Project:	**PG&E PROCESS PROTECTION SYSTEM REPLACEMENT**
Purchase Order No.:	3500897372
Project Sales Order:	993754

PACIFIC GAS & ELECTRIC COMPANY

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

SAFETY ANALYSIS

Document No. 993754-1-915(-NP)

Revision 9

DECEMBER 9, 2014

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:	**Hoan Nguyen**		**V&V Engineer**
Reviewer:	**Dien Mai**		**V&V Engineer**
Approval:	**Kevin Vu**		**IV&V Manager**

Document Change History

Revision	Date	Change	Author
0	02/29/2012	Initial Issue for Use	Hoan Nguyen
1	10/24/2012		

P

Document Change History

Revision	Date	Change	Author
2	11/13/2013		

P

Document Change History

Revision	Date	Change	Author
3	01/28/2014		P
4	04/03/2014		P

Document Change History

Revision	Date	Change	Author
5	05/20/2014		P
6	07/03/2014		P
7	08/07/2014		P

Document Change History

Revision	Date	Change	Author
8	10/22/2014		P
9	12/09/2014		P

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1.0 Introduction

The Pacific Gas & Electric Company (PG&E) Westinghouse Eagle 21 Process Protection System (E21 PPS) for Diablo Canyon Power Plant (DCPP) Units 1 and 2 is to be replaced with the new Invensys Tricon-based Process Protection System (PPS). The new DCPP PPS is capable of monitoring the required parameters, comparing them against set points and providing signals to the external interfaces if operating limits are exceeded. The PPS comprises four Protection Sets. The Protection Sets (I through IV) each comprises three main hardware components such as the Tricon V10, the Westinghouse Advanced Logic System (ALS) platform, and the Maintenance Workstation (MWS).

The PPS will provide:

- Trip and actuation signals to the Solid State Protection System (SSPS) for initiating reactor trip and or ESFAS actuation
- Analog output of plant parameters to the Main Control Room (MCR) for recording and/or indication
- Plant parameters to the Plant Process Computer (PPC) for monitoring
- Output signals to the Main Annunciator System (MAS) for alarming

The primary functionality provided by the new PPS will include:

- Monitor Reactor Coolant System Temperature and Pressure, S/G Level and Pressurizer Level
- Provide signal isolation for process inputs(without processing)
- Perform Safety functions
- Signal Reactor Trips and/or ESFAS actuations

This functionality will be implemented in four TriStation Application Programs (TSAPs), one for each of the four separate PPS Protection Sets. The TSAPs will be downloaded to and executed by the Tricon 3008N main processors.

The PPS is classified as nuclear safety-related.

1.1 Purpose

This report documents the methodology and results of the Safety Analysis. The Safety Analysis report consists of the Interface Analysis, the Criticality Analysis, the Hazard Analysis, and the Risk Analysis. Based on the guidance of IEEE Std 1012-1998 [Reference 2.3.6] , the Safety Analysis is created at the Requirement Phase of the DCPP PPS project and updated incrementally in the subsequent Design Phase, Implementation Phase and Test Phase.

The Interface Analysis is a structured evaluation of the software interfaces with hardware, user, and other PPS components for potential hazards resulting from insufficient interface definitions and/or poor interface design.

The Criticality Analysis is a structured evaluation of the assigned Software Integrity Level (SIL) of the PPS software with regard to undesirable consequences resulting from an incorrect SIL assigned to the deliverables.

The Hazard and Risk Analyses are qualitative or quantitative evaluations of the Protection Set software for undesirable outcome(s) resulting from development defects or erroneous operation of the PPS. The possible outcome(s) include injury, illness, death, mission failure, economic loss, property loss, environmental loss, or adverse social impact. The evaluation includes screening or analysis methods to categorize, eliminate, reduce, and/or mitigate hazards.

The analyses will be used together to examine the role of Tricon Protection Set software in the overall PPS system and its impact on the operation of the PPS. The ultimate objectives of the Safety Analysis program are to identify and correct deficiencies and to provide information on the necessary safeguards to prevent failure and/or mitigate deleterious consequences.

1.2 Scope

The scope of this Safety Analysis is limited to the delivered PPS equipment as defined in the Software Requirements Specification (SRS). However, as the Preliminary Hazard Analysis (PHA) has wider coverage, certain aspects of the analysis will contain information that falls outside the delivered system. Information of this nature will be identified as such.

The delivered system can be broken into hardware and software. Analysis of the V10 Tricon hardware is discussed in details in the Failure Modes and Effects Analysis (FMEA) for the platform [Reference2.2.2] and NTX-SER-09-10 [Reference 2.2.12]. FMEA for DCPP PPS configuration will be developed later in a separate document.

Figure 1 illustrates the scope of Safety Analysis. Only safety impact of the Tricon Protection Set software (also called TSAP) will be addressed in this Safety Analysis.

Safety impact of the Westinghouse Advanced Logic System (ALS) software and the Maintenance Workstation (MWS) software are not within the scope of this Safety Analysis.

The scope of the Safety Analysis is discussed in depth in the associated, subsequent subsections under Interface, Hazard, Criticality and Risk Analysis.

