Enclosure
Attachment 7
PG&E Letter DCL-12-069

Invensys Operations Management Document
"993754-1-906, Revision 1, Software Development Plan"

invensys
Operations Management

invensys
Triconex

Project:	**PG&E PROCESS PROTECTION SYSTEM REPLACEMENT**
Purchase Order No.:	35000897372
Project Sales Order:	993754

PACIFIC GAS & ELECTRIC COMPANY

NUCLEAR SAFETY-RELATED PROCESS PROTECTION SYSTEM REPLACEMENT DIABLO CANYON POWER PLANT

SOFTWARE DEVELOPMENT PLAN (SDP)

Document No. 993754-1-906 (-NP)

Revision 1

July 11, 2012

Non -Proprietary copy per 10CFR2.390
- Areas of Invensys Operations Management proprietary information, marked as [P], have been redacted based on 10CFR2.390(a)(4).

	Name	Signature	Title
Author:	**Ken Harris**		**Project Engineer**
Reviewer	**Shawn Dwire**		**Nuclear Quality Assurance**
Approvals:	**Roman Shaffer**		**Project Manager**

Document Change History

Revision	Date	Change	Author
0	8/17/2011	Initial issue	K. Harris
1	7/11/2012	Updated the following Software Life Cycle Process flow charts: Planning Phase • Removed "Software Project Risk Management Plan" from the Planning Phase outputs. This information will be included in the PMP. • Re-ordered the Planning Phase Outputs. Requirements Phase • Removed "System Design Basis, if required" from the requirements Phase outputs. This document is not required for this project. Design Phase • Added "Hardware Design Description" • Removed "Software Architecture Description" from flow chart and Phase outputs. This is being replaced by the Hardware and Software Design Descriptions. • Added "Reliability Analysis" to flow chart and Phase outputs. • Added "Coding Guidelines" to flow chart and Phase outputs. • Re-ordered Design Phase Outputs. • Minor changes to flow chart to accommodate adding and deleting items, added missing line end arrows. Test Phase • Added Hardware Design Description to the Test Phase Inputs	K. Harris
		In Section 3, the names of the project team members were replaced with their corresponding position titles.	
		Throughout the document various editorial changes.	
		In Table 5 Added ND as the responsible Organization.	

		In Section 2.3.3 and 2.4.3, reordered Table 4 and 5 and the following paragraphs to match the output list in the Software Life Cycle Process flow charts.		
		Added Reference 1.3.3.12 Software Configuration Management Plan.		
		Edited 3.1.1 to reflect the use of standalone laptops for development.		
		Added section 3.2.6 Problem Reporting and Corrective Action.		

Table of Contents

List of Tables

List of Figures

1. Introduction

This Software Development Plan (SDP) is a controlling document that outlines a plan for the software development effort. The software will be used in the Pacific Gas & Electric (PG&E) Diablo Canyon Power Plant (DCPP) Process Protection System (PPS) Project.

1.1. Purpose and Scope

The Software Development Plan defines the life cycle phases of the software development process. The SDP provides the project team with the technical information, required for carrying out the development project.

The purpose of this SDP is to:

- Define an approach to the software development process, which increases the likelihood of detection of human errors and reduces overall risk.
- Define the technical development activities performed in each phase of the development process and how they will be connected to other development activities.
- Describe the methods, tools, and techniques to be used during the design, analysis, development, testing, and integration of the software.
- Describe the personnel or groups responsible for development, validation, and verification of various design outputs.
- Guide the technical aspects of the development project.
- Define the assumptions on the overall software lifecycle.
- Establish a safety-assured and consistent implementation of the final software product.

This SDP is intended for use in the development of software for nuclear safety-related applications that conform to the requirements of 10 CFR 50 Appendix B. The SDP is written to comply with RG 1.173 [Reference 1.3.1.4] and Institute of Electrical and Electronics Engineers (IEEE) Std. 1074 [Reference 1.3.2.1].

1.2. Organization of Software Life Cycle Processes

This SDP utilizes a modified waterfall model for the software development lifecycle process. The lifecycle model is illustrated in Figure 1 and described in detail in Sections 2.1 through 2.7.

