Pacific Gas and
Electric Company®

Barry S. Allen
Site Vice President

Diablo Canyon Power Plant
Mail Code 104/6
P. O. Box 56
Avila Beach, CA 93424

805.545.4888
Internal: 691.4888
Fax: 805.545.6445

April 30, 2013

PG&E Letter DCL-13-043

10 CFR 50.90

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, D.C. 20555-0001

Diablo Canyon Units 1 and 2
Docket No. 50-275, OL-DPR-80
Docket No. 50-323, OL-DPR-82
<u>Supplement to License Amendment Request 11-07, "Process Protection System Replacement"</u>

References:
1. PG&E Letter DCL-11-104, "License Amendment Request 11-07, Process Protection System Replacement," dated October 26, 2011 (ADAMS Accession No. ML11307A331)
2. Digital Instrumentation and Controls Digital I&C-ISG-06, "Task Working Group #6: Licensing Process, Interim Staff Guidance," Revision 1, January 19, 2011 (ADAMS Accession No. ML110140103)
3. PG&E Letter DCL-12-083, "Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement," dated September 11, 2012 (ADAMS Accession No. ML12256A308)
4. NRC Letter from S. Bahadur (NRC) to Clayton Scott (Invensys Operations Management), dated June 12, 2012 (ADAMS Accession No. ML12158A403)
5. NRC Letter from J. E. Dyer (NRC) to James R. Becker (PG&E), dated October 14, 2009

Dear Commissioners and Staff:

In Reference 1, Pacific Gas and Electric Company (PG&E) submitted a license amendment request 11-07 (LAR 11-07) that proposes to permanently replace the DCPP Eagle 21 digital process protection system (PPS) with a new digital PPS that is based on the Invensys Operations Management Tricon Programmable Logic Controller (PLC), Version 10, and the CS Innovations, LLC (a Westinghouse Electric Company), Advanced Logic System (ALS). The Reference 1 LAR is the pilot application for NRC Interim Staff Guidance (ISG) in digital instrumentation and control (I&C) Digital I&C-ISG-06 (Reference 2) that describes the licensing process that may be used in the review of LARs associated with digital I&C system modifications.

In Reference 3, PG&E informed the staff that a design change to the PPS replacement design to use separate maintenance workstations for the ALS and the Tricon subsystems would be made and included in a supplement to LAR 11-07. This letter provides the supplemental information on the design change to the PPS replacement design. In addition, other information provided in Reference 3 and a change to the Technical Specification 1.1 definition for channel operability test is incorporated into LAR 11-07.

Reference 1, was a DI&C-ISG-06 Tier 2 application for use of the Invensys Operations Management Tricon PLC, Version 10, that included deviations from the previously approved topical report for the Tricon PLC, Version 9. In Reference 4, the NRC found it acceptable to reference the Invensys Operations Management Topical Report 7286-545-1-A, Revision 4, "Triconex Approved Topical Report," describing the Version 10.5.1 Tricon PLC. Accordingly, PG&E is requesting a DI&C-ISG-06 Tier 1 application for use of the Invensys Operations Management Tricon PLC, Version 10.

The NRC previously granted a fee exemption for the Reference 1 LAR in accordance with 10 CFR 170.11(b) in Reference 5.

PG&E requests approval of the Reference 1 LAR no later than July 2014, to support preparations for the Unit 1 Refueling Outage Nineteen (1R19) which is currently scheduled to begin in September 2015. PG&E is currently planning to implement the PPS replacement for the first unit in the 1R19. Therefore, PG&E requests the license amendments for Reference 1 be made effective upon NRC issuance, to be implemented prior to entry into Mode 4 following completion of the 1R19 and the Unit 2 Refueling Outage Nineteen. These requested approval and implementation dates supersede those previously requested in Reference 1.

The enclosure to this letter contains the evaluation of the proposed change previously provided in the Enclosure of Reference 1, with supplemental information within the LAR text that is identified by revision bars to facilitate identification of the changes.

This information does not affect the results of the technical evaluation, or the no significant hazards consideration determination, previously submitted in Reference 1.

This communication contains new regulatory commitments (as defined by NEI 99-04) and revisions to previous commitments. The new commitments and revisions to previous commitments are contained in Attachment 1 of the Enclosure.

In accordance with site administrative procedures and the Quality Assurance Program, the proposed amendment has been reviewed by the Plant Staff Review Committee.

Pursuant to 10 CFR 50.91, PG&E is sending a copy of this proposed amendment to the California Department of Public Health.

If you have any questions or require additional information, please contact Tom Baldwin at 805-545-4720.

I state under penalty of perjury that the foregoing is true and correct.

Executed on April 30, 2013.

Sincerely,

Barry S. Allen

Barry S. Allen
Site Vice President

kjse/4328 50271918
Enclosure
cc: Diablo Distribution
cc/enc: Thomas R. Hipschman, NRC Senior Resident Inspector
Arthur T. Howell, III, NRC Region IV
Gonzalo L. Perez, Branch Chief, California Department of Public Health
James T. Polickoski, NRR Project Manager

Evaluation of the Proposed Change

Supplement to License Amendment Request 11-07 Process Protection System Replacement

Figures

Tables

ATTACHMENTS

1. List of Regulatory Commitments
2. Proposed Technical Specification Changes
3. Revised Technical Specification Pages
4. Technical Specification Bases Changes
5. Final Safety Analysis Report Changes

EVALUATION

1. SUMMARY DESCRIPTION

This license amendment request (LAR) requests Nuclear Regulatory Commission (NRC) staff approval for Pacific Gas & Electric Company (PG&E) to permanently replace the Diablo Canyon Power Plant (DCPP) Eagle 21 digital process protection system (PPS) with a new digital PPS that is based on the Invensys Operations Management (IOM) Tricon Programmable Logic Controller (PLC), Version 10, and the CS Innovations, LLC (a Westinghouse Electric Company), (CSI) Advanced Logic System (ALS).

The current Eagle 21 PPS is a digital microprocessor-based system which provides process protection functions for the reactor protection system (RPS) that is comprised of the reactor trip (RT) system (RTS) and engineered safety features actuation system (ESFAS). The proposed PPS replacement consists of a microprocessor-based Tricon PLC and the field programmable gate array (FPGA) based ALS that will improve the reliability and diversity of the PPS.

The NRC has issued Interim Staff Guidance (ISG) in digital instrumentation and control (I&C) DI&C-ISG-06 [1] that describes the licensing process that may be used in the review of LARs associated with digital I&C system modifications. DI&C-ISG-06 [1] includes a description of the applicable regulatory requirements and criteria for digital I&C system modifications. This LAR is the pilot application for use of DI&C-ISG-06 [1] and the LAR format and contents are consistent with the guidance provided in Enclosure E and Section C.3, respectively, of DI&C-ISG-06 [1]. Prior to the submittal of this LAR, PG&E held four pre-application (DI&C-ISG-06 Phase 0) meetings with the staff on August 27, 2009, March 18, 2010, February 3, 2011, and June 7, 2011.

DI&C-ISG-06 [1] describes three different tiers of applications for approval of I&C system modifications. Tier 1 is applicable to LARs proposing to reference a previously approved topical report regarding a digital I&C platform or component(s). Tier 2 is applicable to LARs proposing to reference a previously approved topical report with deviations to suit the plant-specific application. Tier 3 is applicable to license amendments proposing to use a new digital I&C platform or component(s) with no generic approval. This application is a Tier 1 application for use of the Tricon PLC, Version 10, described in Reference 13 and a Tier 3 application for use of the CSI ALS described in Reference 15. In Reference 155, the NRC found it acceptable to reference the Invensys Operations Management Topical Report 7286-545-1-A, Revision 4, “Triconex Approved Topical Report,” describing the Version 10.5.1 Tricon PLC submitted in Reference 13. Accordingly, PG&E is requesting a DI&C-ISG-06 Tier 1 application for use of the Invensys Operations Management Tricon PLC, Version 10.

DI&C-ISG-06 [1], Enclosure B, lists documents that are typically submitted by the licensee in support of a typical Tier 1 and Tier 3 submittal during Phases 1 and 2 of review. The Phase 1 documents that are associated with this application were summarized in Attachment 2 to the Enclosure of PG&E Letter DCL-11-104, dated October 26, 2011 [156]. Submittal of Phase 2 documents that have not been previously submitted to the staff and that are required for the review is being coordinated with the staff as part of the monthly teleconference meetings. Final Safety Analysis Report (FSAR) [26] changes and Technical Specification (TS) Bases [43] changes were submitted for information only in Attachments 2 and 3 of the Enclosure to PG&E Letter DCL-12-050 [157]. Revised Technical Specification (TS) Bases [43] changes and Final Safety Analysis Report (FSAR) [26] changes are provided in Attachments 4 and 5 of the Enclosure of this letter that supersede those previously submitted in PG&E Letter DCL-12-050 [157]. A change to TS 1.1 is contained in Attachments 2 and 3 of the Enclosure of this letter. No other TS changes are requested since the DCPP TS already contain the required definitions and requirements for a digital PPS.

The current Eagle 21 PPS is being replaced to address obsolescence, diagnostic, maintenance, and reliability issues. The Eagle 21 PPS has become obsolete due to multiple parts, such as computer chip sets, no longer being manufactured. Certain failures that can occur within the Eagle 21 PPS are difficult to diagnose due to a lack of comprehensive built-in diagnostic features. The Eagle 21 PPS requires a relatively high level of maintenance to support reliable operation, compared to current PPS designs that are available, which increases personnel occupational radiation exposure and ongoing cost to maintain the existing PPS. In addition, PG&E utilizes guidance provided in Institute of Nuclear Power Operations (INPO) AP 913, "Equipment Reliability Process Description," [96] that specifies zero tolerance for critical component failures. The replacement of the Eagle 21 PPS with a currently available PPS that is significantly more fault tolerant is consistent with nuclear industry guidance provided in INPO AP 913.

2. SIGNIFICANT HAZARDS CONSIDERATION AND ENVIRONMENTAL CONSIDERATION

2.1 Significant Hazards Consideration

PG&E has evaluated whether or not a significant hazards consideration is involved with the proposed amendment by focusing on the three standards set forth in 10 CFR 50.92, "Issuance of Amendment," as discussed below:

1. Does the proposed change involve a significant increase in the probability or consequences of an accident previously evaluated?

   Response: No.

   The proposed change would allow Pacific Gas and Electric Company to permanently replace the Diablo Canyon Power Plant Eagle 21 digital process protection system with a new digital process protection system that is based on the Invensys Operations Management Tricon Programmable Logic Controller, Version 10, and the CS Innovations Advanced Logic System. The process protection system replacement is designed to applicable codes and standards for safety-grade protection systems for nuclear power plants and incorporates additional redundancy and diversity features and therefore, does not result in an increase in the probability of inadvertent actuation or probability of failure to initiate a protective function. The process protection system replacement does not introduce any new credible failure mechanisms or malfunctions that cause an accident. The process protection system replacement design will continue to perform the reactor trip system and engineered safety features actuation system functions assumed in the Final Safety Analysis Report within the response time assumed in the Final Safety Analysis Report Chapter 6 and 15 accident analyses.

Therefore, the proposed change does not involve a significant increase in the probability or consequences of an accident previously evaluated.

2. Does the proposed change create the possibility of a new or different accident from any accident previously evaluated?

Response: No.

The proposed change is to permanently replace the current Diablo Canyon Power Plant Eagle 21 digital process protection system with a new digital process protection system. The process protection system performs the process protection functions for the reactor protection system that monitors selected plant parameters and initiates protective action as required. Accidents that may occur due to inadvertent actuation of the process protection system, such as an inadvertent safety injection actuation, are considered in the Final Safety Analysis Report accident analyses.

The protection system is designed with redundancy such that a single failure to generate an initiation signal in the process protection system will not cause failure to trip the reactor nor failure to actuate the engineered safeguard features when required. Neither will such a single failure cause spurious or inadvertent reactor trips or engineered safeguard features actuations because coincidence of two or more initiation signals is required for the solid state protection system to generate a trip or actuation command. If an inadvertent actuation occurs for any reason, existing control room alarms and indications will notify the operator to take corrective action.

The process protection system replacement design includes enhanced diversity features compared to the current process protection system to provide additional assurance that the protection system actions credited with automatic operation in the Final Safety Analysis Report accident analyses will be performed automatically when required should a common cause failure occur concurrently with a design basis event.

The process protection system replacement does not result in any new credible failure mechanisms or malfunctions. The current Eagle 21 process protection system utilizes digital technology and therefore the use of digital technology in the process protection system replacement does not introduce a new type of failure mechanism. Although extremely unlikely, the current Eagle 21 process protection system is susceptible to a credible common-cause software failure that could adversely affect automatic performance of the protection function. The process protection system replacement contains new, additional diversity features that prevent a common-cause software failure from completely disabling the process protection system.

Therefore, the proposed change does not create the possibility of a new or different accident from any accident previously evaluated.

3. Does the proposed change involve a significant reduction in a margin of safety?

Response: No.

