a good business practice toward development of a high-quality digital system. Therefore, it is recommended that the RTM cover hardware, software, and interface requirements of the digital system to the extent practical.

The RTM have been created to demonstrate that all specified requirements have been successfully implemented in the design and tested in the testing program. A forward path must exist to be able to trace each design requirement to the FAT and, where applicable, to a user manual dictating how each requirement is to be carried out. During the RTM development there may be some requirements that cannot be validated by testing. For these, techniques such as analysis or reviews can be used and noted in the RTM. More information can be found in the EPRI V&V handbook (TR-103291) [2.1.2.5].

The requirements traceability matrix is updated at the end of each life-cycle phase to provide forwards and backwards traceability to and from the HW and SW requirements to ensure that failure modes are documented and tested. After the matrix is completed, verification is performed to ensure that those requirements that are found not to be testable are validated by other means.

4.2.8 Software Requirements Review Report

The SRR is performed to ensure that the SRS adequately and completely reflects the design demands of the functional requirements specification and they are technically feasible. The SRR verifies that the SRS was created in accordance to the above-mentioned standards and is unambiguous, complete, verifiable, consistent, modifiable, traceable and usable during operation and maintenance.

A Software Requirements Review Report will contain information about review activities, review participants, review results and all found discrepancies. Found discrepancies are reported in the form of open items and are subject to the discrepancy reporting process outlined in Section 8.

4.2.9 Software Design Description (SDD)

The design will specify reduction of the overall structure into physical solutions (algorithms, equations, control logic, and data structures) in a manner that the design can be translated into code. The Software Design Description (SDD) will contain a technical description of the software and hardware architecture, and the software with respect to the theoretical basis, mathematical model, control flow, data flow, control logic, and data structure. The SDD will contain a description of the allowable or prescribed ranges for inputs and outputs. For graphical programming environments utilizing function block diagrams to create application programs, the SDD of the application software is published by printing the function modules using software development tools described in the SVVP. The SDD will follow the guidance in IEEE Std. 1016 [2.1.2.25], to the extent practical.

4.2.10 User Documentation

The user documentation consists of manuals describing the hardware, system software and tools to guide users in installing, operating, and maintaining the system. User documentation will include an introduction, a description of the system's limitations, the user's interaction with the software, and any required training necessary to use the software. User documentation will also include the procedure for performing required periodic calibration, tests, and preventive maintenance.

User Manuals should describe operation of the overall system, including configurable parameters, options, program limitations, system-specific scripts, procedures for starting, re-starting of the system, exchange of modules, and all other essential information about the applications software as part of the user documentation to be provided. User Documentation will also be provided that describes I/O specifications and formats, user responses to messages resulting from improper input, and how to obtain user and maintenance support. Refer to IEEE Std. 1063 [2.1.2.32] for further guidance.

4.2.11 Software V&V Reports

Software V&V Reports are published at the end of each software Lifecycle phase per IEEE Std. 1012 [2.1.2.24] identifying the anomalies, corrective actions, and recommendations based on the V&V activities performed in each phase. Refer to Section 3 for the V&V activities to be performed.

4.3 10CFR50 Appendix B Supplier Software Test Documentation

The section below is a general description of the 10CFR50 Appendix B supplier's test documentation. Details of the software test documentation supplied by each of the 10CFR50 Appendix B suppliers are provided in the respective 10CFR50 Appendix B supplier SQAP.

Software testing will be developed following the test documentation requirements outlined in IEEE Std. 829 [2.1.2.21]. The test documentation will include a Software Test Plan(s) (STP), detailed test specifications, and test reports. Additional SQA testing requirements are described in Section 7. Failures in the software detected during testing will be recorded using the problem reporting process described in Section 8.

4.3.1 Software Test Plan(s)

The Software Test Plan(s) and FAT Test Plan will prescribe the scope, approach, resources, and schedule of the testing activities. It identifies the items to be tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. The Factory Acceptance Testing (FAT) Plan describes the formal acceptance testing approach, methodology, and acceptance criteria that will enable the customer to accept the system for delivery. Test plans, test cases, and test procedures are developed in accordance with IEEE Std. 829 [2.1.2.21]. See Section 7 for further details about testing.

4.3.2 Security Test Plan(s)

The objective of testing security functions is to ensure that the system security requirements are validated by the execution of integration, system, and acceptance tests where practical and necessary. Testing includes system hardware configuration (including all connectivity to other systems, including external systems), software integration testing, system integration testing, and system factory acceptance testing.