The PG&E DCPP PPS Replacement Project requires a life cycle that consists of several key phases. The overlap between the DI&C-ISG-06 [Reference 1.3.1.6] Licensing Amendment Request review phases and the Nuclear System Integration Program Manual (NSIPM) [Reference 1.3.3.1] project lifecycle phases is shown in Table 1, below. Section 1.2 of the PG&E DCPP PPS Project Management Plan [Reference 1.3.3.3] provides more detail on the DI&C-ISG-06 Enclosure B documents. These documents will be produced during PPS Replacement Project Phases 1 and 2.

The following table lists the phases or activity groups of the development life cycle.

Table 1 Life Cycle Mapping

PPS Project	DI&C-ISG-06 Enclosure B	NSIPM Project Lifecycle Phase
Phase 1	Phase 1	Acquisition
		Planning
		Requirements
Phase 2	Phase 2	Design
		Implementation
		Test
		Delivery
	Phase 3	Scope of Supply To Be Determined

RG 1.152 [Reference 1.3.1.2], RG 1.173, and IEEE Std. 1074 provide the basis for the software development lifecycle described in this SDP.

1.3. References

1.3.1. NRC References

1.3.1.1. NUREG/CR-6463, Revision 1, "Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems," August 1997

1.3.1.2. RG 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

1.3.1.3. RG 1.172, Revision 0, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

1.3.1.4. RG 1.173, Revision 0, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

1.3.1.5. United States Nuclear Regulatory Commission (NRC) Digital Instrumentation and Controls Interim Staff Guidance 4, (DI&C ISG-04)

1.3.1.6. United States Nuclear Regulatory Commission (NRC) Digital Instrumentation and Controls Interim Staff Guidance 6 (DI&C-ISG-06)

1.3.2. IEEE Standards

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

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

1.3.3. Applicable Internal Documents and References

1.3.3.1. Coding Guidelines 993754-1-907

1.3.3.2. Nuclear Systems Integration Program Manual, (NSIPM) NTX-SER-09-21, Revision 1, dated July 9, 2010

1.3.3.3. Project Management Plan, 993754-1-905

1.3.3.4. Project Quality Plan 993754-1-900

1.3.3.5. Project Traceability Matrix, 993754-1-804

1.3.3.6. Purchase Order Compliance Matrix, 993754-1-800

1.3.3.7. Software Safety Plan, 993754-1-911

1.3.3.8. Software Verification and Validation Plan, 993754-1-802

1.3.3.9. Triconex Project Procedures Manual

1.3.3.10. Project Instruction 7.0 "Application Program Development for the PG&E DCPP PPS Replacement Project, 993754-1-951"

1.3.3.11. Tricon V10 Nuclear Qualified Equipment List (NQEL) 9100150-001

1.3.3.12. Software Configuration Management Plan, 993754-1-909

1.3.4. Acronyms

AFW	Auxiliary Feedwater
ALS	Advanced Logic System

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CASE	Computer-Assisted Software Engineering
CDD	Conceptual Design Document
CFR	Code of Federal Regulations
DCPP	Diablo Canyon Power Plant
DI&C	Digital Instrumentation and Controls
EMI	Electromagnetic Interference
ESFAS	Engineered Safety Feature Actuation System
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FRS	Functional Requirements Specification
HRS	Hardware Requirements Specification
HSI	Human-System Interface
HVT	Hardware Validation Test
I/O	Input/Output
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOM	Invensys Operations Management
IRS	Interface Requirements Specification
ISG	Interim Staff Guidance
IV&V	Independent Verification and Validation
LAR	License Amendment Request
LLR	Lessons Learned Report
LOE	Level of Effort
LTOPS	Low Temperature Overpressure Protection System
MCB	Main Control Board
MCL	Master Configuration List
MDM	Manufacturing Department Manual
ND	Nuclear Project Delivery
NQA	Nuclear Quality Assurance
NRC	U.S. Nuclear Regulatory Commission
NSIPM	Nuclear System Integration Program Manual
OPDT	Over-Power Delta-T
OTDT	Over-Temperature Delta-T
PE	Project Engineer
PG&E	Pacific Gas & Electric Company
PMP	Project Management Plan
PO	Purchase Order
POCM	Purchase Order Compliance Matrix
PPM	Project Procedures Manual