The reactor protection system is fundamental to plant safety and performs reactor trip system and engineered safety features actuation system functions to limit the consequences of Condition II (faults of moderate frequency), Condition III (infrequent faults), and Condition IV (limiting faults) events. This is accomplished by sensing selected plant parameters and determining whether predetermined instrument settings are being exceeded. If predetermined instrument settings are exceeded, the reactor protection system sends actuation signals to trip the reactor and actuate those components that mitigate the severity of the accident.

The process protection system replacement design will continue to perform the reactor trip system and engineered safety features actuation functions assumed in the Final Safety Analysis Report within the response time assumed Final Safety Analysis Report Chapter 6 and 15 accident analyses. The use of the process protection system replacement does not result in a design basis or safety limit being exceeded or changed. The change to the process protection system has no impact on the reactor fuel, reactor vessel, or containment fission product barriers. The reliability and availability of the reactor protection system is improved with the process protection system replacement, and the reactor protection system will continue to effectively perform its function of sensing plant parameters to initiate protective actions to limit or mitigate events.

Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Based on the above evaluation, PG&E concludes that the proposed change does not involve a significant hazards consideration under the standards set forth in

10 CFR 50.92(c), and accordingly, a finding of "no significant hazards consideration" is justified.

2.2 Environmental Consideration

PG&E has evaluated the proposed amendment and has determined that the proposed amendment does not involve (i) a significant hazards consideration, (ii) a significant change in the types or significant increase in the amounts of any effluents that may be released offsite, or (iii) a significant increase in individual or cumulative occupational radiation exposure. Accordingly, the proposed amendment meets the eligibility criterion for categorical exclusion set forth in 10 CFR 51.22(c)(9). Therefore, pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the proposed amendment.

3. SAFETY ANALYSIS

3.1 Current Eagle 21 PPS

The existing PPS is part of the RPS process instrumentation. Process instrumentation is comprised of devices (and their associated interconnection into systems) which measure and process signals for temperature, pressure, fluid flow, and fluid levels, excluding nuclear and radiation measurements. Process instrumentation includes equipment that performs functions such as process measurement, signal conditioning, dynamic compensation, calculations, setpoint comparison, alarm actuation, indicating and recording, which are all necessary for operation of the Nuclear Steam Supply System as well as for monitoring the plant and providing initiation of protective functions whenever process parameters exceed the associated setpoint criteria. The PPS consists of the process instrumentation devices that monitor process parameters and initiate actuation of the RTS and ESFAS. The Eagle 21 PPS is described in FSAR [26] Sections 7.1, 7.2, and 7.3 and TS and TS Bases [43] sections 3.3.1 and 3.3.2.

Figure 3-1 contains an overview of the RTS and ESFAS including the Eagle 21 PPS. The Eagle 21 PPS contains four Protection Sets (Protection Set I, Protection Set II, Protection Set III, Protection Set IV) that receive input from sensors and provide output to two trains (Train A and Train B) of the solid state protection system (SSPS). Figure 3-1 also includes the nuclear instrumentation system (NIS) that provides diverse protection system input to the SSPS and the Anticipated Transient Without Scram Mitigation System Actuation Circuitry (AMSAC) that provides diverse commands to trip the main turbine and initiate auxiliary feedwater (AFW) flow. Steam generator blowdown and sample lines are isolated when the motor-driven AFW pumps start.

The current Eagle 21 PPS, which is located in instrument racks in the auxiliary building, contains analog input module(s), digital filter processor(s), a loop calculation processor, partial trip output module(s), and analog output module(s). The analog input module powers the field sensors and performs signal conditioning. The digital filter processor converts the analog input signals to digital signals, filters them and makes the data available to the loop calculation processor. The loop calculation processor is a centralized processor that provides summation, lead/lag, multiplication, comparator, averaging, and square root conversion, and computes the algorithms and comparisons for the protective functions. The partial trip output modules provide trip and actuation logic. The analog output modules provide isolated analog output information to the plant computer and control systems.

The protection channels which are processed with the Eagle 21 PPS are as follows:

- Reactor coolant average temperature and delta-temperature
- Pressurizer pressure
- Pressurizer water level
- Steam flow
- Feedwater flow
- Reactor coolant flow
- Turbine impulse chamber pressure
- Steam pressure
- Containment pressure
- Reactor coolant wide range temperature
- Reactor coolant wide range pressure
- Steam generator narrow range water level
- Pressurizer vapor temperature

The Eagle 21 protection functions assumed in the FSAR [26] accident analyses are as follows:

- Overtemperature delta-temperature RT
- Overpower delta-temperature RT
- Low and high pressurizer pressure RTs
- High pressurizer level RT
- High-high containment pressure steam line isolation (SLI)
- Low steam line pressure SLI and safety injection (SI)
- Low pressurizer pressure SI
- High containment pressure SI
- Low reactor coolant flow RT
- Steam generator water level low-low RT and AFW initiation
- Steam generator water level high-high turbine trip and feedwater isolation

PG&E requested NRC approval to install the Eagle 21 PPS, including associated TS changes, in PG&E Letter DCL-92-203, dated September 21, 1992 [97] and NRC approval was contained in License Amendments 84 and 83 to Licenses DPR-80 and DPR-82, respectively, dated October 7, 1993 [98].

The RTS and ESFAS, including the Eagle 21 PPS, meet the criteria of Institute of Electrical and Electronic Engineers (IEEE) Standard 279-1971, Criteria for Protection

Systems for Nuclear Power Generating Stations, dated 1971. The applicable standard for the Eagle 21 vendor validation and verification is the guidelines of Regulatory Guide (RG) 1.152, "Criteria for Programmable Digital Computer System Software in Safety-related Systems in Nuclear Plants," dated November 1985 [113], that endorses IEEE Standard 7-4.3.2, "Application Criteria for Programmable Digital Computer System in Safety Systems of Nuclear Power Generating Stations," dated 1982 [114]. The applicable standard for the safety system design is RG 1.153, "Criteria for Power, Instrumentation and Control Portions of Safety Systems," December 1985 [115] that endorses the guidance of IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," dated 1980 [116]. The vendor equipment qualification methodology conformed with IEEE Standard 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," dated 1974 [117]. The Eagle 21 equipment racks and components were subject to multi-axis, multi-frequency seismic inputs in accordance with RG 1.100 "Seismic Qualification of Electrical Equipment for Nuclear Power Plants," dated March 1996 [118], that endorsed IEEE Standard 344, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations" dated 1975 [119].

The Eagle 21 PPS is configured to perform automatic surveillance testing via a centralized test sequence processor. To support installation of Eagle 21, the TS definitions were revised to allow a channel operational test for a digital channel, and to allow a channel functional test for a digital channel that includes the injection of a simulated signal into the channel as close to the sensor input to the process racks as practical to verify operability of all devices in the channel required for channel operability.

The Eagle 21 PPS allows bypassing of an inoperable channel when performing surveillance tests on an operable channel. Placing the inoperable channel in bypass results in an indication to the operator and allows placing an operable channel in the "Test" mode which results in it being placed in trip. The current TS reflect the capability for the inoperable channel to be placed in bypass.

To support the installation of Eagle 21, the setpoint analyses for the protection system functions processed through Eagle 21 were revised to reflect revised setpoint input values for rack calibration accuracy, rack drift, and measurement and test equipment accuracies temperature effect as discussed in Section D of PG&E Letter DCL-92-203. The RTS and ESFAS TS [42] allowable values were revised to incorporate the results of the revised setpoint analysis.

A detailed description of the existing Eagle 21 PPS is contained in Section 4.1.

3.2 PPS Replacement

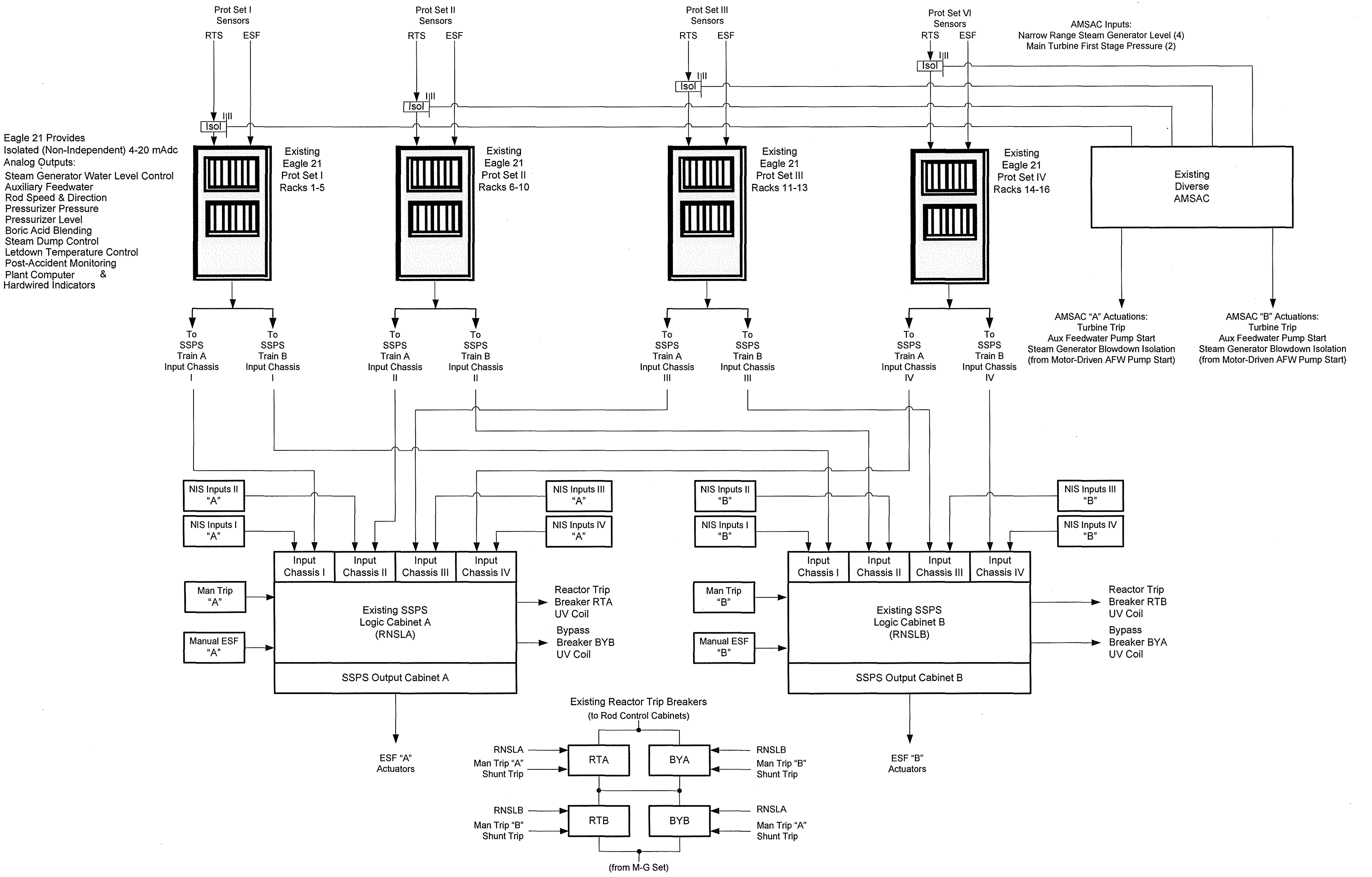
3.2.1 Proposed Architecture

The PPS replacement is based on the Tricon PLC, Version 10, described in Tricon V10 Topical Report Submittal [13] and the CSI ALS described in [15].

The system functional requirements for a digital safety-related system have a significant impact on the quality and safety of the installed software product. PG&E personnel were highly involved in the development of the PPS replacement technology, including performing a review of industry operating experience for the technology, performing a review and inspection of installed applications of the technology, writing the specification requirements, and developing the enhanced diversity aspects of the PPS replacement. Several personnel that were originally involved in the development of the current Eagle 21 PPS were involved in the development of the PPS replacement.

The PPS replacement incorporates reliability and diversity improvements to the current PPS while maintaining simplicity in the architectural design. The microprocessor-based Tricon PLC portion of the platform utilizes a triple modular redundant (TMR) technology that allows continued operation in the presence of multiple faults within the system and allows detection and correction of faults on-line without interruption of the protection capabilities. The ALS portion of the platform is logic-based and does not utilize a microprocessor.