The security requirements and configuration items intended to ensure reliable system operation will be part of the validation of the overall system requirements and design configuration items. Therefore, security design configuration items will be just one element of the overall system validation. Each system security feature will be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access and/or the effects of undesirable behavior of connected systems and does not reduce the reliability of system's safety functions.

Depending upon the scope of the project, testing will address the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Built-in original equipment manufacturer features will also be included for testing.

4.3.3 Software Verification and Validation Final Report

The Software Verification and Validation Final Report (SVVR) summarizes all results of the execution of the SVVP. It lists all deficiencies found; provides the results of reviews, audits and tests. The result of the final report is a certificate of conformance that the software can be released for operational use.

4.4 Other Documentation

4.4.1 Documents

- Software Installation Plan provides a general description of the installation process and the goals of that process. A general description of the environment (such as temperature, humidity, vibration, and rack space) within which the computer system and software system is required to operate should be included in the plan. It describes the organization, roles and responsibilities, and approach required to perform the software installation. Software Installation Planning may be included in the Software Test Plan(s).
- Software Integration Plan describes the software integration process, the hardware/software integration process, and the goals of the processes. It describes the organization, roles and responsibilities, and approach required to perform the software integration. Software Integration Planning may be included in the Software Test Plan (s).
- Hardware Requirement Specification (HRS) similar to the SRS, the Hardware Requirements Specification describes what hardware will be used and what requirements must be met by the hardware to meet the Functional Requirements Specified in the FRS. The HRS is used to define the architecture of the system.

4.4.2 Design Analyses

The design of the system is potentially subject to constraints arising from the following analyses:

- Reliability Analysis evaluates the failure rates of modules in terms of the probability of system failure on demand, compares the overall system availability to the reliability goal(s) specified in the FRS. Reliability analyses are performed per the guidance of IEEE Std. 577 [2.1.2.17] and may be included in the FMEA.
- Failure Modes and Effects Analysis (FMEA) the detailed FMEA will specifically consider systematic random single failures based on the hardware design and architecture of the integrated system. Particular attention is paid to safety functions and software failures. The analysis is typically extended to include common mode failures. Recommendations are made based on potential failures, severity, and risks involved, which could result in design changes to the system. The FMEA will be performed following the guidance of IEEE Std. 352 [2.1.2.15].
- Response Time Analysis this analysis calculates the overall Response Time of the system, which should be lower than the shortest required response time, described in the FRS.

5. Standards, Practices, Conventions, and Metrics

This project adheres to regulatory guidance and ANSI/IEEE, and International standards considered acceptable for software used in nuclear plant safety systems. In particular, NUREG-0800, BTP 7-14 [2.1.1.2], IEEE 603-1991 [2.1.2.18], IEEE 7-4.3.2-2003 [2.1.2.7], and IEEE 1012-1998 [2.1.2.24] are used as the basis for the overall V&V process to be applied to SIL-4 systems. The design of the PPS is intended to meet the requirements of IEEE Standards that are currently endorsed by various NRC Regulatory Guides at the time of the design.

Monitoring of compliance and adherence to these standards is ensured through the reviews and audits conducted (see section 6) by the V&V team under the direction of the10CFR50 Appendix B supplier Lead Verification Engineer. Moreover, the 10CFR50 Appendix B supplier Lead Verification Engineer will approve, and document in future versions of this 10CFR50 Appendix B supplier SQAP, necessary practices, conventions, metrics and deviations from the standards, decided by the 10CFR50 Appendix B

supplier Project Manager and/or 10CFR50 Appendix B supplier Responsible Engineer. Deviations from standards should be clearly justified and documented in the respective SQAP.

5.1 Documentation standards

The documentation standards defined in the 10CFR50 Appendix B supplier SVVP, this SyQAP, and the 10CFR50 Appendix B supplier SQAP will be followed. See sections 4 and 6 for implementation of standards and monitoring of adherence.

5.2 Logic structure (design) standards

IEEE standards will be used for the overall organization of the SRS, SAD and SDD. Function logic diagrams and SAMA diagrams are predefined by the software development tools and cannot be altered by the user.

5.3 Testing Standards and Practices

Test procedures, test scripts and the results of the test are part of the documentation described in Section 7. The structure of test procedures and test scripts is in conformance with IEEE Std. 829 [2.1.2.21] and IEEE Std. 1008 [2.1.2.23] as verified as part of the V&V testing activities described in the 10CFR50 Appendix B supplier SVVP.