PQAE	Project Quality Assurance Engineer
PQAM	Project Quality Assurance Manager
PQP	Project Quality Plan
PPS	Process Protection System
PRC	Project Review Committee
PT2	File extension for the TriStation 1131 application code, i.e., *.PT2
PTM	Project Traceability Matrix
PWR	Pressurized Water Reactor
QA	Quality Assurance
QC	Quality Controls
QPM	Quality Procedures Manual
RFI	Radio-Frequency Interference
RG	Regulatory Guide
RHR	Residual Heat Removal
RTS	Reactor Trip System
RXM	Remote Extender Module, Remote Expansion Chassis
S/G	Steam Generator
SAD	System Architecture Description
SAT	Site Acceptance Test
SCMP	Software Configuration Management Plan
SDD	Software Design Description
SDP	Software Development Plan
SER	Safety Evaluation Report
SI	Safety Injection
SIL	Software Integrity Level
SIntP	Software Integration Plan
SLC	Software Life Cycle
SLCP	Software Life Cycle Process
SQAP	Software Quality Assurance Plan
SRS	Software Requirements Specification
SSP	Software Safety Plan
SSPS	Solid State Protection System
SVVP	Software V&V Plan
SWR	Software Walkthrough Report
TCM	Tricon Communications Module
TRL	Technical Requirements List
TS1131	TriStation 1131
TSAP	TriStation Application Program
V&V	Verification and Validation

2. Life Cycle Processes

The DCPP PPS Replacement Project will utilize a modified waterfall life cycle model as identified below. The software life cycle applicable to this project is illustrated in Figures 1-8. The life cycle phases, as well as their inputs and outputs, are described in Sections 2.1 through 2.7.

The software life cycle applicable to this project is illustrated in Figures 1-8. The life cycle phases, as well as their inputs and outputs, are described in Sections 2.1 through 2.7.

The phases are as follows:

- Acquisition Phase – Request for Quote assistance and Purchase Order Review
- Planning Phase – Project Schedule, Planning Documents, Master Configuration List
- Requirements Phase – Software Requirements Specification, Hardware Requirements Specification, and Project Traceability Matrix.
- Design Phase – Software Design Description, Design Drawings, Project Traceability Matrix
- Implementation Phase – Project Software Application Development, Verification Document Development and Test Procedure/Test Cases execution, Hardware Assembly
- Test Phase – Acceptance Test Procedure Development, Project Traceability Matrix, Factory Acceptance Test Execution
- Delivery Phase – Package System for Shipment, Certificate of Conformance, System Shipment

The typical waterfall life cycle would continue with the Installation/Acceptance Testing Phase, Operation Phase, Maintenance Phase and Retirement Phase. These phases are not within the scope of the DCPP PPS Replacement Project for Invensys Operations Management and therefore are not included in the modified waterfall life cycle.

Phase Completion Meetings shall be held by the Project Review Committee (PRC) at the completion of the Requirements, Design, Implementation, and Test Phases. The PRC shall assess the risks and make recommendations for incorporating lessons learned prior to starting activities associated with the next project phase. The Project Review Committee (PRC) shall meet for project related activities, with the minimum PRC members for each activity as defined below:

PRC Members	Project Activities
PM, PE, PQAE, *IV&V/TD; Customer as	**Test Activities** – Approve test procedures, release for test, review and evaluate test results to determine acceptability of the tests, and to discuss any problems identified during the testing, e.g., test procedure problems (ICNs issued), test failures/test anomalies (SIDRs issued), etc.

applicable.	Additionally, any lessons learned should be discussed during the meeting.
PM, PE, PQAE, *IV&V/TD	**Phase Exit** - Review project activities associated with the major project phases (requirements, design, implementation, and test) and evaluate the risks and provide recommendations associated with lessons learned prior to entering the next project phase. The phase summary reports provide metrics that should be considered when evaluating the risks for entering the next project phase (see PPM 7.02 for phase summary report details).
PM, PE, PQAE, *IV&V/TD	**Other** - Review and/or evaluate additional project activities as deemed appropriate by the Project Manager.