Figure 3-1 Eagle 21 PPS


Prot Set I Sensors
RTS ESF
Prot Set II Sensors
RTS ESF
Prot Set III Sensors
RTS ESF
Prot Set VI Sensors
RTS ESF
AMSAC Inputs:
Narrow Range Steam Generator Level (4)
Main Turbine First Stage Pressure (2)
Isol
I|II
Eagle 21 Provides
Isolated (Non-Independent) 4-20 mAdc
Analog Outputs:
Steam Generator Water Level Control
Auxiliary Feedwater
Rod Speed & Direction
Pressurizer Pressure
Pressurizer Level
Boric Acid Blending
Steam Dump Control
Letdown Temperature Control
Post-Accident Monitoring
Plant Computer &
Hardwired Indicators
Existing Eagle 21 Prot Set I Racks 1-5
Existing Eagle 21 Prot Set II Racks 6-10
Existing Eagle 21 Prot Set III Racks 11-13
Existing Eagle 21 Prot Set IV Racks 14-16
Existing Diverse AMSAC
To SSPS Train A Input Chassis I
To SSPS Train B Input Chassis I
To SSPS Train A Input Chassis II
To SSPS Train B Input Chassis II
To SSPS Train A Input Chassis III
To SSPS Train B Input Chassis III
To SSPS Train A Input Chassis IV
To SSPS Train B Input Chassis IV
AMSAC "A" Actuations:
Turbine Trip
Aux Feedwater Pump Start
Steam Generator Blowdown Isolation
(from Motor-Driven AFW Pump Start)
AMSAC "B" Actuations:
Turbine Trip
Aux Feedwater Pump Start
Steam Generator Blowdown Isolation
(from Motor-Driven AFW Pump Start)
NIS Inputs II "A"
NIS Inputs I "A"
NIS Inputs III "A"
NIS Inputs IV "A"
NIS Inputs II "B"
NIS Inputs I "B"
NIS Inputs III "B"
NIS Inputs IV "B"
Input Chassis I
Input Chassis II
Input Chassis III
Input Chassis IV
Man Trip "A"
Manual ESF "A"
Existing SSPS Logic Cabinet A (RNSLA)
SSPS Output Cabinet A
Reactor Trip Breaker RTA UV Coil
Bypass Breaker BYB UV Coil
Man Trip "B"
Manual ESF "B"
Existing SSPS Logic Cabinet B (RNSLB)
SSPS Output Cabinet B
Reactor Trip Breaker RTB UV Coil
Bypass Breaker BYA UV Coil
ESF "A" Actuators
ESF "B" Actuators
Existing Reactor Trip Breakers
(to Rod Control Cabinets)
RNSLA
Man Trip "A" Shunt Trip
RTA
BYA
RNSLB
Man Trip "B" Shunt Trip
RNSLB
Man Trip "B" Shunt Trip
RTB
BYB
RNSLA
Man Trip "A" Shunt Trip
(from M-G Set)

Although extremely unlikely, the current Eagle 21 PPS is susceptible to a credible common cause software failure (CCSF) that could adversely affect automatic performance of the protection function and require manual operator action to be taken. The use of built-in diversity in the design of the PPS replacement eliminates the need for manual operator actions to address CCSF and precludes the need for an external diverse actuation system and enhances the simplicity of the PPS replacement.

In accordance with the guidance in NUREG-0800, Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth (D3) in Digital Computer Based Instrumentation and Control Systems," Revision 5, March 2007 [4] PG&E completed and submitted the D3 topical report for the PPS Replacement to the NRC for approval in [6]. The NRC staff issued a Safety Evaluation Report (SER) for the D3 topical report in [7].

The PPS replacement has been designed to meet the following updated standards and new guidance:

- IEEE Standard 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations [21]
- IEEE Standard 308-1980 [30],
- IEEE Standard 7-4.3.2-2003, [80]
- IEEE Standard 384-1981 [89]
- EPRI TR-107330 [81]
- RG 1.152, Revision 3 “Criteria For Use Of Computers In Safety Systems Of Nuclear Power Plants.” [45]
- RG 5.71, Revision 0, “Cyber Security Programs for Nuclear Facilities,” January 2010 [46]

The PPS replacement has been designed to meet ISG-04 [2], except for Section 1, “Interdivisional Communications,” Staff Position 10. The PPS replacement has been designed to an alternative justification for this position based on the combination of redundancy within the Tricon subsystem and both redundancy and diversity in the ALS subsystem, along with administrative controls.

The above standards and guidance apply only to the PPS portion of the protection system.

The proposed project replaces in its entirety the current Westinghouse Eagle 21 PPS with a new PPS that has improved reliability, diversity, diagnostic, and testing capabilities. Figure 3-2 contains an overview of the RTS and ESFAS including a simplified representation of the PPS replacement. The scope of the PPS replacement is illustrated in the shaded portion of Figure 3-2. Equipment in the unshaded portion of Figure 3-2 is not being replaced or modified as part of the PPS Replacement Project. The existing Eagle 21 PPS four redundant Protection Sets, as shown in Figure 3-1, will be replaced with four redundant and independent Protection Sets (Protections Set I, Protection Set II, Protection Set III, Protection Set IV) that receive input from sensors and provide output to two trains (Train A and Train B) of the SSPS. Each Protection Set in the PPS replacement contains a software-based Triconex Tricon V10 processor subsystem described in Reference 13 and a diverse safety-related CSI ALS subsystem described in Reference 15.

The built-in diversity provided by the logic-based ALS ensures that all accidents and events credited with automatic PPS mitigation in DCPP FSAR [26] Chapter 15 analyses continue to be mitigated automatically with concurrent software CCF. The PPS replacement automatically mitigates events that currently require manual protective action should a CCF disable the primary and backup protection functions. A detailed description of the allocation of automatic protection functions between the Tricon subsystem and the ALS subsystem is presented in section 4.2.

Each Protection Set is independent of the other Protection Sets and is protected from adverse influence from the other Protection Sets. The PPS replacement does not utilize or implement inter-divisional safety-to-safety communications. Within a protection set, the PPS replacement incorporates safety-to-non safety communications. The PPS replacement architecture is designed to ensure that communications between safety and non-safety equipment that resides within the Protection Set adhere to the guidance described in the ISG 4 Staff Positions.

Each of the four Protection Sets contains a separate non-safety related maintenance workstation (MWS) for the Tricon subsystem and the ALS subsystem (a total of eight MWSs for the PPS). A detailed description of the PPS replacement is contained in Section 4.2.

3.2.2 Communications

Figure 3-3 provides a simplified representation of the communications architecture for a single Protection Set. The Tricon, ALS, Tricon subsystem MWS, and ALS subsystem MWS communications are summarized below.

3.2.2.1 The Plant Data Network (PDN) Gateway Switch in Figure 3-3 is current plant equipment that connects to a PDN Gateway Computer. The PDN Gateway Computer is currently a Dell server that collects data from the Process Control System and sends this data through the PDN to the Plant Process Computer (PPC) using InStep eDNA communication software.

3.2.2.1 Tricon Communications

There are no communications paths between redundant Protection Sets in the Tricon portion of the PPS replacement. The non-safety-related Tricon MWSs, discussed in detail in Section 4.2.13.3, within a redundant Protection Set communicate only with the safety-related controllers within that Protection Set. The Tricon Communications

Module (TCM) output media from the Tricon is fiber optic to provide electrical isolation. A media converter converts the fiber optic media to 100baseT Ethernet.

A NetOptics Model PA-CU port aggregator tap device is utilized to ensure that only one-way communication takes place between the Tricon processors and the PDN Gateway Switch connected to the PDN Gateway Computer. The NetOptics device permits two-way communications between the Tricon TCM and the MWS, while permitting the PDN Gateway Switch read-only access to the Tricon TCM and the MWS. The non-safety PDN Gateway Switch connects to the PDN Gateway Computer that provides data through the PDN to the PPC.

3.2.2.2 ALS Communications

There are no communication paths between redundant safety divisions in the ALS portion of the PPS replacement as shown in Figure 3-3. The two Electronic Industries Alliance EIA-422 standard ALS communication channels (TxB1 and TxB2) from the ALS-102 in each ALS chassis to the PDN Gateway Switch and the ALS MWS, respectively, are isolated, serial, and one-way. The communications channels do not receive any data, handshaking, or instructions from the PDN Gateway Computer connected to the PDN Gateway Switch. Handshaking is an automated process of negotiation that dynamically sets parameters of a communications channel established between two entities before normal communication over the channel begins. The ALS processes reactor coolant system (RCS) temperature signals and transmits the conditioned and scaled data to the Tricon via analog 4-20 milliampere (mA) signals.

The Test ALS Bus (TAB) communication channel provides communications between ALS Service Unit (ASU) maintenance software in the ALS MWS and the ALS chassis. This Electronic Industries Alliance EIA-485 standard communication path is normally physically disconnected, with two-way communication permitted only when the communication link is physically connected (enabled) between the TAB and the ALS MWS. No communication is possible on the TAB when the communication link is physically disconnected. The Protection Set containing the ALS chassis remains functional with TAB communications enabled. The information is collected in a non-obtrusive manner and does not affect the on-going operation of the system.

Figure 3-2 PPS Replacement

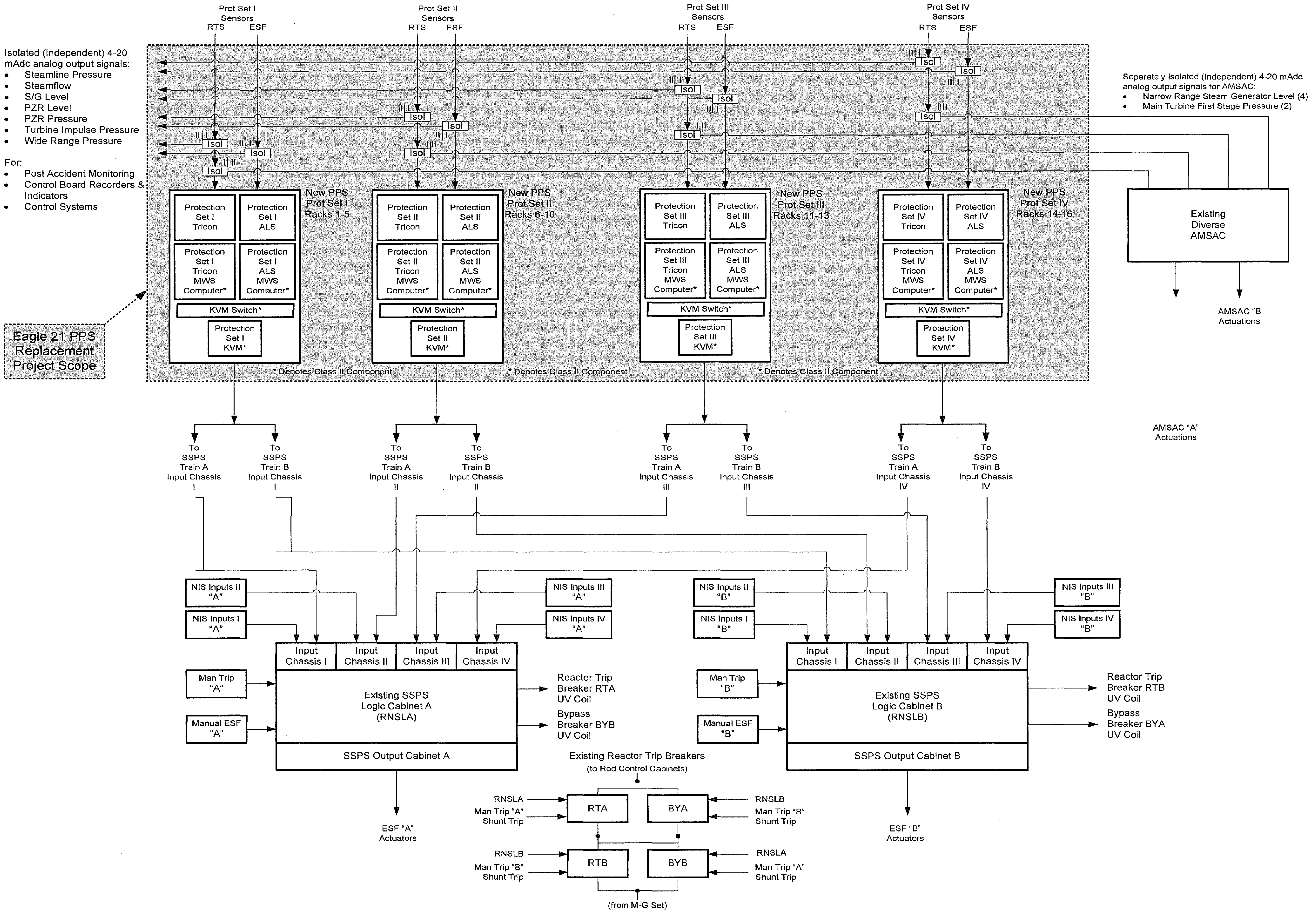
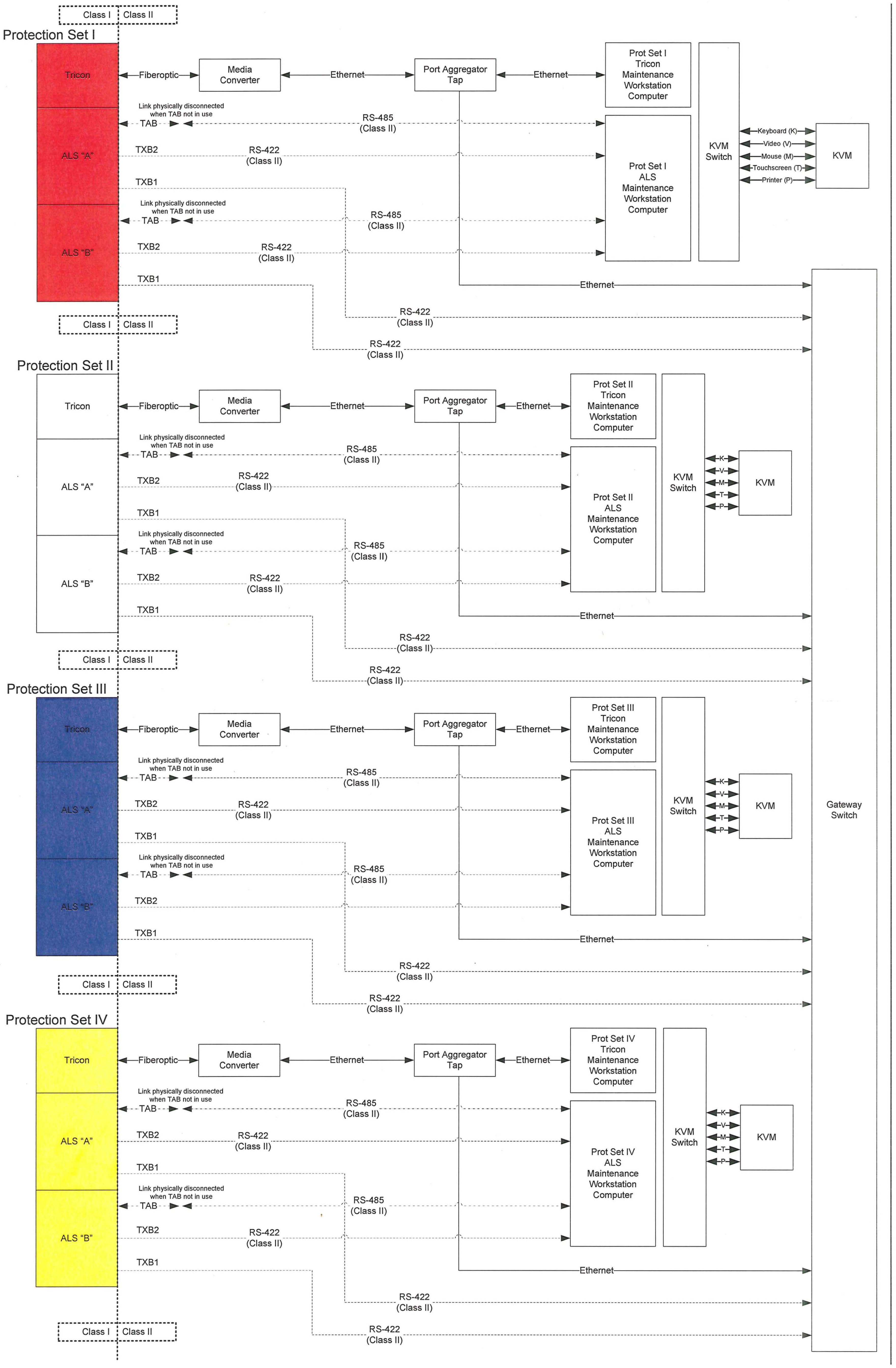