5.4 Selected SQA Product and Process Metrics

A minimum set of quality metrics should be defined in each of the 10CFR50 Appendix B supplier SVVP. A required metric is the requirements coverage ratio, defined as the fraction of requirements specified in the SRS that are traceable into the SDD and testing program.

6. Software Reviews and Audits

Reviews and audits are part of the Verification and Validation (V&V) activity. Accordingly, all reviews and audits, as well as the necessary arrangements and methods for these reviews and audits will be specified in the SyVVP as well as each of the 10CFR50 Appendix B supplier SVVPs. The procedures for software reviews are based closely on the ANSI/IEEE Std. 1028 [2.1.2.26]. In general, technical reviews evaluate specific software elements to verify requirements and conformance to regulations, codes, and standards; a code walkthrough is a method used for the early evaluation of documents, models, designs, and code; inspections are performed to evaluate documents and code before technical review or testing, and independent reviews and audits are performed to assess compliance with software requirements, specifications, baselines, standards, procedures, instructions, codes, and contractual and licensing requirements.

Verification reviews will be documented identifying the participants and their specific responsibilities during the review. Review documentation will include review comments and their disposition, which will be retained until they are incorporated into the updated software. Comments and dispositions not incorporated will be retained in accordance with established procedures. Following incorporation of comments, reviewed documents will be updated and placed under configuration control. Found discrepancies are reported in the form of open items and are subject to the discrepancy reporting process outlined in Section 8.

The following IEEE-730 [2.1.2.19] reviews and audits or their equivalents are used in the process of performing V&V:

6.1 Software Requirements Review (SRR)

The Software Requirements Review is held to ensure adequacy of the requirements stated in the SRS. The SRS will be reviewed each time it is updated. The output from the review will consist of verification review comments, which will be documented in an SRR Report and transmitted to the development organization. The report will identify all deficiencies discovered during the review. The review process may require several iterations. This review is described further in Section 4.

6.2 Architectural Design Review (ADR)

An Architectural Design Review is a preliminary review to verify the technical adequacy of the basic design, and check the compatibility of the functional and performance requirements for the system. The ADR verifies consistency of the interfaces between the software and hardware. The basic design concepts are verified for consistency and technical feasibility.

6.3 Detailed Design Review (DDR)

A Detailed Design Review is held to determine the acceptability of the detailed software designs as depicted in the detailed design description in satisfying the requirements of the SRS to include: all functions, specified in the FRS are implemented; the described interface is completely implemented; and test requirements are implemented. The software design review will verify that the software design is traceable to the requirements.

6.4 Software Verification and Validation Plan Review (SVVPR)

The SVVPR is held to evaluate the adequacy and completeness of the verification and validation methods defined in the SVVP. This review is completed by the Project Manager with support from the Lead Verification Engineer and is signified by approval of the SVVP. The SVVP should be reviewed and updated at the end of each phase of the software development life cycle to consider any new or different V&V activities for the next life cycle based on lessons learned from previous lessons learned and operating experience.

6.5 Functional Audit

This audit is held prior to the software delivery to verify that all requirements specified in the SRS have been met. Functional Audits are held together with the system design team prior to the system delivery during FAT testing. The Project Manager's and Customer or Customer Representative's approval of FAT Test Results signify acceptance of the system for delivery.

6.6 Physical Audit

This audit is held to verify that the software and documentation are internally consistent and ready for delivery.

6.7 In-process Audits

In-process audits of a sample of the design are held to verify consistency of the design, including code versus design documentation, interface specifications of the hardware and software, implementation of the design versus functional requirements, and functional requirements versus test descriptions. For this project, this will be accomplished by performing forward and backwards traceability analyses from the functional requirements through testing using a RTM.

6.8 Managerial Reviews

Managerial reviews are held periodically to assess the execution of all of the actions and items identified in the SQAP. These reviews will be held by the Project Manager or his designee. Additionally SQA will attend project and staff meetings as feasible to assess and report on organizational effectiveness. Observations, both positive and negative, will be included in monthly activities reports.

6.9 Software Configuration Management Plan Review (SCMPR)

The SCMPR is held to evaluate the adequacy and completeness of the configuration management methods defined in the SCMP. This review is performed by the Project Manager with support from the Lead Verification Engineer and is signified by their approval of the SCMP.

6.10 Post Implementation Review

A review will be held at the conclusion of the project to assess the development activities performed during the project and to provide recommendations for improvement and to develop lessons-learned. The Post Implementation review will be conducted by the Project Manager with input from SQA personnel, project technical personnel, and the system design team.