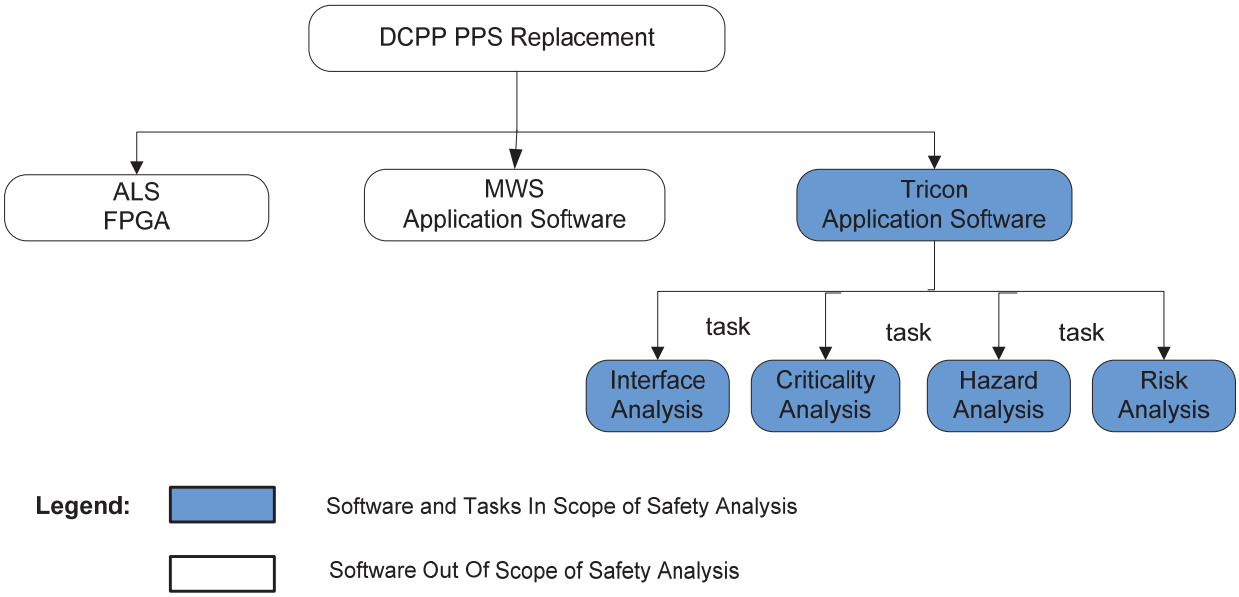

Figure 1 – Scope of Safety Analysis

2.0 References

2.1 PPS Documents

2.1.1 PPS Interface Requirements Specification Rev 9
2.1.2 08-0015-SP-001, PPS Functional Requirements Specification Rev 9
2.1.3 [DELETED]

2.2 Invensys Documents

2.2.1 7286-545-1, V10 Tricon Topical Report- Application Guide, Appendix B
2.2.2 9600164-531, Failure Modes and Effects Analysis (FMEA) for Tricon version 10.2 Programmable Logic Controller
2.2.3 9600164-532, Reliability / Availability Study for Tricon version 10 Programmable Logic Controller
2.2.4 [DELETED]
2.2.5 9700100-012, TriStation 1131 Developer's Workbench
2.2.6 [DELETED]
2.2.7 [DELETED]
2.2.8 993754-11-809, PPS Software Requirements Specification
2.2.9 [DELETED]
2.2.10 [DELETED]
2.2.11 [DELETED]
2.2.12 NTX-SER-09-10, Tricon V10 Conformance to ISG-04
2.2.13 993754-1-817, Maximum TSAP Scan Time
2.2.14 993754-11-810, PPS Software Design Description Protection Set I
2.2.15 993754-1-811, PPS Failure Modes and Effect Analysis
2.2.16 993754-1-819, Reliability Analysis
2.2.17 993754-1-830, TAB-PAN-TAN Review
2.2.18 7286-545-1, Triconex Topical Report
2.2.19 993754-1-907, Software Development Plan Coding Guidelines
2.2.20 993754-11-700 PGE DCPP PPS (TSAP)
2.2.21 993754-11-902-1 Protection Set I FAT Procedure
2.2.22 993754-11-902-0 Protection Set I HVT Procedure
2.2.23 993754-12-810, Software Design Description PPSII-IV
2.2.24 993754-12-700 PGE DCPP PPS (TSAP)
2.2.25 993754-13-700 PGE DCPP PPS (TSAP)
2.2.26 993754-14-700 PGE DCPP PPS (TSAP)
2.2.27 993754-12-SWR-45 Software Walkthrough Report
2.2.28 993754-13-SWR-46 Software Walkthrough Report
2.2.29 993754-14-SWR-47 Software Walkthrough Report

2.3 Miscellaneous Documents

2.3.1 CEI/IEC 300-3-9, Dependability Management, Part 3 – Section 9: Risk Analysis of Technological Systems

2.3.2 NUREG-0492, Fault Tree Handbook

2.3.3 NUREG/CR-6430, Software Safety Hazard Analysis

2.3.4 Regulatory Guide 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants

2.3.5 RG 1.53, Application of the Single-Failure Criterion to Safety Systems

2.3.6 IEEE Standard 1012-1998, IEEE Standard for Software Verification and Validation

2.3.7 NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems

2.3.8 BTP 7-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

3.0 Abbreviations, Acronyms and Definitions

3.1 Abbreviations and Acronyms

ALS	Advanced Logic System
BTP	Branch Technical Position
CRC	Cyclic Redundancy Code
DCPP	Diablo Canyon Power Plant
DDE	Dynamic Data Exchange
Delta-T	Differential (Reactor) Coolant Temperature
DTTA	DeltaT/Tavg (Differential Temperature & Average Temperature)
ETA	External Termination Assembly
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis (in the context of a Preliminary Hazard Analysis)
IEEE	Institute of Electrical and Electronics Engineers
HVT	Hardware Validation Test
I/O	Input/Output
IV&V	Independent Verification & Validation
KVM	Keyboard, Video Display, and Mouse
MAS	Main Annunciator System
MCR	Main Control Room
MP	Main Processor
MWS	Maintenance Workstation
M&TE	Measuring and Test Equipment
NIS	Nuclear Instrument System
NRC	US Nuclear Regulatory Commission
NUREG	US Nuclear Regulatory Commission Regulation
OOS	Out of Service
OTDT	Overtemperature Delta-Temperature
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PG&E	Pacific Gas & Electric Company
PPC	Plant Process Computer

PPS	Process Protection System
RNARA	Rack Nuclear Auxiliary Relay A
RNASA	Rack Nuclear Auxiliary Safeguards A
RTD	Resistance Temperature Detector
RXM	Remote Extender Modules
SIL	Software Integrity Level
SRS	Software Requirements Specification
SSPS	Solid State Protection System
TCM	Tricon Communication Module
TS1131	TriStation 1131 Developer Workbench
TSAA	Tricon System Access Application
TSAP	TriStation Application Program
TSX	Tricon Operating System

3.2 Definitions

Accident	An undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss
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.
Incident	An event that involves no loss (or only minor loss) but with the potential for loss under different circumstances
Hazard	A state or set of conditions that, together with other conditions in the environment, will lead to an accident (loss event).
Hazard Identification	Process of recognizing that a hazard exists and defining its characteristics.
Risk	Combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.
Risk Analysis	Systematic use of available information to identify hazards and to estimate the risk to individual or populations, property or the environment.
Safety	Freedom from accidents or losses.
Trip	Reactor Trip or ESFAS Actuation signal.