Prot Set I Sensors
RTS ESF
Prot Set II Sensors
RTS ESF
Prot Set III Sensors
RTS ESF
Prot Set IV Sensors
RTS ESF
Isolated (Independent) 4-20 mAdc analog output signals:
• Steamline Pressure
• Steamflow
• S/G Level
• PZR Level
• PZR Pressure
• Turbine Impulse Pressure
• Wide Range Pressure
For:
• Post Accident Monitoring
• Control Board Recorders & Indicators
• Control Systems
Isol
Separately Isolated (Independent) 4-20 mAdc analog output signals for AMSAC:
• Narrow Range Steam Generator Level (4)
• Main Turbine First Stage Pressure (2)
New PPS Prot Set I Racks 1-5
New PPS Prot Set II Racks 6-10
New PPS Prot Set III Racks 11-13
New PPS Prot Set IV Racks 14-16
Protection Set I Tricon
Protection Set I ALS
Protection Set I Tricon MWS Computer*
Protection Set I ALS MWS Computer*
KVM Switch*
Protection Set I KVM*
Protection Set II Tricon
Protection Set II ALS
Protection Set II Tricon MWS Computer*
Protection Set II ALS MWS Computer*
KVM Switch*
Protection Set II KVM*
Protection Set III Tricon
Protection Set III ALS
Protection Set III Tricon MWS Computer*
Protection Set III ALS MWS Computer*
KVM Switch*
Protection Set III KVM*
Protection Set IV Tricon
Protection Set IV ALS
Protection Set IV Tricon MWS Computer*
Protection Set IV ALS MWS Computer*
KVM Switch*
Protection Set IV KVM*
Existing Diverse AMSAC
AMSAC "B Actuations
AMSAC "A" Actuations
Eagle 21 PPS Replacement Project Scope
* Denotes Class II Component
* Denotes Class II Component
* Denotes Class II Component
To SSPS Train A Input Chassis I
To SSPS Train B Input Chassis I
To SSPS Train A Input Chassis II
To SSPS Train B Input Chassis II
To SSPS Train A Input Chassis III
To SSPS Train B Input Chassis III
To SSPS Train A Input Chassis IV
To SSPS Train B Input Chassis IV
NIS Inputs II "A"
NIS Inputs I "A"
NIS Inputs III "A"
NIS Inputs IV "A"
NIS Inputs II "B"
NIS Inputs I "B"
NIS Inputs III "B"
NIS Inputs IV "B"
Input Chassis I
Input Chassis II
Input Chassis III
Input Chassis IV
Existing SSPS Logic Cabinet A (RNSLA)
SSPS Output Cabinet A
Man Trip "A"
Manual ESF "A"
Reactor Trip Breaker RTA UV Coil
Bypass Breaker BYB UV Coil
ESF "A" Actuators
Input Chassis I
Input Chassis II
Input Chassis III
Input Chassis IV
Existing SSPS Logic Cabinet B (RNSLB)
SSPS Output Cabinet B
Man Trip "B"
Manual ESF "B"
Reactor Trip Breaker RTB UV Coil
Bypass Breaker BYA UV Coil
ESF "B" Actuators
Existing Reactor Trip Breakers (to Rod Control Cabinets)
RNSLA
Man Trip "A" Shunt Trip
RTA
BYA
RNSLB
Man Trip "B" Shunt Trip
RNSLB
Man Trip "B" Shunt Trip
RTB
BYB
RNSLA
Man Trip "A" Shunt Trip
(from M-G Set)

Figure 3-3 PPS Replacement Communications



3.2.2.3 Non-Safety-Related MWS

Separate and independent non-safety-related MWSs shown in Figure 3-2 and Figure 3-3 are provided for the Tricon and ALS subsystems, respectively, for each Protection Set to allow PPS information processing and display, and to facilitate maintenance. The two MWSs in each Protection Set share common peripheral devices such as the keyboard, video display, mouse, touchscreen interface, and printer through a Keyboard-Video-Mouse (KVM) switch. The Tricon MWS is dedicated to the Tricon PPS subsystem in the respective set; the ALS MWS is dedicated to the ALS PPS subsystem in that set. The two MWSs cannot communicate with each other nor can they communicate with the MWSs in redundant protection sets.

The non-safety-related Tricon MWS is used to maintain and configure the Tricon and also to view data from Tricon. The non-safety ALS MWS likewise is used to maintain and configure the ALS. With the TAB communication link between the TAB and the ALS MWS physically disconnected, the ALS broadcasts data in a read-only manner for display on the ALS MWS. When the TAB has been placed in service by physically connecting the TAB communication link between the TAB and the ALS MWS, the MWS is used to perform the maintenance functions associated with the ASU.

A MWS may access data only within its own Protection Set. Communication of any MWS with any other Protection Sets is not possible. There are no means of connecting any Protection Set to another MWS without reconfiguring the Protection Set controllers and communications cabling.

3.2.2.4 Triconex Communications with Tricon MWS

Under operating plant conditions the MWS simply displays plant parameters and diagnostic information. The controls for access to functions beyond displaying data is security-related information per 10 CFR 2.390 and was submitted. to the NRC staff in PG&E Letter DCL-11-123, dated December 20, 2011 [164]. The MWS will be used for PPS information processing and display, and to facilitate maintenance such as modifying Tricon safety system parameters. Use of the MWS is in accordance with site-specific administrative (procedural) and physical-access controls.

Data isolation between the safety-related Tricon control processor and the non-safety MWS is performed by the safety-related TCM. Fiber optic cable electrically isolates the Tricon from external non-safety-related devices.

3.2.2.5 ALS Communication with ALS MWS

Communications from the ALS to the MWS are via the transmit-only (no handshake) ALS-102 communication channel TxB2. The TxB2 communications channel does not receive any data, handshaking, or instructions from the MWS.

Two-way TAB communications between ASU application software in the MWS and the ALS chassis are used to perform ALS maintenance and calibration functions. This

EIA-485 communication path is normally physically disconnected. Two-way communications are permitted only when the TAB communication link is physically connected between the TAB and the ALS MWS. An ALS trouble alarm is initiated on the Main Annunciator when the TAB is enabled. Communications on the TAB are not possible if the communication link is physically disconnected.

3.2.3 Development Process

The hardware and software development for the PPS replacement utilizes a development process that complies with IEEE Standard 603-1991 [21] Clause 5.3 "Quality," and IEEE Standard 7-4.3.2-2003 [80] Clause 5.3, "Quality," including the digital system development life cycle. IOM used a product development process for the Tricon platform including processes distinctively tailored to development of software used in designing and maintaining programmable logic devices (PLDs). CSI used a hardware development process for development of the ALS. The ALS is an FPGA-based system that does not execute software. However, the FPGA is configured by using software tools and therefore a quality control procedure was used in the development of the FPGA. Details on the development process used is contained in Sections 4.2.11, 4.3, 4.5, 4.10.2.3, and 4.11.1.1.

3.2.4 Validation and Verification (V&V)

The validation and verification (V&V) effort for the PPS replacement utilizes a process and activities that comply with IEEE Standard 7-4.3.2-2003 [80] Clause 5.3.3, "Validation and Verification". IOM has a Software V&V Plan that establishes the V&V process for Tricon platform hardware including how V&V activities will be performed. CSI has a V&V Plan that defines the techniques, procedures, and methodologies that will be used to provide V&V for the ALS platform design and test development and the test activities for the platform development and implementation. PG&E has a System Verification and Validation Plan for the PPS Replacement Project that defines the activities for V&V by PG&E, IOM, and CSI. Details on the software V&V process is contained in Section 4.5.6.

3.2.5 Software Configuration Management

Software configuration management complies with IEEE Standard 7-4.3.2-2003 [80] Clause 5.3.5, "Software Configuration Management". IOM has a PPS Replacement Configuration Management Plan (CMP) that defines how software configuration management is applied and establishes the content of the Software Configuration Management Plan (SCMP). CSI has an ALS CMP that describes the organization and practices used for the ALS. PG&E has a DCPP Software Configuration Management procedure for Software Configuration Management for Plant Operations and Operations Support to provide configuration management. Details on the software configuration management are contained in Section 4.5.7.

3.2.6 Safety Analysis Summary

The PPS replacement incorporates redundancy, independence, and diversity while providing simplicity in the architectural design. PG&E has completed and submitted the D3 topical report for the PPS Replacement to the NRC and the NRC staff has issued a SER for the D3 topical report. The hardware and software development for the PPS replacement utilizes a development process that complies with IEEE Standard 603-1991 [21] Clause 5.3 "Quality," and IEEE Standard 7-4.3.2-2003 [80] Clause 5.3, "Quality," including the digital system development life cycle, in order to provide a high quality and well defined development process that results in a quality PPS. The V&V effort for the PPS replacement utilizes a process and activities that comply with IEEE Standard 7-4.3.2-2003 [80] Clause 5.3.3, "Validation and Verification" to ensure the PPS replacement meets required specified functional requirements and criteria. Finally, the Software configuration management used for the PPS Replacement Project complies with IEEE Standard 7-4.3.2-2003 [80] Clause 5.3.5, "Software Configuration Management," control the system and programming throughout its development and use. Therefore, PG&E concludes the proposed PPS replacement complies with the 10 CFR 50 regulations and that the public health and safety will be protected with NRC staff approval to use the PPS replacement.

3.3 Effect on TS and Accident Analyses

The available diagnostic and self-test capabilities of the PPS replacement components eliminate the need to inject a signal into the channel in order to verify OPERABILITY during performance of the channel operability test (COT) surviellance. Therefore, the TS 1.1 COT definition is revised to provide separate and more appropriate definitions for the current analog, bistable, and current Eagle 21 PPS digital channels, and the Tricon/ALS PPS digital channels. The TS change is contained in Section 4.12.1.

The PPS replacement has been designed and specified such that it continues to meet the current TS [42] and FSAR [26] Chapter 6 and 15 accident analysis requirements. This has been accomplished by providing functional requirements in the PPS Replacement Functional Requirements Specification (FRS) [28] that are the same as or better than the current Eagle 21 PPS for instrument rack calibration accuracy, rack drift, temperature effect values, and response time. Therefore, no revised TS RTS and ESFAS setpoints are required for the PPS replacement. To support the implementation of the current Eagle 21 digital PPS, the TS were revised in License Amendments 84 and 83, dated October 7, 1993 [98] to allow a channel operational test for a digital channel, to allow a channel functional test for a digital channel that includes the injection of a simulated signal into the channel as close to the sensor input to the process racks as practical to verify operability, and to allow bypassing an inoperable channel when performing surveillance tests on an operable channel.