*For testing activities, the Test Director for the specific activity (e.g., HVT, FAT, etc.) should represent Nuclear IV&V at the PRC meetings.

The PM is responsible for developing and issuing PRC meeting minutes which provide an overview of the PRC meeting.

When deemed appropriate by the Project Manager, a conditional release may be initiated to allow activities in a subsequent phase to be performed prior to completing activities in the current phase. Prior to approval, the conditional release shall be reviewed by the PRC, and the customer, as required.

Once a phase has been exited, minor changes to an approved document(s) may be processed with a successor document(s), e.g., the project is in the design phase and review of the SDD identifies minor changes to the SRS. In this case the SRS is not required to be approved prior to routing the SDD for review. The SRS and SDD can be routed for review together. Major revisions to documents shall follow the normal process. This will require exiting the phase, where the revision is identified, and returning to the phase where the document to be revised had originated.

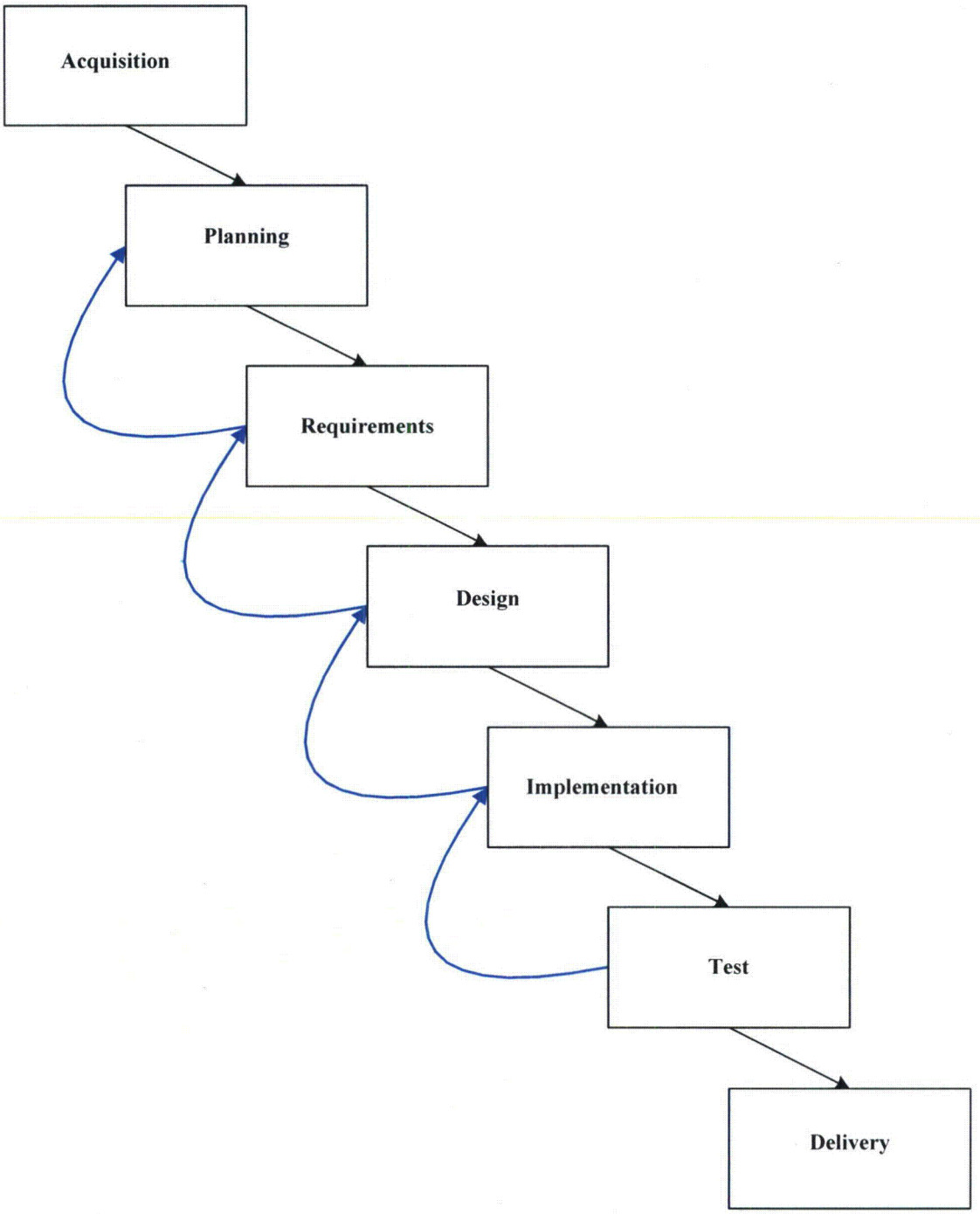

Figure 1. PPS Replacement Project Software Life Cycle Process Overview

P

P

P

P

2.1. Acquisition Phase

During the Acquisition Phase, the customer Request for Proposal and/or Purchase Order are received, reviewed. The Purchase Order Compliance Matrix (POCM) [Reference 1.3.3.6] is prepared. Initial budgets are created and bids submitted. These activities are performed by the Nuclear Project Delivery (ND) in support of the organization that prepares the proposal.

See Figure 2 for further details.

P

P

2.3. Requirements Phase

During the Requirements Phase the high level functional design requirements are translated into verifiable, traceable technical requirements that define the software required to operate the system. These requirements will be used directly in the design, verification, and validation of the software, system or equipment.

The Requirements Phase inputs, outputs, and activities are illustrated in Figure 4 .

P

P

2.4. Design Phase

This phase transforms the Software Requirements created in the Requirements Phase into detailed software design. The Software Architecture will also be defined and documented.

The Design Phase inputs, outputs, and activities are illustrated in Figure 5.

P

2.5. Implementation Phase