4.0 Preliminary Hazard Analysis

The Preliminary Hazard Analysis (PHA) is performed by Invensys Operations Management IV&V engineers at the Requirements Phase based on guidance contained in NUREG/CR-6430 [Reference 2.3.3]. The PHA is updated in the Design Phase and Implementation Phase per NUREG/CR-6430, and additional hazards may be identified in the subsequent phases.

The PHA identifies possible hazards to the PPS, evaluates each of the hazards and describes their expected impact of the Invensys Tricon-based Protection Set software functionality. The expected impact of Westinghouse ALS FPGA and MWS software functionality are not within the scope of this analysis.

The PHA process uses the Fault Tree Analysis (FTA) method. The analysis is performed in the Requirements Phase of the project life cycle to identify the basic events that could potentially lead to a hazard. The process of focusing on a particular undesired event and the Fault Tree construction is based on the guidance of NUREG-0492 [Reference 2.3.2].

FTA is based on analysis of the logical system architecture illustrated in Figure 2. The FTA diagram below comprises rectangles that represent factors that could contribute to hazards and circles that represent basic events. The TOP LEVEL HAZARD is the failure of the PPS Tricon Protection Set software (TSAP):

- To send Class I trip signals to the SSPS
- To annunciate Class II Trouble/Failure Alarms at the MAS

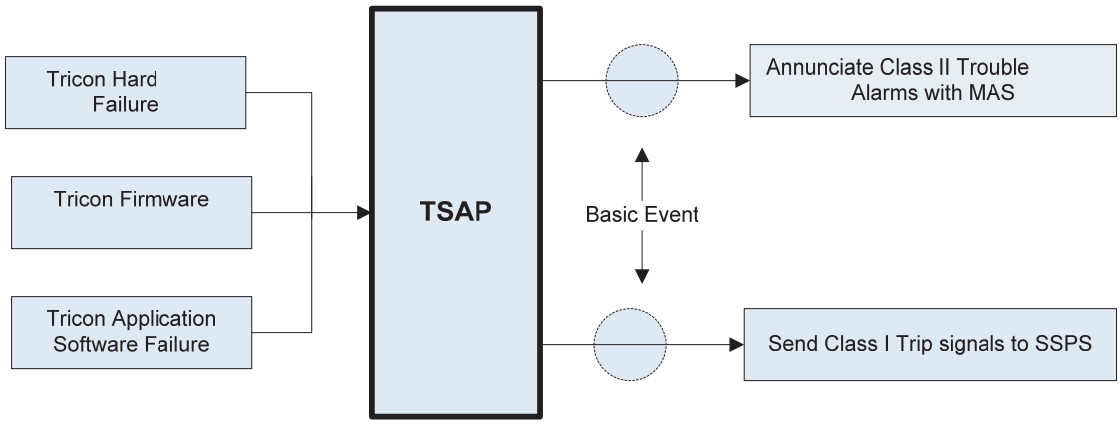

Figure 2 – Identification of TOP LEVEL HAZARD

- Class I Trip signals are discrete outputs from the safety-related Tricon Primary RXM Chassis in each Protection Set. See Section 3.1.1.2.1 in SRS Protection Set I, II, III, and IV for a complete listing of partial trip signals in four Protection Sets.
- Class II Trouble or Failure Alarms are discrete outputs from the non-safety-related Tricon Remote RXM chassis in each Protection Set. See Section 3.1.1.2.8.1 in SRS for a complete listing of Trouble or Failure Alarms in four Protection Sets.

Design and Instrument Class are defined as follows in the PG&E FRS [Reference 2.1.2]:

Table 1. Design and Instrument Class

Term	Definition
Instrument Class IA	Instrument Class IA instruments and controls are those that initiate and maintain safe shutdown of the reactor, mitigate the consequences of an accident, or prevent exceeding 10 CFR 100 off-site dose limits.
Instrument Class IB	Class IB instruments and controls are those that are required for post-accident monitoring of Category 1 and 2 variables in accordance with Regulatory Guide 1.97, Revision 3.
Instrument Class II	Instrument Class II components are Design Class II devices with non-safety-related functions. However, certain Class II components are subjected to some graded quality assurance requirements.

P

P

P

P

P

4.1 Preliminary Hazard List

The following Preliminary Hazard List (PHL) documents the basic events elaborated during the FTA and ties each event to a potential hazardous consequence.

Three elements comprising a hazard are identified in the PHL:

- **Basic Event**: indicates source of the hazard
- **Causal Factor**: describes initiating mechanism
- **Consequence**: describes impacts on the PPS which TSAP in each Protection Set might have

P

4.2 Results

P

5.0 Interface Analysis

5.1 Purpose

5.1.1 Requirements Interface Analysis

The Interface Analysis is intended to verify and validate the requirements for the Protection Set software interfaces with hardware, user, operator, and other systems. The following criteria will be used for verifying and validating the interface requirements:

- Correctness
- Consistency
- Completeness
- Accuracy
- Testability

See IEEE Std 1012-1998 for definition of the above criteria.

Input documents to the Interface Analysis are:

1) PPS Replacement Interface Requirements Specification (IRS) [Reference 2.1.1]
2) PPS Replacement Functional Requirements Specification (FRS) [Reference 2.1.2]
3) Software Requirements Specification (SRS) [Reference 2.2.8]

There is no separate Invensys Interface Requirements Specification. It is a part of the Invensys SRS, Section 3.1 (External Interface Requirements).

The Interface Analysis is prepared based on the guidance of IEEE Std 1012-1998.

5.1.2 Design Interface Analysis

The Interface Analysis is intended to verify and validate the Protection Set software design interfaces with hardware, user, operator, and other software. The IEEE 1012-1998 criteria below will be used for verifying and validating the interface designs:

- Correctness
- Consistency
- Completeness
- Accuracy
- Testability

In addition, this section also intends to satisfy NUREG/CR-6101- recommended Design Interface Analysis. It will verify that the interfaces among the design elements in each PPS Protection Set have been properly designed and do not introduce a safety hazard.