6.11 User Documentation Review

A review of user documentation will be performed to assess the adequacy of user documentation in regards to completeness, clarity, correctness, and usability.

6.12 Software Safety Reviews

An assessment will be made at the end of each software lifecycle phase to confirm that the activities performed during that phase did not introduce any new software hazards. This assessment will be performed by independent V&V personnel.

6.13 Configuration Management Reviews

The effectiveness of configuration management will be evaluated at the end of each software Lifecycle phase by SQA personnel.

7. Test

All software verification and validation activities will be documented as required by each of the 10CFR50 Appendix B [2.1.1.1] suppliers Software Verification and Validation Plan (SVVP). The content related to testing in the 10CFR50 Appendix B SVVP will be derived from the IEEE Standard for Verification and Validation Plans (IEEE Std. 1012 [2.1.2.24]) and the IEEE Standard for Software Test Documentation (IEEE Std. 829 [2.1.2.21]). Software Test Plan(s) (STP) will be created per IEEE Std. 829 to define the scope, approach, resources, and schedule of testing activities. A separate FAT Plan will be developed.

8. Problem Reporting and Corrective Action

Problem reporting and corrective action procedures are part of the SCM activity and documented accordingly in the SCMP as well as the individual 10CFR50 Appendix B suppliers' SCMP.

The actual implementation of the procedures is under the responsibility of each of the individual Project Managers, while the 10CFR50 Appendix B supplier Lead Verification Engineer is in charge of ensuring and monitoring the policy. Moreover, the 10CFR50 Appendix B Lead Verification Engineer will record problem statistics and observe their trends.

Software anomalies can be reported at any stage in the life cycle. Anomalies can fall into a number of classifications according to the degree of regression in the life cycle. Selection of the problem classification defines the phase of the life cycle at which corrective action needs to start.

The 10CFR50 Appendix B suppliers' SVVP will describe the method of reporting and resolving anomalies, including the criteria for reporting an anomaly, the anomaly report distribution list, and the authority and time lines for resolving anomalies. The section will define the anomaly criticality levels. Classification for software anomalies may be found in IEEE Std. 1044[2.1.2.28].

8.1 Anomaly Resolution and Reporting

Anomalies are software discrepancies discovered by the V&V team, either during independent testing or observation of testing by the design and testing organizations. Anomalies can be compliance problems or simply enhancement suggestions. V&V anomalies identified by the V&V team must be reported to the design team. The V&V team will use the normal, applicable discrepancy reporting process of the project. Either the 10CFR50 Appendix B suppliers' corrective action process or the PG&E corrective action process may be used; in either case a tracking mechanism must be used.

The tracking system must include a flag or other means to identify open items that are V&V discoveries and anomalies. Anomalies will be classified and assessed for project risk, in accordance with the requirements of this SyQAP.

8.2 Task Iteration Policy

The 10CFR50 Appendix B suppliers' SVVP will describe the criteria used to determine the extent to which a V&V task will be repeated when its input is changed or task procedure is changed. These criteria may include assessments of change, software integrity level, and effects on budget, schedule, and quality.

Each V&V task performed, using designer-supplied documentation, will be assessed for possible re-performance whenever that documentation is revised. For instance, the release of a revised SRS would trigger assessment not only of those activities in which the SRS itself was evaluated, but also of those activities that used the SRS as a reference for the evaluation of other documentation (i.e., SDD).

V&V personnel will conduct such assessments based on the extent of the changes, the criticality of the functions affected, and the anticipated impact on the software quality. Their findings will be documented and V&V tasks re-performed to the extent required. This typically requires a revision of the report for that phase.

9. Tools, Techniques, and Methodologies

Tools, techniques and methods for software production will be defined at the project level, and documented in the relevant 10CFR50 Appendix B suppliers' documents. It is an SQA activity, under the responsibility of each of the 10CFR50 Appendix B supplier Lead Verification Engineers, to check that appropriate tools, techniques and methods are selected and to monitor their correct application.

Each of the 10CFR50 Appendix B supplier Lead Verification Engineers may decide that additional tools, techniques and methods are required to support the respective monitoring activity. These will be documented and described in that particular 10CFR50 Appendix B supplier's SQAP.