In addition, to support the implementation of the current Eagle 21 digital PPS, the setpoints analysis for the protection system functions processed through Eagle 21 were revised to reflect revised setpoint input values for rack calibration accuracy, rack drift, and temperature effect values as discussed in Section D of PG&E Letter DCL-92-203 [97] and the RTS and ESFAS TS [42] allowable values were revised to incorporate the results of the revised setpoint analysis.

The PPS replacement has been designed with sufficient diversity such that there is no credible single failure or CCSF that will prevent a required automatic protection function from being performed. Therefore, no revised FSAR [26] Chapter 6 or 15 accident analyses or revised accident analysis analytical methods are required for the PPS replacement.

3.4 Definitions

Definitions for terms used in this LAR are defined below.

Component: Items from which the system is assembled (such as resistors, capacitors, wires, connectors, transistors, tubes, switches, and springs).

Module: Any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit. A module can be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Channel: An arrangement of components, modules and software as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single action signals are combined.

Diversity and Defense-In-Depth (D3) Requirement imposed on the Protection System design to ensure that required protective actions will occur to protect against Anticipated Operational Occurrences and Design Basis Accidents (as described in the FSAR [26]) concurrent with a CCF (usually assumed to be software) that disables one or more echelons of defense.

Protection Set: A Protection Set is a physical grouping of process channels with the same Class-1E electrical channel designation (I, II, III, or IV). Each of the four redundant Protection Sets is provided with separate and independent power feeds and process instrumentation transmitters. Thus, each of the four redundant Protection Sets is physically and electrically independent of the other sets. A Protection Set may be referred to as a “rack set”.

Protective Function — A protective function is the sensing of one or more variables associated with a particular generating station condition, signal processing, and the initiation and completion of the protective action at values established in the design bases.

Single Failure — Any single event that results in a loss of function of a component or components of a system. Multiple failures resulting from a single event shall be treated as a single failure.

Train: — The SSPS portion of RTS/ESFAS. The RTS contains the logic circuitry necessary to automatically open the RT breakers that consists of two redundant logic trains that receive input from the protection channels. Each of the two trains, A and B, is capable of opening a separate and independent RT breaker (52/RTA and 52/RTB). The ESFAS contains a logic portion consisting of two redundant logic trains that receive inputs from the process protection channels and perform the needed logic to actuate the ESF.

4. SYSTEM DESCRIPTION (Section D.1 of DI&C-ISG-06 [1])

This section has been prepared using the guidance of DI&C-ISG-06 [1], Section D.1, System Description. Section 4.1 first describes the existing PPS functions and functions performed by other protective systems at DCPP. Section 4.2 then identifies the scope of the PPS replacement, the hardware being used for the DCPP PPS replacement, how the hardware items function, how the various hardware items are interconnected, and the software that is integrated with the hardware components. The PPS replacement performs all protection functions performed by the current PPS.

For the PPS replacement, there are no exceptions to the guidance and regulatory documents cited in Section 4.2 and following sections. Compliance is described generally in the referenced vendor topical reports; however, the topical reports are generic and by their nature cannot discuss all aspects of the platform as used in a specific application such as the PPS replacement. The PG&E project specification documents provide requirements for the specific DCPP PPS replacement application. Application-specific Phase 1 and Phase 2 vendor documentation describes how the project requirements are fulfilled. Such documentation includes:

1. DCPP Units 1 & 2 PPS Replacement FRS [28]

2. Westinghouse PPS Replacement Project ALS System Requirement Specification [17].
3. CSI document Number (No.) 6116-00011, Diablo Canyon PPS ALS System Design Specification [19]
4. CSI document No. 6116-10201 Diablo Canyon PPS ALS-102 FPGA Requirements Specification [20]
5. DCPP Tricon Software Requirements Specification (SRS) [75]

Where vendor documents that discuss specific compliance are available, they are cited.

The documentation and description are on two levels. First, the individual Protection Sets (i.e., divisions) that implement the protective functions in the PPS replacement are described, including the signal flows between the various hardware items. Second, the overall system is described with particular emphasis on additional hardware items not included in the description of the channels or divisions, such as voters, communications with workstations or non-safety systems, bypass functions/switches, and diverse actuation systems. The data communication pathways are described in detail using the guidance in DI&C-ISG-06 [1] Section D.7, "Communications."

Throughout this document, mention will be made of Process Protection Sets and channels. It is important to understand these terms as used at DCPP because the terminology is somewhat different from that used at other installations.

A process channel is an arrangement of components, modules and software as required to generate *a single protective action signal* when required by a generating station condition [FSAR [26] Section 7.1].

Redundant process instrumentation channels are separated by locating the electronics in different protection "sets". The PPS at DCPP is comprised of four such Protection Sets. Each Protection Set is further comprised of various process "channels". Table 4-1 illustrates a typical relationship among Protection Sets and process channels for the Pressurizer Pressure Protection function.

4.1 DCPP PPS Overview

The protective functions initiated by the PPS are broadly classified into the following two major categories: tripping of the reactor and the actuation of ESF. This discussion focuses on the PPS safety-related functions from two functionally defined systems: the RTS and the ESFAS.

The design basis of the PPS is to actuate the RTS and/or the ESFAS, whenever necessary to:

- Prevent core damage from an anticipated transient
- Limit core damage from infrequent faults

- Preserve the integrity of the RCS pressure boundary during limiting fault conditions
- Limit site radiological releases to acceptable limits

Table 4-1 Pressurizer Pressure Protection Channels and Protection Sets

Protection Set	Sensor Input to Channel	Channel	Channel Output to SSPS
I	PT-455	PZR Pressure Low Rx Trip PZR Pressure High - Unblock SI (P-11) PZR Pressure High Rx Trip PZR Pressure Low-Low SI PZR Pressure High - PORV	PC-455C PC-455B PC-455A PC-455D PC-455E
II	PT-456	PZR Pressure Low Rx Trip PZR Pressure High - Unblock SI (P-11) PZR Pressure High Rx Trip PZR Pressure Low-Low SI PZR Pressure High - PORV	PC-456C PC-456B PC-456A PC-456D PC-456E
III	PT-457	PZR Pressure Low Rx Trip PZR Pressure High - Unblock SI (P-11) PZR Pressure High Rx Trip PZR Pressure Low-Low SI PZR Pressure High - PORV	PC-457C PC-457B PC-457A PC-457D PC-457E
IV	PT-474	PZR Pressure Low Rx Trip PZR Pressure High - PORV PZR Pressure High Rx Trip PZR Pressure Low-Low SI	PC-474A PC-474B PC-474C PC-474D

Note: Power Operated Relief Valve (PORV) outputs go to the Auxiliary Safeguards Rack, not the SSPS.

The PPS provides signals that automatically shut down the reactor when the limits of safe operation are approached. The safe operating region is defined by several considerations, such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. Therefore, the PPS monitors process variables that are directly related to equipment mechanical limitations, such as pressurizer pressure and water level, and variables that directly affect the heat transfer capability of the reactor, such as reactor coolant flow and temperatures. Upon coincidence that multiple directly measured process or calculated variables exceed setpoints, the reactor is shut down to protect against damage to fuel cladding or loss of system integrity that could lead to release of radioactive fission products. The ESFAS actuates various engineered safety features (ESF) equipment that performs protective actions to mitigate the consequences of postulated accidents. Coincidence logic functions are performed by the SSPS described in the next section of this LAR.

The PPS is highlighted in Figure 4-1 to illustrate the scope of this project, as well as to illustrate the major systems with which the PPS interfaces.

The remainder of this section describes PPS functions in detail Refer to Figure 4-2 for a simplified depiction of the existing Eagle 21 PPS architecture.

The DCPP FSAR [26] Chapter 15 design basis events described in this section are discussed in more detail in the previously approved DCPP D3 Assessment [6, 7]. The Assessment lists each event by FSAR [26] Chapter 15 section and includes primary, backup and diverse mitigation. The Assessment describes the methodology to ensure that events credited with automatic mitigation in the DCPP FSAR [26] will continue to be mitigated automatically given a concurrent CCF in the PPS replacement.

Figure 4-1 Westinghouse Pressurized Water Reactor Protection System Concept

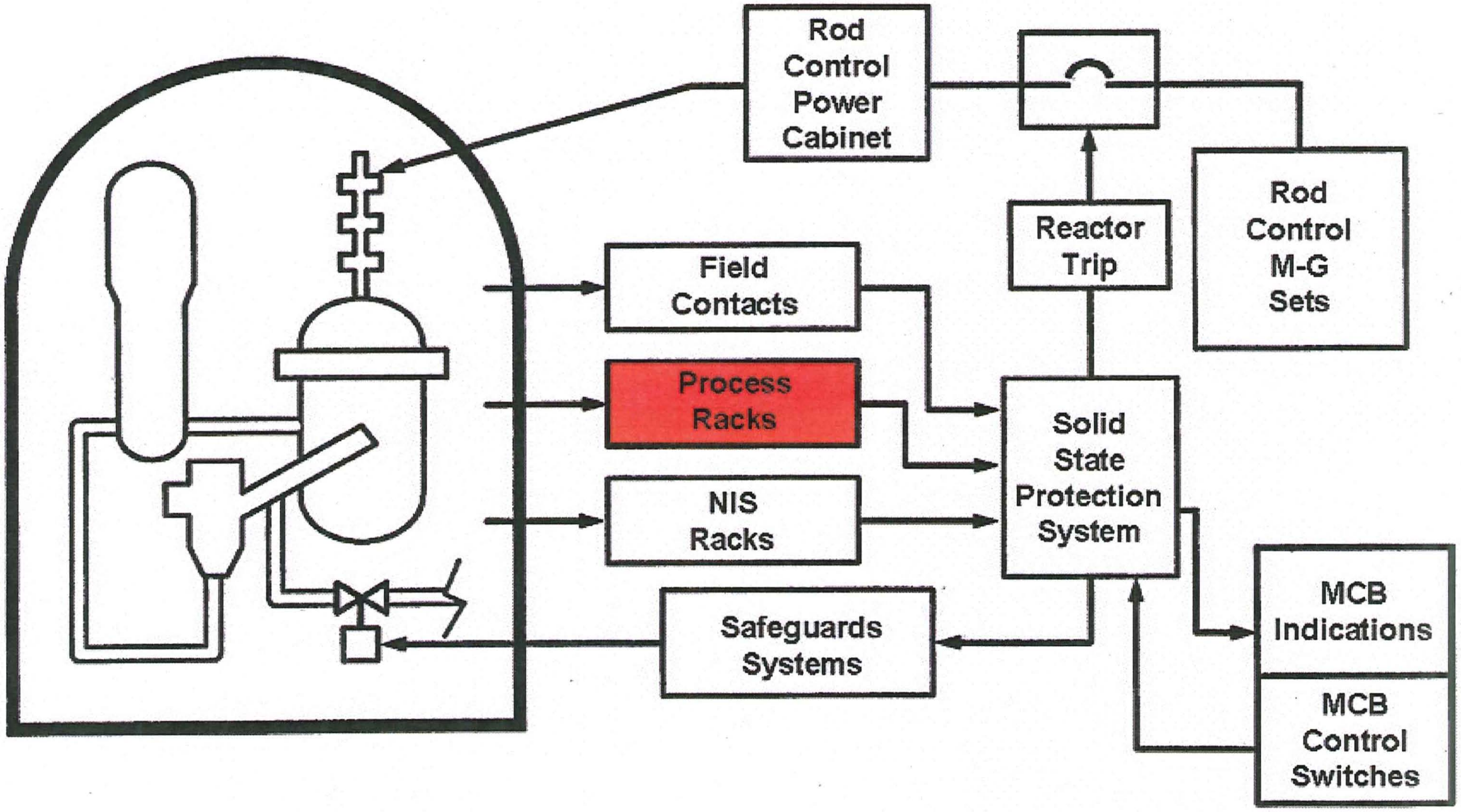
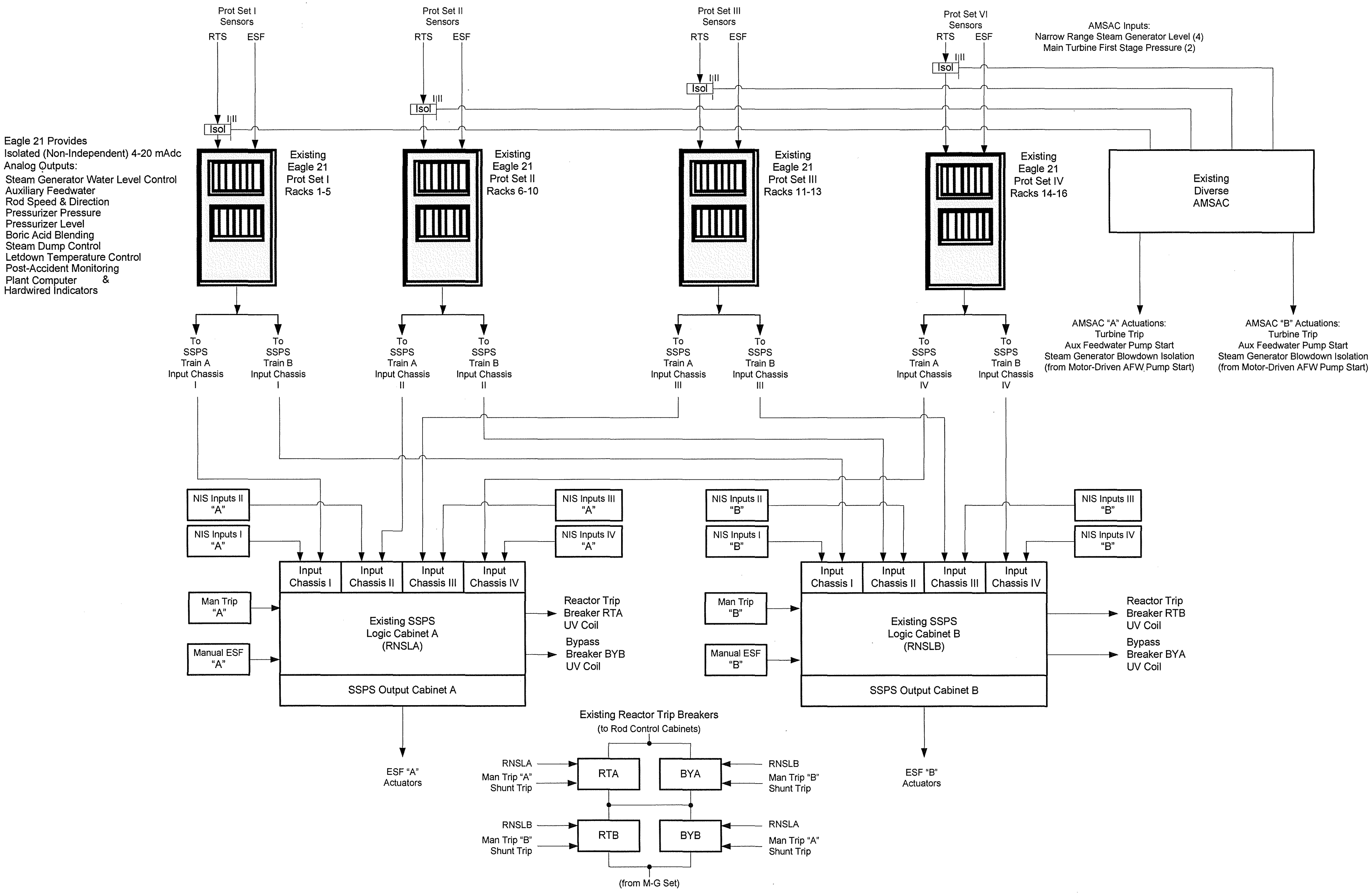