Input documents to the Interface Analysis are:

1) PPS Replacement Interface Requirements Specification (IRS) [Reference 2.1.1]
2) Software Requirements Specification (SRS) [Reference 2.2.8]
3) Software Design Descriptions (SDD) [Reference 2.2.14]

There is no separate Invensys Interface Design Specification. It is a part of the Invensys SDD.

The Interface Analysis is prepared based on the guidance of IEEE Std 1012-1998 and NUREG/CR-6101 [Reference 2.3.7].

5.2 Scope

5.2.1 Requirements Interface Analysis

The scope of the Interface Analysis is limited to verifying and validating the interface requirements for the Protection Set software (also known as TSAP). The interface requirements consist of the following six entities that the Protection Set TSAP interfaces with:

P

P

P

P

P

P

P

5.3 Output

Outputs of the Interface Analysis are an IV&V Task Report and a list of hazards. The Task Report is documented in this section.

5.3.1 Interface Analysis Task Report

Requirement Phase – PG&E Design Inputs Rev 9, SET I, II, III, IV

The Interface Analysis task in the Requirement Phase Revisited was based on the following input documents:

1) 993754-11-809 SRS revision 4
2) PG&E FRS revision 9
3) PG&E IRS revision 9

IV&V performed the Interface Analysis by reviewing the Rev 9-based requirements in one SRS. The evaluation criteria are to verify and validate the requirements for the Protection Set software interfaces with hardware, user, operator, and other systems for correctness, consistency, completeness, accuracy, and testability. The evaluation result is that the criteria are met and no new interface hazard is identified.

Design Phase – PG&E Design Inputs Rev 9, SET I

The Interface Analysis task in the Design Phase Revisited was based on the following input documents:

1) 993754-11-810 SDD revision 2
2) PG&E FRS revision 9
3) PG&E IRS revision 9
4) CD-ER 993754-27, CD-ER 993754-28 and CD-ER 993754-29

IV&V performed the Interface Analysis by reviewing the Rev 9-based detailed design elements in the SDD. The evaluation criteria are to verify and validate that the PPSI software design interfaces with hardware, software and other components for correctness, consistency, completeness, accuracy, and testability in accordance with IEEE 1012-1998 guidance on Design V&V Interface Analysis activity. The evaluation result is that the criteria are met and no new interface hazard is identified.

Implementation Phase – PG&E Design Inputs Rev 9, SET I

The Interface Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-11-810 PPSI SDD revision 3
2) 993754-11-700 PGE DCPP PPS rev 1

The Interface Analysis was performed by analyzing the PPSI TSAP to identify potential hazards. The evaluation criteria are to verify that the PPSI TSAP source code interfaces with hardware, software and other components for correctness, consistency, completeness, accuracy and testability in accordance with IEEE 1012-1998 guidance on Implementation Phase V&V Hazard Analysis activity. The evaluation result is that the criteria are met and no new interface hazard is identified.

Design Phase – PG&E Design Inputs Rev 9, SET II, III, IV

The Interface Analysis task in the PPSII – IV Design Phase was based on the following input documents:

1) 993754-12-810 SDD PPS II – IV revision 0 [Reference 2.2.23]
2) PG&E FRS revision 9
3) PG&E IRS revision 9

IV&V performed the Interface Analysis by reviewing the delta changes between PPSI design elements and those for PPSII, III and IV. The evaluation criteria are to verify and validate that the PPSII - IV software design interfaces with hardware, software and other components for correctness, consistency, completeness, accuracy, and testability in accordance with IEEE 1012-1998 guidance on Design V&V Interface Analysis activity. The evaluation result is that the criteria are met and no new interface hazard is identified.

Implementation Phase – PG&E Design Inputs Rev 9, SET II, III, IV

The Interface Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-12-810 SDD PPSII-IV revision 1
2) 993754-12-700 PGE DCPP PPS (TSAP)
3) 993754-13-700 PGE DCPP PPS (TSAP)
4) 993754-14-700 PGE DCPP PPS (TSAP)
5) 993754-12-SWR-45 Software Walkthrough Report
6) 993754-13-SWR-46 Software Walkthrough Report
7) 993754-14-SWR-47 Software Walkthrough Report

The Interface Analysis was performed by analyzing the PPSII – IV TSAP and based on findings from IV&V Software Code Walk-throughs to identify potential hazards. The evaluation criteria are to verify that the PPSII – IV TSAP source code interfaces with hardware, software and other components for correctness, consistency, completeness, accuracy and testability in accordance with IEEE 1012-1998 guidance on Implementation Phase V&V Hazard Analysis activity. The evaluation result is that the criteria are met and no new interface hazard is identified.

5.3.2 List of Interface Hazards

Each hazard is uniquely identified by an ID, namely H-<number>(alphabetic character). The Hazard ID is tied to a specific requirement number in the SRS, namely R-<number>.

The hazard ID will be used by the Hazard Tracking mechanism to track each hazard status and its mitigation in each phase of the Protection Sets software development.

Table 5. List of Interface Hazard

P

P

6.0 Criticality Analysis

6.1 Purpose

6.1.1 Requirements Criticality Analysis

The Requirement-Phase Criticality Analysis is intended to review and verify the software integrity level of the Protection Set software components.

The Software Integrity Level (SIL) of the Protection Set software is established as SIL-4 because the functionality of the replacement PPS application software, as specified in the FRS, affects the critical performance of the nuclear-safety-related Reactor Trip and Engineered Safety Features functions.

The individual Protection Set software components at the Requirement Phase are the Invensys Software Requirements Specifications (SRS) for Protection Set I, II, III, and IV.

Because the Protection Set software was already assigned SIL-4, its SRSs must be also assigned SIL-4.

Table 6. Application Software Integrity Level

SOFTWARE COMPONENTS	SIL
Software Requirements Specifications (SRS)	4

Input documents to the Criticality Analysis are:

1) PG&E PPS IRS
2) PG&E PPS FRS
3) Invensys SRSs (Protection Set I, II, III, IV)

The Criticality Analysis is prepared based on the guidance of IEEE Std 1012-1998.

6.1.2 Design Criticality Analysis

The Design-Phase Criticality Analysis is intended to review and verify the SIL of the Protection Set software components. Invensys Tricon Interface technologies and the prior Criticality Task Report do not cause the PG&E-assigned SIL-4 to be lowered for the software components.

The individual Protection Set software components at the Design Phase are the Invensys Software Design Description (SDD) for Protection Set I.