Each of the 10CFR50 Appendix B supplier's SVVPs will describe documents, hardware and software V&V tools, techniques, methods, and operating and test environment to be used in the V&V process. Acquisition, training, support, and qualification information for each tool, technology, and method will be included. Tools that insert code into the software will be verified and validated to the same rigor as the highest software integrity level of the software. Tools that do not insert code will be verified and validated to assure that they meet their operational requirements. If partitioning of tool functions can be

demonstrated, only those functions that are used in the V&V processes will be verified to demonstrate that they perform correctly for their intended use.

Methods/tools require a description of the methods, equipment, instrumentation and tools used to carry out each V&V task. Test methods should be specified for unit, integration, validation, installation and regression testing. The plan should specify a process for selecting tools. The hardware and software environment within which the V&V tools are to be applied and any necessary controls should be described. V&V methods include document reviews, design reviews, requirements traceability analysis, independent testing and validation, problem identification, risk assessment, and metrics performance.

10. Media Control

Software configuration management (SCM), i.e. methods and facilities used to maintain, store, secure and document controlled versions of the identified software during all phases of the software life cycle) will be implemented according to the SCMP and the individual 10CFR50 Appendix B supplier SCMP(s).

All software items, for example documentation, source code, executable code, files, tools, test software and data, will be subjected to configuration management procedures. The configuration management procedures will establish methods for identifying, storing and changing software items through development, integration and transfer.

10.1 Media Control

The media for storing each deliverable work product and the associated documentation will be defined by the Appendix B suppliers SCMP(s). The 10CFR50 Appendix B supplier SCMP(s) will define requirements for code control and have a disaster recovery plan. The 10CFR 50 Appendix B supplier SCMP(s) will delineate the standards and procedures that will conform with the applicable security policies to ensure the system design products (hardware and software) do not contain dead code, undocumented code (e.g., back door coding), malicious code (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes), and other unwanted or undocumented functions or applications.

11. Supplier Control

Supplier control will be maintained by PG&E performing reviews, inspections, and audits. All project documents developed by the suppliers will undergo PG&E review prior to final approval. Inspections can be performed to monitor the execution of any testing. PG&E I&C Project(s) Engineering will perform a review and approve the 10CFR50 Appendix B suppliers SQAP(s).

Tools and support software for system software or programmable logic will be confirmed to have been implemented in accordance with an appropriate Quality Assurance program for the whole life cycle of the software, e.g., an approved 10 CFR Part 50 Appendix B program. The system software or programmable logic should be evaluated to determine that it is adequate in terms of both the documentation and available supplier support during the Operation and Maintenance lifecycle phases.

12. Records Collection, Maintenance and Retention

The project manager is responsible for ensuring all documentation and records will be maintained in accordance with AD10.ID1 [2.1.3.6]. This includes, as a minimum the following:

- All final approved documents listed in Section 4 of this SyQAP.
- All formal Review and Comment Resolution Sheets.
- All Audits will be stored per IAW applicable QV requirements.
- Problem Reports and Log.

- All written Project Correspondence (Incoming and Outgoing)
- All final approved Supplier Documentation
- Issued Purchase Orders and any subsequent Change Orders
- Records of performance of any Training

All software documentation, formal correspondence, or other documents required by this plan will be archived in the following location:

NPG Library/Engineering/Strategic Projects/Project Management/ICOM/Current Approved

Projects/RPS – Eagle 21

13. Training

The PG&E PPS Project Engineering Team will conduct Project Specific Training for PG&E PPS Project Engineering team members on Project administration to include (but not be limited to):

- Project formal correspondence (Incoming and Outgoing)
- Software control (including version control)
- LAN Access and File Storage location
- Project Administration • Project Problem Reporting
- Selected PG&E Procedures (AD10.ID1 [2.1.3.6], CF2.ID9 [2.1.3.3], etc.)
- Other Training to be determined by I&C Project(s) Engineering as required.

The PG&E PM will ensure that all team members have been trained on the elements of this SyQAP as outlined above. The training will be documented on Form 69-20164, Work Group Specific Training.

The 10CFR50 Appendix B suppliers will ensure the following:

- The personnel assigned will be qualified in accordance with appropriate codes and standards.
- The overall management of training is the responsibility of the Project Manager. Training can be considered as a means to reduce risk levels due to the technical experience and skills of the human resources for the project. If a risk factor due to training or skill deficiency is actually identified, this should be documented.
- The Project Manager will verify that training needs have been properly assessed and documented, and monitor the implementation of training plans.

14. Risk Management

Risk Management requires specification of the methods used to identify and manage risks associated with the V&V process.