Figure 4-2 Simplified Diablo Canyon Process Protection System (Existing Eagle 21)



4.1.1 SSPS

The PPS monitors plant parameters, compares them against setpoints and provides signals to the SSPS if setpoints are exceeded. The SSPS evaluates the signals and performs RTS and ESFAS functions to mitigate Abnormal Operational Occurrences and Design Basis Events described in FSAR [26] Chapter 15. The Abnormal Operational Occurrences are referred to as American Nuclear Society (ANS) Condition I "Operational Transients" in FSAR [26] Chapter 15 and are addressed in FSAR Chapter 15.1. The design basis accidents are referred to as ANS Condition II "faults of moderate frequency," ANS Condition III "infrequent faults," and ANS Condition IV "limiting faults" and are addressed in FSAR Chapter 15.2, 15.3, and 15.4 respectively. The SSPS is composed of two redundant, essentially identical trains (A and B) that are physically and electrically separated. The existing SSPS is not being modified by the PPS Replacement Project.

Inputs to the SSPS that are diverse from the PPS are derived from nuclear instrumentation sensors that are processed through the NIS, radiation monitoring sensors that are processed through the radiation monitoring system, and seismic sensors that are processed through the seismic monitoring system. Other diverse input signals are derived directly from the process sensor by way of contacts in the sensor (such as auto stop oil pressure switches on the turbine, auxiliary contacts on circuit breakers, limit switches on turbine stop valves, etc.) or from control switches located in the control room.

Contacts of the SSPS input relays provide inputs to the logic portion of the SSPS where the coincidence logic (2-out-of-3, 2-out-of-4, etc.) is performed. Additional redundant inputs enter the logic directly from the control board switches and pushbuttons.

Power is supplied to the undervoltage (UV) coils of the RT switchgear by the SSPS. The RT signal to the UV coils de-energizes the power source for the coils. The SSPS logic provides automatic RT signals to the RT switchgear.

The solid state logic also operates master relays in the output bay of the SSPS. The master relay contacts, in turn, operate slave relays that actuate the ESF. The slave relays are used for contact multiplication.

Information concerning the PPS status is transmitted to the control board status lamps and annunciators by way of the SSPS control board demultiplexer and to the PPS by way of the SSPS computer demultiplexer. The SSPS provides about 200 isolated signals to the computer and the control board by way of demultiplexers. The multiplexing permits the transmittal of a large amount of status information over a small number of conductors, thereby simplifying and reducing the field wiring requirements. Time sharing of the multiplexer conductors is the principle used by the multiplexing system.

4.1.2 RT Switchgear

When the RT switchgear receives a RT signal from the SSPS, it de-energizes the RT breaker UV coil and energizes the shunt trip mechanism to open the RT breakers [Figure 4-2]. Opening of the RT breakers removes power to the control rod drive mechanisms permitting the control rods to fall by gravity into the reactor core, which rapidly inserts negative reactivity. The existing RT Switchgear is not being modified by the PPS Replacement Project.

The SSPS logic train A sends a trip signal to trip RT breaker A and bypass breaker B by way of each respective breaker UV coil and the shunt trip relay (RT breaker only). An equivalent, but independent trip signal is sent simultaneously from train B to RT breaker B and bypass breaker A, also by way of the individual breaker UV coil and shunt trip relay.

4.1.3 RTS Functions

Nuclear instrumentation, process protection instrumentation, seismic instrumentation or field sensors generates initiation signals which are sent to the SSPS when a plant parameter relative to plant safety exceeds a setpoint. The SSPS generates actuation signals to the RT breaker UV coil and shunt trip attachment when logical coincidence conditions are satisfied. This opens the RT breakers and releases the control rods, allowing them to fall by gravity into the reactor core.

The conditions that require a RT to prevent core damage are as follows:

1. Departure from nucleate boiling (DNB) ratio (DNBR) approaching the limiting value
2. Fuel rod linear power density approaching its rated value
3. RCS overpressure creating stresses approaching system design limits

The plant variables required to be monitored to generate a RT are as follows:

1. Neutron flux
2. RCS temperature (narrow range)
3. RCS pressure (pressurizer pressure)
4. Pressurizer water level
5. Reactor coolant flow
6. Reactor coolant pump (RCP) operational status (bus undervoltage, bus underfrequency, and pump motor circuit breaker position)
7. Steam generator water level (narrow range)
8. Turbine/generator operational status (trip fluid pressure and stop valve position)
9. Seismic acceleration

The variables for items 6, 8, and 9 are generated by discreate devices outside the PPS and provide direct contact inputs to the SSPS and the signals associated with the variables operate independently from the PPS. In addition, a manual RT, a RT on manual or automatic SI, and a hardware problem related RT are provided.

PPS monitored variables are identified in Section 4.10.3.4.

4.1.4 ESFAS Functions

The capability is provided to sense plant conditions that require the initiation of the ESF. The ESF act to limit the consequences of faulted conditions. The ESFAS automatically provides output signals for the timely actuation of the various ESF functions, consistent with the design bases of these systems.

The conditions that require the actuation of ESF are as follows:

1. Primary System Accidents
    a. Rupture of small pipes or cracks in large pipes
    b. Rupture of RCS pipes
    c. Steam generator tube rupture (SGTR)
    d. Rod ejection accident
2. Secondary System Accidents
    a. Rupture of a major Steamline or Feedwater line
    b. Minor secondary system pipe breaks
    c. Loss of main feedwater (MFW)
    d. Loss of offsite alternating current (AC) power
    e. Feedwater malfunction (excessive feedwater flow accidents)

The plant variables required to be monitored for the automatic initiation of ESF are as follows:

1. RCS pressure (Pressurizer pressure)
2. Containment pressure
3. Steamline pressure
4. Steamline pressure rate of change
5. Steam generator water level (narrow range)
6. Containment exhaust radiation (generated outside the PPS)
7. RT breaker position (Permissive P-4) (generated outside the PPS)

The variables for item 6, containment exhaust radiation, and item 7, RT breaker position, are generated outside the PPS and provide direct contact inputs to the SSPS and the signals associated with the variables operate independently from the PPS.

Protective functions initiated by the ESFAS to limit plant fault conditions are as follows:

1. SI Actuation (SI Signal)
2. Turbine Trip
3. Containment Spray
4. Containment Isolation Phase A
5. Containment Isolation Phase B
6. Containment Ventilation Isolation (CVI)
7. Main Steam Isolation
8. MFW Isolation
9. AFW Initiation

The low Steamline pressure, the low Pressurizer pressure, or the high containment pressure protection functions initiate SI actuation and a subsequent RT. SI actuation initiates an "S" safety signal, Feedwater Isolation, Containment Phase "A" Isolation, and CVI. Feedwater Isolation, Containment Phase "A" isolation, and CVI are individually latched, either in the SSPS cabinets or implicitly latched by the nature of the actuated component. The "S" signal is latched in the SSPS cabinet. Manual action is required to reset latched signals.

4.1.5 Existing Source Range NIS Protection Functions

The source range and intermediate range nuclear instrumentation form the first two overlapping steps of nuclear protection. The power range nuclear instrumentation provides the third and final overlapping step in nuclear protection.

The source range NIS primary protection function is to provide input signals to the SSPS low power RTs and indication. The source range function trips the reactor when 1-out-of-2 source range channels read above the trip setpoint. The NIS is entirely independent of the PPS.

4.1.6 Existing Intermediate Range NIS Protection Functions

The intermediate range nuclear instrumentation provides the second of three overlapping steps of nuclear protection. The intermediate range nuclear instrumentation function is to provide a high neutron flux RT. The intermediate range function trips the reactor when 1-out-of-2 intermediate range channels read above the trip setpoint. The NIS is entirely independent of the PPS.

4.1.7 Existing Power Range NIS Protection Functions

The nuclear power range instrumentation provides the third overlapping step in nuclear protection. The power range nuclear instrumentation function provides high neutron flux RTs. Two trip setpoints are provided. The function of the high setpoint is to provide protection during power operation and is always active. The function of the low setpoint is to provide protection during startup. The power range function (high and low setpoints) trips the reactor when 2-out-of-4 power range channels read above the trip setpoint. The power range nuclear instrumentation also provides input to the Overtemperature and Overpower protection channels of the PPS. The NIS signal processing is entirely independent of the PPS.

4.1.8 Thermal Overtemperature and Overpower Protection Functions

The Thermal Overpower and Overtemperature Protection functions ensure fuel integrity is maintained by initiating two RTs: the thermal overpower trip (also known as overpower ΔT, OPΔT, or OPDT) and the thermal Overtemperature trip (also known as Overtemperature ΔT, OTΔT, or OTDT). These signals are generated in the PPS.

The thermal Overpower trip function is provided specifically to ensure operation within the fuel design basis. The overpower ΔT function trips the reactor when 2-out-of-4 overpower ΔT channels are above the trip setpoint.

The thermal Overtemperature trip function is provided specifically to ensure operation within the DNB design basis and to ensure operation within the hot leg boiling limit. The Overtemperature ΔT function trips the reactor when 2-out-of-4 Overtemperature ΔT channels are above the trip setpoint.

Reactor coolant temperature instrumentation also functions to generate the Tavg signal. Permissive P-12 is enabled when 2-out-of-4 Tavg channels read below the low-low Tavg setpoint. The P-12 setpoint is set below the no-load Tavg temperature. Permissive P-12 blocks closed all steam dump valves.

4.1.9 Pressurizer Pressure Protection Functions

The Pressurizer pressure channels perform the following protection functions:

1. Provide a high Pressurizer pressure RT function to prevent over pressurization of the RCS.

2. Provide a low Pressurizer pressure RT function to limit core boiling.

3. Provide a low Pressurizer pressure SI System actuation for Loss of Coolant Accidents (LOCA) and Steamline break protection.

4. Provide PORV automatic actuation signal to prevent RCS Pressurizer overfill without challenging the Pressurizer safeties for inadvertent SI at power.

5. Generate Pressurizer SI Permissive P-11, which allows the operator to manually block the low Pressurizer pressure SI actuation and enable high negative Steamline pressure rate Steamline isolation actuation at low reactor coolant pressures.