SOFTWARE COMPONENTS	SIL
Software Design Description (SDD)	4

Input documents to the Criticality Analysis are:

1) Invensys SDDs (Protection Set I)

The Criticality Analysis is prepared based on the guidance of IEEE Std 1012-1998.

6.2 Scope

6.2.1 Requirements Criticality Analysis

The scope of the Criticality Analysis is limited to reviewing and verifying the software integrity level of the Tricon Protection Set software and its individual components.

The ALS and MWS software components are not in the scope of this analysis.

6.2.2 Design Criticality Analysis

It has the same scope as the Requirements Criticality Analysis.

6.3 Output

Output of the Criticality Analysis is an IV&V Task Report and it is documented in this section.

6.3.1 Criticality Analysis Task Report

Requirement Phase – PG&E Design Inputs Rev 9, SET I, II, III, IV

The Criticality Analysis task in the Requirement Phase Revisited was based on the following input documents:

1) 993754-11-809 SRS revision 4
2) PG&E FRS revision 9
3) PG&E IRS revision 9

The Criticality Analysis was conducted in the Requirements Phase Revisited using one SRS. As the Diablo Canyon project is moving from Rev 5 to Rev 9, the SRS is re-structured to capture the requirements common for all four Protection Sets and the delta changes applicable to each Protection Set.

The evaluation criterion is to verify the SIL assignment of the SRS for correctness. The result of the evaluation is that the SIL-4 assignment is correct. No anomaly was found. It is recommended that the software components at the Design Phase be maintained at the same SIL, i.e., SIL-4 even with PG&E design input changes.

Design Phase – PG&E Design Inputs Rev 9, SET I

The Criticality Analysis task in the Design Phase Revisited was based on the following input documents:

1) 993754-11-810 SDD revision 2
2) PG&E FRS revision 9
3) PG&E IRS revision 9
4) CD-ER 993754-27, CD-ER 993754-28 and CD-ER 993754-29

The evaluation criteria are to verify that the software design, implementation methods, and interfacing technologies don't cause previously-assigned software integrity levels to be

raised or lowered for a software element in accordance with IEEE 1012-1998 guidance on Design V&V Criticality Analysis activity.

The evaluation result is that the criteria are met with no inconsistent or undesired software integrity consequences introduced in the Design Phase Revisited.

Implementation Phase – PG&E Design Inputs Rev 9, SET I

The Criticality Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-11-810 PPSI SDD revision 3
2) 993754-11-700 PGE DCPP PPS rev 1

The evaluation criteria are to verify that the PPSI TSAP source codes don't cause previously-assigned software integrity levels to be raised or lowered for a software element in accordance with IEEE 1012-1998 guidance on Implementation V&V Criticality Analysis activity. The evaluation result is that the criteria are met with no inconsistent or undesired software integrity consequences introduced in the Implementation Phase.

Design Phase – PG&E Design Inputs Rev 9, SET II, III, IV

The Criticality Analysis task in the PPSII – IV Design Phase was based on the following input documents:

1) 993754-12-810 SDD revision 0
2) PG&E FRS revision 9
3) PG&E IRS revision 9

The evaluation criteria are to verify that the differences between PPSI and PPSII, III, and IV in software design, implementation methods, and interfacing technologies don't cause previously-assigned software integrity levels to be raised or lowered for a software element in accordance with IEEE 1012-1998 guidance on Design V&V Criticality Analysis activity.

The evaluation result is that the criteria are met with no inconsistent or undesired software integrity consequences introduced in the PPSII- IV Design Phase.

Implementation Phase – PG&E Design Inputs Rev 9, SET II, III and IV

The Criticality Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-12-810 SDD PPSII-IV revision 1
2) 993754-12-700 PGE DCPP PPS (TSAP)
3) 993754-13-700 PGE DCPP PPS (TSAP)
4) 993754-14-700 PGE DCPP PPS (TSAP)
5) 993754-12-SWR-45 Software Walkthrough Report
6) 993754-13-SWR-46 Software Walkthrough Report
7) 993754-14-SWR-47 Software Walkthrough Report

The evaluation criteria are to verify that the PPSII, III, IV TSAP source codes don't cause previously-assigned software integrity levels to be raised or lowered for a software element in accordance with IEEE 1012-1998 guidance on Implementation V&V Criticality Analysis activity. The evaluation result is that the criteria are met with no inconsistent or undesired software integrity consequences introduced in the Implementation Phase.

7.0 Hazard Analysis

7.1 Purpose

7.1.1 Requirements Hazard Analysis

The Hazard Analysis is intended to identify the Protection Set software requirements that contribute to the PPS Replacement hazards and validate that the software addresses and mitigates each hazard.

The functional requirements within the four SRSs have been analyzed with guidance from IEEE Std 1012-1998 and NUREG/CR-6430, Section 3.

Input documents to the Hazard Analysis are:

1) PG&E PPS IRS
2) PG&E PPS FRS
3) Invensys SRSs (Protection Set I, II, III, IV)
4) Invensys Maximum TSAP Scan Time [Reference 2.2.13]

The objective of the assessment below is to analyze and evaluate all software command-triggered or hardware switch-triggered bypassed, tripped and incident conditions to identify potential hazards of the Tricon Protection Set. The Tricon Protection Set software deviating from requirement specifications could lead to an inadvertent or unintended response by PG&E plant operation; in that manner it facilitates a hazard. Total thirty one (31) conditions are divided into six (6) groups. Conditions with the same current state belong to the same group.

Result of the assessment is the identification of one new hazard.

The following notes are used in the assessment:

1) **Current State**: denotes the existing condition of a protective function right before the request is made.
2) **Request**: refers to plant operator's attempt to place a protective function/channel out-of-service for online test and maintenance.
3) **Incident**: refers to the happening of a non-deliberate action (e.g. detectable Tricon hardware component failures).
4) **Intended Behavior**: refers to the following two circumstances:
   - In many conditions, the Tricon Protection Set supposes to behave correctly because the stated behaviors follow the PG&E design inputs (stated in FRS and IRS sections) and Invensys software requirement specifications.

- The presumption of how the Tricon Protection Set would behave as if intended by PG&E design. The presumptions are made for several conditions due to lack of the PG&E sections or Invensys explicit software requirements.