During the Implementation Phase, the software described in the SDD is translated into an application that will run on the Triconex platform. This application (PT2 file) is then turned over to Nuclear IV&V for verification testing.

The Implementation Phase inputs, outputs, and activities are illustrated in Figure 6.

P

P

2.6. Test Phase

The purpose of the Test Phase is to demonstrate the software performs the intended function by performing validation of the software on the target or production hardware. The Test Phase inputs, outputs, and activities are illustrated in Figure 7.

P

2.7. Delivery Phase

The Delivery Phase inputs, outputs, and activities are illustrated in Figure 8.

The purpose of the Delivery Phase is to prepare the system for shipment to the customer.

P

3. Methods, Tools and Techniques

3.1. Computing systems to be used for software development

Equipment and tools used by the Invensys Operations Management project team during the project lifecycle are listed below. Control of material (e.g., test equipment and safety-related V10 Tricon hardware) and equipment calibration (e.g., for hardware validation and factory acceptance testing) will be handled in accordance with the applicable PPM.

P

3.2. Methods

3.2.1. Independent Verification and Validation

Independent Verification and Validation shall be performed on software design outputs from each phase of the development process. Software for this project is Nuclear Safety Related and will be classified Software Integrity Level 4 (SIL-4) in accordance with the procedures provided in the SVVP.

3.2.2. Testing

Software testing is a process of technical investigation intended to ensure that the specification, design, and implementation of the software product are fault-free.

Nuclear IV&V has primary responsibility for developing the test documents and conducting the testing. The functional responsibilities of Nuclear IV&V are defined in the PMP.

3.2.3. Safety Analysis (Criticality/Hazard/Risk/Interface)

Safety Analysis (SA) shall be performed on software products as defined in the Software Safety Plan (SSP). The SA shall be performed by Nuclear IV&V in accordance with the SSP.

P

P

3.3. Tools

TS1131 is the tool to be used for development of software for the PG&E DCPP PPS Replacement Project.

Tools required for project execution, which include compilers, emulators, simulators, and hardware, shall be evaluated and documented as specified.

P

3.4. Development methods

3.5. Technical standards to be followed

See Section 4 for list of Standards.