The Pressurizer pressure signals are also used as an input to the OTΔT and OPΔT setpoints described above. These signals are generated in the PPS.

In addition, low temperature overpressure protection (LTOP) is provided by wide range RCS pressure measurement channels PT-403A and PT-405A, which open the Pressurizer PORV PCV-455C and PCV-456, respectively upon an overpressure condition while the reactor is at low temperature. This protection function is performed in the Auxiliary Safeguards Rack and is independent of the SSPS.

The high Pressurizer pressure RT works in conjunction with the Pressurizer relief valves and Pressurizer safety valves to prevent RCS over pressurization. The Pressurizer pressure function trips the reactor when 2-out-of-4 Pressurizer pressure channels read above the trip setpoint. This trip is always active.

The low Pressurizer pressure RT function limits core boiling. The Pressurizer pressure function trips the reactor when 2-out-of-4 Pressurizer pressure channels read below the trip setpoint. The low Pressurizer pressure RT is automatically blocked when Low Power Permissive P-7 is cleared. Permissive P-7 is developed as the logical "OR" of Permissive P-10 and Permissive P-13. Power Range at Power Permissive P-10 is enabled when 2-out-of-4 power range channels are above the P-10 setpoint. Permissive P-13 is developed from 2-out-of-2 turbine impulse chamber pressure channels below the P-13 setpoint. Settings of the bistable comparators used to develop the permissives are not affected by the PPS Replacement Project.

The low Pressurizer pressure SI actuation provides protection in the event of a LOCA or Steamline break. The low Pressurizer pressure SI actuation setpoint is lower than the setpoint for low Pressurizer pressure RT discussed previously. The Pressurizer pressure function actuates SI when 2-out-of-4 Pressurizer pressure channels read below the actuation setpoint. The low Pressurizer pressure SI actuation is interlocked with Pressurizer SI Permissive P-11. The P-11 signal, generated by 2-out-of-3 Pressurizer pressure channels reading below the permissive setpoint, allows blocking of the low Pressurizer pressure SI actuation. Typically, low Pressurizer pressure SI is manually blocked during cooldown and depressurization of the RCS. The block may be manually removed for return to normal operation. The manual low Pressurizer pressure SI block is automatically removed when the Pressurizer pressure signals rise above the P-11 setpoint. Clearing of the P-11 signal also opens the accumulator isolation valves.

4.1.10 Pressurizer Level Protection Function

The high Pressurizer water level trip is provided as a back-up to the high Pressurizer pressure trip. This trip also prevents releasing water through the Pressurizer safety valves for certain transient conditions. The Pressurizer level function trips the reactor when 2-out-of-3 Pressurizer level channels are above the trip setpoint. This trip is automatically blocked when Low Power Permissive P-7 is cleared. These signals are generated in the PPS.

4.1.11 Reactor Coolant Loop Low Flow Protection Function

The primary reactor coolant loop low flow protection function is to protect the core from exceeding DNB limits during loss of reactor coolant flow by tripping the reactor. Forced reactor coolant flow would be reduced or lost following loss of power to one or more RCP, a loss of offsite power, or RCP bus underfrequency (UF). A RT is also required to ensure RCS cooling capability following an RCP locked rotor or shaft break. Since core flow decreases quickly during these transients, the Overtemperature ΔT trip does not respond fast enough to provide protection for loss of coolant flow events. These signals are generated in the PPS.

Each reactor coolant loop has three reactor coolant flow channels. Low reactor coolant flow in 2-out-of-3 channels in a loop (flow below the trip setpoint) generates a low flow signal for the loop. These low loop flow signals are interlocked with Low Power Permissive P-7 and Loss of Flow Permissive P-8. When Permissive P-7 is cleared, RT on low flow is blocked. Between Permissives P-7 and P-8 (only P-7 enabled), a RT on low flow in any one loop is blocked and the low flow function trips the reactor when 2-out-of-4 reactor coolant loops generate low flow signals. When Permissive P-8 is enabled, the low flow function trips the reactor when 1-out-of-4 reactor coolant loops generate a low flow signal.

With Low Power Permissive P-7 enabled, a RT is permitted on "low flow sensed" in any two loops. This "low flow sensed" for one loop may be in the form of the low flow signal for that loop or the RCP breaker open signal for that loop. Thus, combinations of low flow signals only, RCP breaker open signals only, or low flow signals and RCP breaker open signals may generate the RT.

4.1.12 RCP Bus Underfrequency Protection Function

The RCP bus underfrequency RT is a protective function used to protect the core from exceeding DNB limits during loss of reactor coolant flow due to a grid underfrequency condition. The low flow RT is not necessarily adequate to prevent DNBR from exceeding the limit value under these conditions except for very small rates of frequency decrease. Underfrequency on the 12 kV bus trips the reactor when 2-out-of-3 underfrequency sensors on either 12 kV bus indicate below the trip setpoint.

The underfrequency trip is interlocked with Low Power Permissive P-7 so that the trip signal is blocked when P-7 is cleared.

The 2-out-of-3 underfrequency signals on either of the two 12 kV buses are also used as a non-safety-related trip of the four RCP breakers to protect the motors if the grid frequency decreases significantly. These signals are developed outside the PPS.

4.1.13 RCP Bus UV Protection Function

The RCP bus UV protection function is to protect the core from exceeding DNB limits during loss of reactor coolant flow by tripping the reactor. This function provides protection to the core if AC power is lost to both RCP buses. The low flow RT does not respond quickly enough to provide adequate protection. UV on the 12 kV bus trips the reactor when 1-out-of-2 UV sensors on both 12 kV buses indicate below the trip setpoint. The UV trip is interlocked with Low Power Permissive P-7 so that the trip signal is blocked when Permissive P-7 is cleared. These signals are developed outside the PPS.

4.1.14 RCP Breaker Position Protection Function

The RCP breaker position protection function is provided to protect the core from exceeding DNB limits during loss of reactor coolant flow by tripping the reactor. This trip provides backup protection for the partial loss of flow accident in more than one loop, in which low flow is the primary trip, and for the total loss of flow accident in which 12 KV UV and underfrequency are the primary trips. The RCP breaker position trip was included to enhance the overall reliability of the RTS. Its function is not assumed or credited in any analysis. These signals are developed outside the PPS.

4.1.15 Seismic Acceleration RT Function

The seismic acceleration trip function provides a RT on seismic accelerometers sensing accelerations exceeding a predetermined setpoint to provide a RT due to the location of DCPP in a high seismic zone. The seismic trip is neither protective nor anticipatory; rather it is a DCPP licensing commitment. The seismic monitoring system provides digital inputs to the SSPS where the logic to generate a RT is performed. These signals are developed outside the PPS.

4.1.16 Containment Pressure Protection Functions

The containment pressure functions protect the containment building against over pressurization and minimize the release of radioactive fission products following mass and energy releases resulting from a high energy line rupture. Events that could result in a mass and energy release include various size LOCA, Steamline breaks, and Feedline breaks. Two containment pressure signals are provided. These are designated high and high-high in order of increasing containment pressure setpoint. These signals are generated in the PPS.

The protection functions performed by the high containment pressure signal are:

1. SI initiation
2. RT on a SI signal
3. Containment Isolation (Phase A Actuation)

The containment pressure function trips the reactor and initiates SI when 2-out-of-3 containment pressure channels read above the high trip/actuation setpoint.

The protection functions performed by the high-high containment pressure signal are:

1. Steamline isolation
2. Containment spray actuation
3. Containment isolation (Phase B actuation)

The containment pressure function initiates the above actions when 2-out-of-4 containment pressure channels read above the high-high actuation setpoint.

To prevent inadvertent actuation, containment spray on either an automatic or a manual containment spray signal requires a SI signal to be present concurrently. In addition, manual containment spray actuation requires actuation of two manual switches simultaneously.

The high-high containment pressure containment spray actuation signal and containment isolation phase B actuation signal are both latched signals requiring manual reset to remove the actuation signals even if the high-high containment pressure signal has cleared. The containment spray actuation signal and the containment isolation phase B actuation signal each has its own momentary manual reset controls. The containment spray manual reset control also resets the manual containment spray actuation signal.

Each high-high containment pressure channel can be bypassed for testing by a test bypass control on that channel (Refer to Section 4.3.8 of IEEE Standard 279 [99], Section 4.10 of this LAR, IEEE Standard 603 [21] compliance, and Section 4.11 of this LAR, IEEE Standard 7-4.3.2 [80] compliance). This is accomplished using manual bypass switches.

4.1.17 Steam Generator Level Protection Functions

The steam generator level protection functions prevent loss of reactor heat sink. A RT and AFW actuation, including steam generator blowdown and sample line isolation, are generated on low-low steam generator level. The steam generator level function trips the reactor and actuates AFW flow when 2-out-of-3 steam generator level channels read below the low-low trip/actuation setpoint in one or more steam generators.

The low-low steam generator level trip signals are delayed by the PPS trip time delay (TTD) functions. The TTD time interval is a direct function of reactor power level and the number of low-low steam generator level trip signals per Protection Set. The TTD is based on a low-low level in any single steam generator (S/G) below 50 percent power determined from reactor coolant Δ T. The TTD is zero when power is at 50 percent or above.

The steam generator high-high level protection function provides a turbine trip and Feedwater Isolation when 2-out-of-3 steam generator channels in any loop read above the high-high actuation setpoint. The Turbine Trip and Feedwater Isolation are designed to protect the integrity of the main steam lines, to protect the turbine from excessive moisture carryover and to protect against overfilling the steam generator, but are not required for reactor protection. The SI signal, which initiates the same two functions, is latched-in by a retentive memory circuit in the SSPS. The signal must be reset manually from the control room

The Feedwater Isolation consists of feedwater control valve and bypass control valve closure by both logic trains. Feedwater isolation valve closure is by Train A and feedwater pump trip is by Train B. When feedwater control valve and bypass control valve closure on a SI signal or high-high steam generator level (P-14) occurs coincident with RT (P-4), the valve closure signal is latched-in by a feedback signal. The only means of resetting these signals are to reset the RT breakers and to remove both the high-high steam generator level condition and the SI signal. This latched-in function serves to comply with IEEE Standard 279 [99] Section 4.16 by providing a means of ensuring completion of a protective action once initiated and requiring deliberate action on the part of the operator to return to normal operation. This function is always active.

The Feedwater Isolation valve closure (Train A) signal, feedwater pump trip (Train B) signal and the turbine trip signal that results in a RT, if power is above the Power Range at Power Permissive P-9 setpoint, are generated from the output of a retentive memory for the same input signal from steam generator high-high level or SI signal. This retentive memory provides latched-in signals for these functions. These functions can be returned to normal operation by the Feedwater Isolation Manual Reset switch in the control room. These functions are always active.

Feedwater control valve and bypass control valve closure is also initiated by low Tavg coincident with RT (P-4). This signal is latched-in by a retentive memory circuit in the SSPS. The signal must be reset manually from the control Room. The manual reset overrides this actuation signal, if present, until the actuation signal is removed.

4.1.18 Low Steamline Pressure Protection Function

This protection function actuates Steamline isolation and SI to provide protection for high energy secondary line breaks. The low Steamline pressure protection function actuates Steamline isolation and SI when 2-out-of-3 rate compensated pressure channels on any Steamline read a pressure below the low pressure setpoint. These signals are developed in the PPS.

When the Pressurizer SI Permissive (P-11) is present, the low Steamline pressure protection function may be manually blocked and is automatically reset when the Pressurizer pressure is above the P-11 setpoint. Blocking the low Steamline pressure protection function enables the high negative Steamline pressure rate protection function.

4.1.19 High Negative Steamline Pressure Rate Protection Function

This protection function actuates Steamline isolation to provide protection for Steamline break when the plant is between cold and hot shutdown conditions. The high negative Steamline pressure rate function actuates Steamline isolation when 2-out-of-3 pressure channels on any Steamline indicate a pressure rate greater than the negative pressure rate setpoint. These signals are developed in the PPS.

The high negative Steamline pressure rate Steamline isolation function is permitted when the low Steamline pressure protection function is manually blocked.

4.1.20 Protection Functions Associated With Steam Dump Control System

This protection function blocks steam dump on Low-Low Tavg (P-12) to prevent excessive cooldown due to steam dump control system failure. The steam dump block function is to limit the consequences of a steam dump system failure to those associated with one stuck-open valve (the worst postulated single failure).

Steam dump is blocked when P-12 is enabled by 2/4 T_{avg} below the P-12 setpoint. The P-12 setpoint is set below the no-load Tavg temperature. The steam dump block signal blocks air to the dump valves and vents the valve diaphragms. These signals are developed in the PPS. The P-12 setpoint is not affected by the PPS Replacement project.

The steam dump control system is a non-safety-related system. The block signals are interlocked with two independent pilot solenoid valves on each steam dump valve. These valves are not safety-related, but are interlocked with the P-12 signal from the SSPS. Each train of SSPS sends an independent signal to one of the pilot solenoid valves.

Four of the steam dump valves are designated as cooldown condenser dump valves, and are required for plant cooldown. Two manual controls (one per train) allow blocking the P-12 Permissive for the four cooldown condenser valves. The manual block can be manually reset if desired. The block is automatically reset when Permissive P-12 is cleared.