5) **Fatal Diagnostic**: a detectable failure that could result in loss of ability to perform a safety function.

6) **Comparator Output**: Raw out signal from the software comparator.

7) **Tricon Output**: Discrete output from the Tricon

8) **Bistable Output**: Discrete output from the PPS Rack (Input to SSPS).

P

P

P

P

P

P

P

7.1.2 Design Hazard Analysis

The Hazard Analysis is intended to verify that logic design and associated data elements correctly implement the PPS software requirements and introduce no new hazard in accordance with IEEE 1012-1998 guidance.

The Hazard Analysis also intends to satisfy the following four NUREG/CR-6101-recommended analyses:

- Design Logic Analysis – to determine whether the PPS software design algorithms and control logic correctly implement the Protection Set safety requirements.
- Design Data Analysis – to determine whether the PPS data-related design elements are consistent with the Protection Set software requirements.
- Design Constraint Analysis – to evaluate restrictions imposed on the PPS software requirements if any by the design of the PPS software system, and determines that no new safety hazards have been created.
- Timing and Sizing Analysis – to evaluate whether there are sufficient resources to satisfy the timing and sizing requirements.

Input documents to the Hazard Analysis are:

1) Invensys SDDs (Protection Set I)
2) PPS Failure Modes and Effects Analysis [Reference 2.2.15]
3) Reliability Analysis [Reference 2.2.16]
4) Invensys Maximum TSAP Scan Time

P

7.1.2.1 Design Logic Analysis

P

P

P

P

P

P

P

P

P

P

P

P

P

P

7.1.3 Implementation Phase Analysis

The Hazard Analysis is intended to verify that the PPSI TSAP source codes correctly implement the PPS software design elements and introduce no new hazards. The hazard analysis process in this phase is performed in accordance with NUREG/CR-6101 guidance, which is based on guidelines in BTP 7-14 [Reference 2.3.8].

Input documents to the Hazard Analysis in the Implementation Phase are:

1) PPSI SDD
2) PPSI TSAP [Reference 2.2.20]
3) Maximum TSAP Scan Time

The Hazard Analysis also intends to satisfy the following four NUREG/CR-6101-recommended analyses:

- Code Logic Analysis – to determine whether the PPSI TSAP correctly implements the PPSI software design.
- Code Data Analysis – to determine whether the definitions of TSAP tagnames correctly implement the PPSI I/O design.
- Code Interface Analysis – to verify the compatibility of internal and external interfaces among software components (TSAP Custom Function Blocks and Program Modules) and other PPSI system component (MWS software).
- Code Constraint Analysis – to ensure the PPSI TSAP operates within the constraints imposed by the application performance requirements and the PPSI software design.

7.1.3.1 Code Logic Analysis

The Code Logic Analysis evaluates the sequence of operations presented by the Structured-Text (ST) and Function Block Diagram (FBD) codes of the PPSI TSAP to identify hazards and safety violations. The potential hazards in the Implementation Phase would be software failures that cause TSAP to produce incorrect or unexpected results and/or scan overrun.

The codes in Custom Function Blocks and Program Modules are analyzed for the common causes of software failures. Also included is the discussion of how a potential hazard associated with each common cause is mitigated in the specific implementation.

P

P

P

7.1.3.3 Code Interface Analysis

Internal and external interfaces are evaluated to ensure their implementations are consistent with the TSAP interface design and do not create a potential hazard.

P

7.1.4 Test Phase Analysis

The Hazard Analysis is intended to verify the PPSI test instrumentation does not introduce new hazards. The hazard analysis process in this phase is performed in accordance with IEEE 1012-1998 guidance.

Input documents to the Hazard Analysis in the Test Phase include:

1) PPSI TSAP [Reference 2.2.20]
2) PPSI FAT procedure [Reference 2.2.21]
3) PPSI HVT procedure [Reference 2.2.22]

The potential hazards in the Test Phase could be created with the validation testing tools and methods capable of altering the TSAP logics while the TSAP is running on a real hardware. Six validation tools and methods are analyzed below for hazard identification. Also included is the discussion of how a potential hazard is mitigated in the specific validation method.

P

7.2 Scope

The scope of the Hazard Analysis is limited to analyzing the Tricon Protection Set requirements that could potentially cause system hazards.

The ALS-related functional or performance requirements are not evaluated for hazards in this analysis.

The functional and performance requirements that specify the MWS in normal operation are not evaluated for hazards in this analysis.

7.3 Output

Outputs of the Hazard Analysis are an IV&V Task Report and a set of hazard lists. The Task Report is documented in this section.

7.3.1 Hazard Analysis Task Report

Requirement Phase – PG&E Design Inputs Rev 9, SET I, II, III, IV

The Hazard Analysis task conducted in the Requirement Phase Revisited was based on the following input documents:

1) 993754-11-809 SRS revision 4
2) PG&E PPS FRS revision 9
3) PG&E IRS revision 9

The Hazard Analysis was performed by analyzing the Rev 9-based functional requirements in one SRS for potential hazard identifications. As the Diablo Canyon project is moving from Rev 5 to Rev 9, the SRS is re-structured to capture the requirements common for all four Protection Sets and the delta changes applicable to each Protection Set.

The evaluation criteria are to analyze the software requirements for satisfying software qualities relating to potential hazards such as Accuracy, Capacity, Functionality, Reliability, Robustness, Safety and Security per guidance from NUREG/CR-6430, Section 3 – Requirement Hazard Analysis.

PG&E Cyper Security policy is beyond the scope of this document because it is implemented in MWS.

The evaluation result includes the identification of one new hazard (see detail for H-6 in Section 7.3.2) and closure of two Rev 5-based hazards (see details for H-4 and H-5 in Section 8.3.2).

Design Phase – PG&E Design Inputs Rev 9, SET I

The Hazard Analysis task conducted in the Design Phase Revisited was based on the following input documents:

a. 993754-11-810 SDD revision 2
b. PG&E PPS FRS revision 9
c. PG&E IRS revision 9
d. CD-ER 993754-27, CD-ER 993754-28 and CD-ER 993754-29

The Hazard Analysis was performed by analyzing the Rev 9-based detailed designs in the SDD for potential hazard identifications. The evaluation criteria are to verify that the software design and associated data elements correctly implement the critical requirements and introduce no new hazards in accordance with IEEE 1012-1998 guidance on Design V&V Hazard Analysis activity.