3.6. Technical Documentation

Below is the list of the technical documents required for the development of the V10 Tricon Protection Set application code. The below list includes summary descriptions of the documents. The documents are identified by title and document number based on the numbering scheme in Appendix A of the PMP. Authors, reviewers, and approvers are also shown.

The PPS Replacement Project Software Verification and Validation Plan, 993754-1-802, provides additional details on the verification and validation activities performed by Nuclear IV&V. The Software Quality Assurance Plan, 993754-1-801, defines the quality affecting activities to be followed in the design, development, review, and testing for the PPS Replacement Project to ensure the specified quality requirements are met.

Requirements Phase:

4. Standards

The following documents are developmental references for this Plan:

- Title 10 of the Code of Federal Regulation Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants
- NUREG-0800, "Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants," Chapter 7, "Instrumentation and Controls," Revision 5
- NUREG-0800, "Standard Review Plan (SRP) for the Review of Safety Analysis Reports for Nuclear Power Plants," Branch Technical Position (BTP) 7-14 Revision 5, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- NUREG/CR-6101. "Software Reliability and Safety in Nuclear Reactor Protection Systems." 1993.
- NUREG/CR-6463, Revision 1, "Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems," August 1997
- RG 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
- RG 1.153, Revision 1, Criteria for Safety Systems
- RG 1.168, Revision 1, Verification, Validation, Reviews, and Audits For Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.169, Revision 0, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.170, Revision 0, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.171, Revision 0, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.172, Revision 0, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173, Revision 0, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- United States Nuclear Regulatory Commission (NRC) Digital Instrumentation and Controls Interim Staff Guidance 4, (DI&C ISG-04)
- United States Nuclear Regulatory Commission (NRC) Digital Instrumentation and Controls Interim Staff Guidance 6 (DI&C-ISG-06)
- Electric Power Research Institute (EPRI) TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996

- IEEE 7-4.3.2-2003, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- IEEE 603-1991 including correction sheet dated January 30, 1995, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- IEEE 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology
- IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans
- IEEE 828-1990, Standard for Software Configuration Management Plans
- IEEE 829-1983, Standard for Software Test Documentation
- IEEE 830-1993, IEEE Recommended Practice for Software Requirements Specifications
- IEEE 1008-1987, IEEE Standard for Software Unit Testing
- IEEE 1012-1998, Standard for Software Verification and Validation
- IEEE 1016-1998, IEEE Recommended Practice for Software Design Descriptions
- IEEE 1028-1997, Standard for Software Reviews
- IEEE 1042-1987, Guide to Software Configuration Management
- IEEE 1058.1-1987, IEEE Standard for Software Project Management Plans
- IEEE 1074-1995, IEEE Standard for Developing Software Life Cycle Processes
- IEEE 1219-1998, IEEE Standard for Software Maintenance
- IEEE 12207-1996, IEEE/Electronic Industries Alliance (EIA) Standard for Software Life Cycle Processes
- Purchase Order Compliance Matrix, 993754-1-800
- Technical Requirements List , 993754-1-808
- Project Management Plan, 993754-1-905
- Software Development Plan, 993754-1-906
- Project Risk Management Plan, 993754-1-908
- Project Quality Plan, 993754-1-900
- Software Quality Assurance Plan, 993754-1-801
- Software Configuration Management Plan, 993754-1-909
- Software Integration Plan, 993754-1-910
- Hardware Requirements Specification, 993754-1n[1]-807
- Software Requirements Specification, 993754-1n[1]-809
- System Architecture Description, 993754-1-914
- Software Design Description, 993754-1-810
- Software Verification and Validation Plan, 993754-1-802
- Software Safety Plan, 993754-1-911

- Validation Test Plan, 993754-1-813
- Software Verification Test Plan, 993754-1-868
- Hardware Validation Test Procedure, 993754-1n[1]-902-0
- Factory Acceptance Test Procedure, 993754-1n[1]-902-1
- Input/Output List, 993754-1-806
- V10 Tricon Protection Set Application Code, 993754-1n[1]-700
- Failure Modes and Effects Analysis, 993754-1-811
- Master Configuration List, 993754-1-803
- Project Traceability Matrix, 993754-1-804
- Triconex Project Procedures Manual