Risk management includes identification of risk factors that may cause the V&V task to fail to perform its functions, and methods to recover from any such failure. These plans may range from doing nothing (i.e. live with the risk) to redesign. Redesign options can include eliminating the software feature if acceptable.

The plan should provide procedures for evaluating the risks associated with each project development activity. Risk evaluation will be documented as a V&V activity report. The V&V engineer will brief the Project Manager of project management (cost and schedule) risks. The V&V engineer will, also brief the Project Manager of the software safety risks.

Risk is defined as the probability of an adverse event or outcome multiplied by the cost or impact of its occurrence. Risk evaluation can therefore be done using probabilistic or risk-informed methods, such as are recommended in RG 1.174 [2.1.1.14].

However, estimates of software reliability are considered questionable, and the use of quantitative reliability goals for computer-based safety systems is predicated on deterministic criteria for the computer system in its entirety (i.e., hardware, system software, firmware, application, and interconnections).

The V&V engineer for each of the 10CFR50 Appendix B suppliers should publish a list of the open items believed to pose the greatest project and/or safety risks; in order that they are kept visible for project management until a satisfactory risk mitigation strategy is devised. It is expected that these open items will be worked aggressively by the design and V&V organizations.

15. Glossary

15.1 Definitions

Acceptance	Official recognition that a product (usually hardware or software CI) 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 CI. (A baseline is subject to configuration control and is updated to reflect approved changes to the CI throughout its life cycle.)
Baseline Load	For software, a complete software package stored in a designated location that is capable of running on its own from a system reboot. A load will have all software code, all local area network (LAN) code, all human machine interfaces (HMI) code, and any databases required for software functionality.
Build	Intermediate version of a system or CI that provides a demonstrable subset of capabilities needed to meet requirements allocated to the system or CI.
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.
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.
Concept 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 CI 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 (CI)	• 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 CIs 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 CI can be composed of hardware or software or, for major CIs, 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.
Critical Characteristics	Those important design, material, and performance characteristics of a commercial grade item that, once verified, will provide reasonable assurance that the item will perform its intended critical non-safety function.
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.
Dead Code	• Software code that is not required or specified by the software design documents (SRS and SDD) that has the potential to adversely impact a safety significant function. Examples of software that would be considered Dead Code: • Test functions that were not specified in the SRS or SDD; and if activated, the test function could adversely impact a safety significant function. • Programs that have been installed (possibly for future use) and then disabled; and if enabled, this software code could have an adverse impact on a safety significant function. • Any code that is not intended to be challenged or tested during the V&V process. Examples of software that would not be considered Dead Code: • A tag-name inserted into the code for monitoring purposes only. • The insertion of non-executable comments or notes. • The use of a validated function or function block that may or may not execute internal code based on input conditions.

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.
Design Step	A defined activity of the design process.
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.
Administrator	Individual responsible for controlling the test process and performing other duties as set forth in this plan.
Fault Tolerance	The quality of fault tolerance that is achieved when a system has the ability to complete critical functions within its required performance characteristics in spite of power or equipment failures and software faults.
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.
Identity Check	A check of software to confirm the correct version is loaded. This comprises primarily of a comparison of specific checksums.
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.
Locked Down	For the purposes of this SyQAP the term Locked Down is referring to software that is completed and ready for V&V testing. Any additional changes to software that has been Locked Down requires a formal change process IAW CF2ID9 form 8.5.
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.
Measurement Data	Data made up of value instances of measures.

Open Item	A notation of a characteristic, datum, detail, etc. which constitutes an error or discrepancy, or deviation, from the required status or condition of a properly completed project. Open Items are each given a record in a database with a unique (to the project) identifier and maintained by the project manager or project engineer. The entry contains information to track the cycle of the item from discovery of the item until final resolution.
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.
Preventive Action	Preventive action is action taken to eliminate the causes of a potential nonconformity, defect, or other undesirable situation in order to prevent occurrence.
Process Audit	Process Audit determines whether planned activities are being performed, designated products are being developed, and specified standards and procedures are being followed. At an intermediate point in each life cycle phase, Quality Management conducts a Process Audit and reports findings to project management.
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 CI 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.
Regression analysis and testing	Determine the extent of V&V analyses and tests that must be repeated when changes are made to any previously examined software products. Assess the nature of the change to determine potential ripple or side effects and impacts on other aspects of the system. Rerun test cases based on changes, error corrections, and impact assessment, to detect errors spawned by software modifications.
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 CI 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 CI 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.

16. SyQAP Change Procedure and History

This section is not applicable. Page two contains a Revision History Page per PG&E procedures.