The evaluation result includes the closure of one Rev 9-based hazard (see detail for H-6 in Section 7.3.2). No new hazard is identified in the Design Phase Revisited.

Implementation Phase – PG&E Design Inputs Rev 9, SET I

The Hazard Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-11-810 PPSI SDD revision 3
2) 993754-11-700 PGE DCPP PPS rev 1
3) 993754-1-817 Maximum TSAP Scan Time revision 1

The Hazard Analysis was performed by analyzing the Rev 9-based Structured Texts and Function Block Diagrams in the PPSI TSAP for potential hazard identifications. The evaluation criteria are to verify that the PPSI TSAP source codes correctly implement the PPSI software design elements and introduce no new hazards in accordance with IEEE 1012-1998 guidance on Implementation V&V Hazard Analysis activity. The evaluation result is that no new hazards were identified in the Implementation Phase.

Test Phase – PG&E Design Inputs Rev 9, SET I

The Hazard Analysis task conducted in the Test Phase was based on the following input documents:

1) 993754-11-700 PGE DCPP PPS rev 3
2) 993754-11-902-1 PPSI FAT Procedure
3) 993754-11-902-0 PPSI HVT Procedure

The Hazard Analysis was performed by analyzing the validation tools and methods for potential hazard identifications. The evaluation criterion is to verify that the test instrumentation does not introduce new hazards in accordance with IEEE 1012-1998 guidance on Test V&V Hazard Analysis activity. The evaluation result is that no new hazard was identified in the Test Phase.

Design Phase – PG&E Design Inputs Rev 9, SET II, III, IV

The Hazard Analysis task conducted in the PPSII – IV Design Phase was based on the following input documents:

1) 993754-12-810 SDD PPS II - IV revision 0
2) PG&E PPS FRS revision 9
3) PG&E IRS revision 9

The Hazard Analysis was performed by analyzing the delta changes between PPSI design and that for PPS II, III, and IV to identify potential hazards. In general, the PPSI hazard analysis and mitigation discussion in Section 7.1.2 (Design Hazard Analysis) is also applicable to the PPS II, III and IV.

The evaluation criteria are to verify that the software design differences between PPSI and PPSII, III and IV correctly implement the critical requirements and introduce no new hazards in accordance with IEEE 1012-1998 guidance on Design V&V Hazard Analysis activity.

The evaluation result is that no new hazard is identified in the PPSII – IV Design Phase.

Implementation Phase – PG&E Design Inputs Rev 9, SET II, III and IV

The Hazard Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-12-810 SDD PPSII-IV revision 1
2) 993754-12-700 PGE DCPP PPS (TSAP)
3) 993754-13-700 PGE DCPP PPS (TSAP)
4) 993754-14-700 PGE DCPP PPS (TSAP)
5) 993754-1-817 Maximum TSAP Scan Time revision 1
6) 993754-12-SWR-45 Software Walkthrough Report
7) 993754-13-SWR-46 Software Walkthrough Report
8) 993754-14-SWR-47 Software Walkthrough Report

Deficiency findings from the IV&V Software Code Walk-throughs [Reference 2.2.27 through 2.2.29] were evaluated for potential hazard identifications.

P

The evaluation result is that no new hazards were identified in the PPSII – IV Implementation Phase.

Test Phase – PG&E Design Inputs Rev 9, SET II, III and IV

The Hazard Analysis task conducted in the Test Phase was based on the following input documents:

1) 993754-12-700 PGE DCPP PPS
2) 993754-13-700 PGE DCPP PPS
3) 993754-14-700 PGE DCPP PPS
4) 993754-12-902-1 PPSII FAT Procedure
5) 993754-13-902-1 PPSIII FAT Procedure
6) 993754-14-902-1 PPSIV FAT Procedure
7) 993754-12-902-0 PPSII HVT Procedure
8) 993754-13-902-0 PPSIII HVT Procedure
9) 993754-14-902-0 PPSIV HVT Procedure

The Hazard Analysis was performed by analyzing the validation tools and methods for potential hazard identifications. The evaluation criterion is to verify that the test instrumentation does not introduce new hazards in accordance with IEEE 1012-1998 guidance on Test V&V Hazard Analysis activity. The evaluation result is that no new hazard was identified in the Test Phase.

7.3.2 List of Hazards

Each hazard is uniquely identified by an ID, namely H-<number>(alphabetic character). The Hazard ID is tied to a specific requirement number in the SRS, namely R-<number>.

The hazard ID will be used by the Hazard Tracking mechanism to track each hazard status and its mitigation in each phase of the Protection Sets software development.

P

P

P

P

P

P

8.0 Risk Analysis

8.1 Purpose

The Risk Analysis is intended to review and evaluate the frequency of occurrence and the severity of the consequence(s) associated with a hazard. The analysis also provides recommendations to eliminate or mitigate the risks.

Input documents to the Risk Analysis are:

1) PG&E PPS IRS
2) PG&E PPS FRS
3) Invensys SRS
4) The Hazard Lists, Section 7.0 and Section 5.0

The Risk Analysis is prepared based on the guidance of IEEE Std 1012-1998 and CEI/IEC 300-3-9-1995 [Reference 2.3.1].

8.2 Scope

The scope of the Risk Analysis is limited to evaluating the risks related to the Tricon Protection Set software hazards.

The ALS-related risks are not evaluated in this analysis.

The MWS-related risks in normal operation are not evaluated in this analysis.

8.3 Output

Outputs of the Risk Analysis are an IV&V Task Report and a list of risk assessments. The Task Report is documented in this section.

8.3.1 Risk Analysis Task Report

Requirement Phase – PG&E Design Inputs Rev 9, SET I, II, III, IV

The Risk Analysis task conducted in the Requirement Phase Revisited was based on the following input documents:

1) 993754-11-809 SRS revision 4
2) PG&E FRS revision 9
3) PG&E IRS revision 9

The Risk Analysis was performed in the Requirements Phase Revisited by reviewing and evaluating the new Rev 9-based hazard found in the Hazard Analysis.

The evaluation criteria are to review the potential hazards for consequence severity and occurrence frequency. The evaluation result is that a mitigation plan is recommended for one new hazard.

Design Phase – PG&E Design Inputs Rev 9, SET I

The Risk Analysis task conducted in the Design Phase Revisited was based on the following input documents:

1) 993754-11-810 SDD revision 2
2) PG&E IRS revision 9
3) PG&E IRS revision 9
4) CD-ER 993754-27, CD-ER 993754-28 and CD-ER 993754-29

The Risk Analysis was performed in the Requirements Phase Revisited by reviewing and evaluating the new Rev 9-based hazard found in the Hazard Analysis.

The evaluation criteria are to review the Design Phase hazards for consequence severity and occurrence frequency in accordance with IEEE 1012-1998 guidance on Design V&V Risk Analysis activity. The evaluation result is that no mitigation plan is recommended because all hazards identified in the previous phase are closed.

Implementation Phase – PG&E Design Inputs Rev 9, SET I

The Risk Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-11-810 PPSI SDD revision 3
2) 993754-11-700 PGE DCPP PPS rev 1

The Risk Analysis was performed by reviewing and evaluating the new Rev 9-based hazard if any found in the Hazard Analysis. The evaluation criteria are to review the Implementation Phase hazards for consequence severity and occurrence frequency in accordance with IEEE 1012-1998 guidance on Implementation V&V Risk

Analysisactivity. The evaluation result is that no mitigation plan is recommended because no new hazard is identified in the Implementation Phase.

Test Phase – PG&E Design Inputs Rev 9, SET I

The Risk Analysis task conducted in the Test Phase was based on the following input documents:

1) 993754-11-700 PGE DCPP PPS rev 3
2) 993754-11-902-1 PPSI FAT Procedure
3) 993754-11-902-0 PPSI HVT Procedure

The Risk Analysis was performed by reviewing and evaluating the new hazard if any found in the Hazard Analysis. The evaluation criteria are to review the Test Phase hazards for consequence severity and occurrence frequency in accordance with IEEE 1012-1998 guidance on Test V&V Risk Analysis activity. The evaluation result is that no mitigation plan is recommended because no new hazard was identified in the Test Phase.

Design Phase – PG&E Design Inputs Rev 9, SET II, III, IV

The Risk Analysis task conducted in the PPSII – IV Design Phase was based on the following input documents:

1) 993754-12-810 SDD revision 0
2) PG&E FRS revision 9
3) PG&E IRS revision 9

The Risk Analysis was performed by reviewing and evaluating the new hazard found in the Hazard Analysis.

The evaluation criteria are to review the PPSII – IV Design Phase hazards for consequence severity and occurrence frequency in accordance with IEEE 1012-1998 guidance on Design V&V Risk Analysis activity. The evaluation result is that no mitigation plan is recommended because no new hazard is identified.

Implementation Phase – PG&E Design Inputs Rev 9, SET II, III, and IV

The Risk Analysis task conducted in the Implementation Phase was based on the following input documents:

1) 993754-12-810 SDD PPSII-IV revision 1
2) 993754-12-700 PGE DCPP PPS (TSAP)
3) 993754-13-700 PGE DCPP PPS (TSAP)
4) 993754-14-700 PGE DCPP PPS (TSAP)
5) 993754-12-SWR-45 Software Walkthrough Report
6) 993754-13-SWR-46 Software Walkthrough Report
7) 993754-14-SWR-47 Software Walkthrough Report

The Risk Analysis was performed by reviewing and evaluating the new Rev 9-based hazard if any found in the Hazard Analysis. The evaluation criteria are to review the Implementation Phase hazards for consequence severity and occurrence frequency in accordance with IEEE 1012-1998 guidance on Implementation V&V Risk Analysis activity. The evaluation result is that no mitigation plan is recommended because no new hazard is identified in the Implementation Phase.

Test Phase – PG&E Design Inputs Rev 9, SET II, III, and IV

The Risk Analysis task conducted in the Test Phase was based on the following input documents:

1) 993754-12-700 PGE DCPP PPS
2) 993754-13-700 PGE DCPP PPS
3) 993754-14-700 PGE DCPP PPS
4) 993754-12-902-1 PPSII FAT Procedure
5) 993754-13-902-1 PPSIII FAT Procedure
6) 993754-14-902-1 PPSIV FAT Procedure
7) 993754-12-902-0 PPSII HVT Procedure
8) 993754-13-902-0 PPSIII HVT Procedure
9) 993754-14-902-0 PPSIV HVT Procedure

The Risk Analysis was performed by reviewing and evaluating the new hazard if any found in the Hazard Analysis. The evaluation criteria are to review the Test Phase hazards for consequence severity and occurrence frequency in accordance with IEEE 1012-1998 guidance on Test V&V Risk Analysis activity. The evaluation result is that no mitigation plan is recommended because no new hazard was identified in the Test Phase.

8.3.2 List of Risk Assessments

The below list is the result of the quantitative risk analysis, including estimates of the frequency of the hazard and the associated severity.

P

P

P

P

9.0 Conclusions

Requirement Phase – PG&E Design Inputs Rev 9, SET I, II, III, IV

It is recommended that hazard H-6 be mitigated in the Design Phase Revisited.

Design Phase – PG&E Design Inputs Rev 9, SET I

There is no further recommendation because there is no outstanding hazard.

Implementation Phase – PG&E Design Inputs Rev 9, SET I

Although mitigations are provided for the potential hazards discussed in Section 7.1.3.1 (Code Logic Analysis), there are two recommendations strictly from a good programming practice:

1) Checking for a non-zero denominator should be performed before the division operation.
2) Checking for a non negative number should be performed before the square root function invocation.

Test Phase – PG&E Design Inputs Rev 9, Set I

There is no further recommendation because there is no outstanding hazard.

Design Phase – PG&E Design Inputs Rev 9, SET II – IV

There is no recommendation because there is no outstanding hazard.

Implementation Phase – PG&E Design Inputs Rev 9, SET II – IV

There is no recommendation because there is no outstanding hazard.

Test Phase – PG&E Design Inputs Rev 9, Set II – IV

There is no further recommendation because there is no outstanding hazard.

10.0 Attachments

The Hazard Tracking List is attached below.

DCPP Hazard Tracking List.xls

DCPP PPS Hazard Tracking List

Document DCPP Hazard Tracking List is the attachment to the Safety Analysis,
Note 993754-1-915.
Revision # 9
Author Hoan Nguyen
Date 9-Dec-14

P

P

P

P