4.1.21 Turbine Derived Protection Function

The following existing plant protection system functions are derived from the turbine:

1. RT on turbine trip (Developed independently of the PPS)
2. Turbine impulse chamber pressure input to Turbine Low Power Permissive P-13 (Developed in the PPS)

The RT on turbine trip (turbine trip-RT) protects the reactor against loss of heat sink. At power levels above the P-9 setpoint, a RT occurs when at least 2-out-of-3 turbine auto-stop trip fluid pressure signals (in either logic train A or B) are below a fixed setpoint or when all four turbine stop valves are closed. RT on turbine trip is blocked when Power Range at Power Permissive P-9 is cleared. Turbine trip also generates a non-safety-related generator unit trip. Permissive P-9 is generated by 2 of 4 power range channels above the P-9 permissive setpoint. The P-9 setpoint is not affected by the PPS Replacement Project.

Turbine impulse chamber pressure is used as an indicator of turbine load and provides input for Turbine Low Power Permissive P-13. Permissive P-13 provides input for Low Power Permissive P-7.

4.1.22 Radiation Derived Protection Function

The existing radiation derived protection function terminates containment purging and pressure equalization during power operation and during core alterations or movement of irradiated fuel within containment. The containment exhaust is monitored for radioactivity by redundant radiation monitoring channels. When either of these monitoring channels reaches its high radiation alarm setpoint, a CVI signal is initiated. During Modes 1-4, the CVI signal is generated in the SSPS. During refueling Mode 6, when the SSPS may be de-energized, means are provided to generate the CVI signal independently of the normal SSPS power supply.

4.1.23 Manual RT

The function of the existing manual RT is to trip the reactor without using the automatic RT circuitry. Manual RT is accomplished by actuating open a normally closed contact wired in series between the SSPS output logic and the RT switchgear. This interrupts power to the trip breaker and bypass breaker undervoltage (UV) coils, resulting in a RT. In addition, a shunt trip relay is wired in parallel for each RT breaker. This relay simultaneously actuates the shunt trip function in each trip breaker. Redundant contacts allow either of the two controls provided to initiate a RT in both trains.

The manual RT control at the control console is equipped with a momentary reset position for resetting the RT breakers. Resetting the RT breakers is not a safety-related function. The reset switch is required for reactor restart.

4.1.24 Manual SI

There are two momentary controls in the existing control room systems level manual SI initiation. Redundant contacts allow either control to initiate SI in both trains. In addition, the manual SI actuation controls actuate the same RT breaker shunt trip function as the manual RT controls discussed in the previous section.

4.1.25 Manual Steamline Isolation

Manual Steamline isolation is accomplished by closing the main steam isolation valves and all main steam isolation bypass valves using the existing individual control switches. These controls are located in the control room. This function is not a part of the PPS hardware but is implemented within the Steamline isolation and bypass valve operation function. These controls are electrically downstream of PPS initiations and are therefore functional at all times.

4.1.26 Manual Containment Isolation, Phase A

There are two existing controls in the control room for systems level containment isolation phase A. Actuating either control initiates containment isolation phase A and CVI. Redundant contacts allow either control to initiate these functions in both trains. These controls are electrically downstream of PPS initiations and are therefore functional at all times.

4.1.27 Manual Containment Spray

The existing manual containment spray function has special functions designed to reduce the risk of inadvertent containment spray while still meeting IEEE Standard 279 [99] single failure criteria. Four momentary controls are provided in the control room. These controls are grouped into two pairs. Manual actuation of both controls in either pair initiates CVI and containment isolation phase B only. Concurrent manual containment spray signal and an interlocking automatic or manual SI actuation signal must be present to start the containment spray pumps and open the discharge valves. Redundant contacts allow either pair of controls to initiate these functions in both trains. These controls are electrically downstream of PPS initiations and are therefore functional at all times.

4.1.28 AMSAC

Isolated non-safety-related steam generator narrow range level and turbine first stage pressure analog signals are provided to the existing non-safety-related AMSAC system. The AMSAC trips the main turbine and, initiates AFW flow in the event an Anticipated Transient Without Scram (ATWS) results in the loss of the secondary heat sink. The steam generator blowdown and sample lines are isolated by signals from auxiliary contacts in the motor driven AFW pump control circuits.

The AMSAC is diverse and independent from the safety-related PPS, and is not safety-related. The level and pressure signals are isolated at the front end of the Eagle 21 PPS by analog current loop isolators that are independent of Eagle 21 digital processing. The PPS replacement provides equivalent isolation as specified in the PPS replacement FRS [28], Section 3.2.

The AMSAC is initiated by steam generator water level below the AMSAC trip setpoint. In addition to having a lower steam generator low water level setpoint than the PPS, a time delay is built into the initiating sequence to allow a RT to be initiated by the PPS before AMSAC is initiated. A main turbine load control interlock (C-20) is used to arm the AMSAC when turbine load is above a preset value. The AMSAC receives a single narrow range steam generator level signal from each steam generator (one from each of the four Protection Sets). The AMSAC initiation results when 3-out-of-4 steam generator level signals are below a predetermined setpoint. A preset time delay allows feedwater system transients to momentarily disrupt the feedwater flow without initiating the AMSAC. The AMSAC steam generator level trip setpoint is not affected by the PPS Replacement Project.

The AMSAC design is diverse from the design of the existing Eagle 21 PPS. Although both designs are based on microprocessors, each design uses a different type of microprocessor and interface bus to assure diversity and to eliminate common mode failures.

The non-safety related AMSAC input signals are isolated from the safety-related PPS measurement circuits by Instrument Class IA isolators which are part of the PPS and meet all of the Class IE requirements for isolators used for preventing control and protection system interaction. The isolators are used to prevent any electrical faults in the AMSAC from preventing the PPS from performing its safety-related functions.

The AMSAC output signals are isolated from the actuated devices by output relays which are classified Instrument Class IA. The output relays provide isolation between the safety-related control circuits actuated by the AMSAC and the non-safety-related AMSAC.

The AMSAC is diverse from the PPS replacement in terms of manufacturers, equipment design and software. The AMSAC was manufactured by Westinghouse using the now-obsolete Intel 8086 processor family. The Tricon portion of the PPS replacement is manufactured by Triconex using Motorola processors and entirely different architecture and programming. The ALS portion of the PPS replacement is manufactured by CSI using FPGA architecture and technology and does not utilize a microprocessor. With the AMSAC input signals isolated prior to any digital processing by Tricon or ALS PPS components, the AMSAC continues to satisfy the requirements of 10 CFR 50.62 regarding diversity from the protection system from sensor to actuated devices.

4.2 DCPP PPS Replacement Description

The PPS Replacement Project replaces in its entirety the Westinghouse Eagle 21 PPS hardware currently housed in PPS Racks 1 – 16 as illustrated in the shaded portion of Figure 4-3 (corresponding to the shaded portion of Figure 4-1). Equipment in the unshaded portion of Figure 4-3 is not being replaced or modified by this project.

PPS replacement functions are implemented in the same four (4) redundant Protection Sets shown in the shaded portion of Figure 4-3 as the existing Eagle 21 PPS. Each Protection Set uses a software-based Triconex Tricon processor described in Tricon V10 Topical Report Submittal [13] to mitigate events where the previously approved DCPP Eagle 21 PPS Replacement D3 Analysis [6] determined that existing diverse and independent automatic mitigating functions are available to mitigate the effects of postulated CCF concurrent with FSAR [26] Chapter 15 events. For the events where the DCPP PPS Replacement Diversity and Defense in Depth Analysis [6] determined that additional diversity measures were necessary to preclude manual mitigative action, automatic protective functions are performed in the diverse safety-related CSI ALS described in the ALS Topical Report Submittal [15] shown in the shaded portion of Figure 4-3. The PPS Replacement D3 strategy is described in Section 4.7 of this LAR.

Figure 4-4 illustrates a typical allocation of the automatic protection functions described in the previous section between the Tricon and the ALS in each of the four (4) redundant Protection Sets illustrated in the shaded portion of Figure 4-3. Automatic protective functions identified in Table 4-2 are generated in a software-based Triconex Tricon processor. Automatic protective functions identified in Table 4-3 are generated in a diverse Class IE CSI ALS to preclude manual action that would otherwise be required to mitigate events that occur with a concurrent CCF to the PPS. Table 4-4 lists the diverse protection functions not affected by the PPS replacement.

Figure 4-4 also illustrates the equipment outside the shaded portion of Figure 4-3 that is not affected by the Eagle 21 PPS Replacement Project. The PPS Replacement Project does not make any changes to the SSPS permissive or safety function logic.

Permissive function initiation signals generated within the existing PPS will continue to be performed by the replacement PPS and are not affected by the PPS Replacement Project. Permissive function initiation signals that are generated independently of the existing PPS will continue to be generated independently. The bistable comparator setpoints for the permissives are not changed by the PPS Replacement Project.

Figure 4-3 Simplified Diablo Canyon Process Protection System (After Replacement)

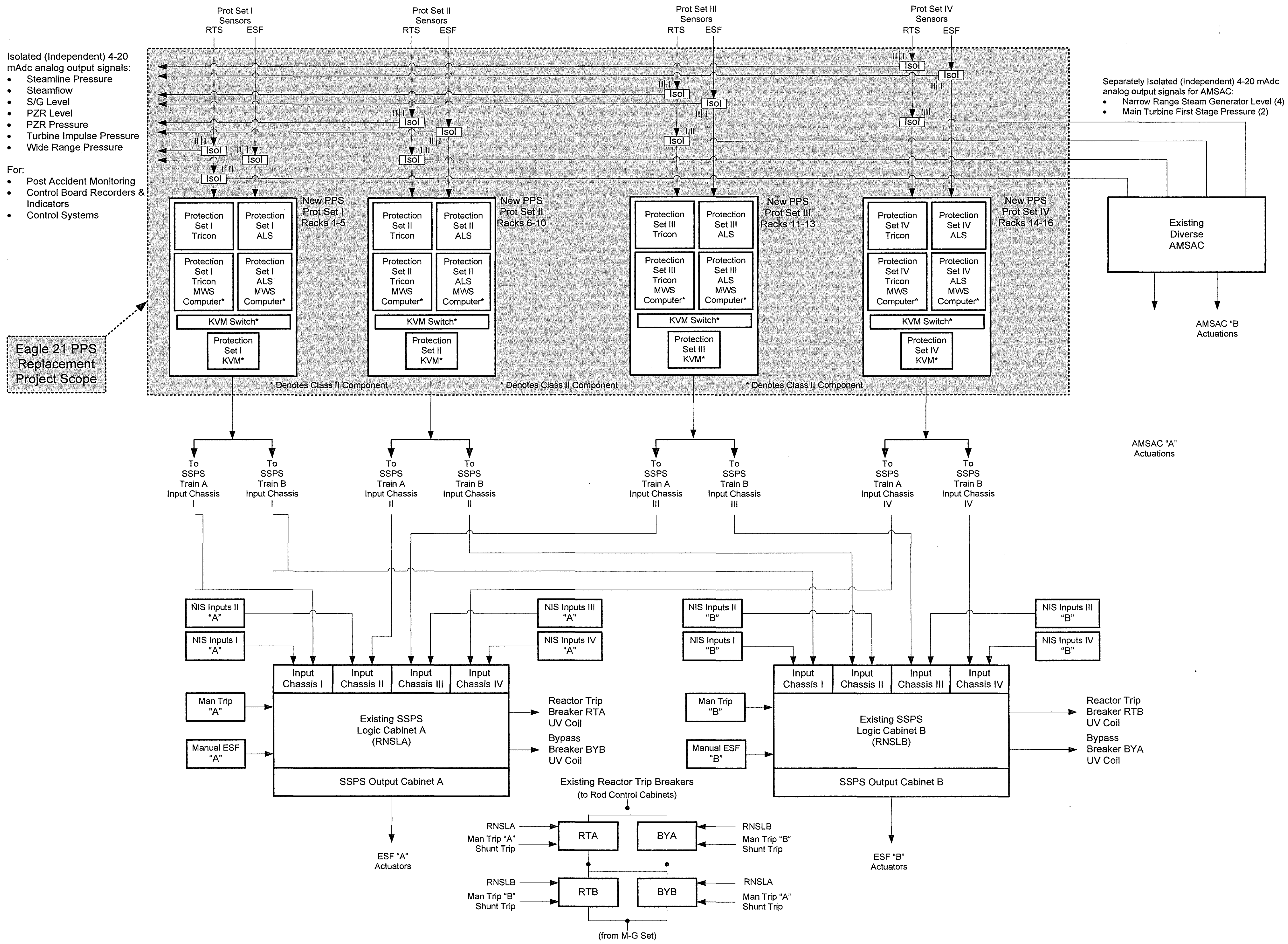

Prot Set I Sensors
RTS
ESF
Prot Set II Sensors
RTS
ESF
Prot Set III Sensors
RTS
ESF
Prot Set IV Sensors
RTS
ESF
Isolated (Independent) 4-20 mAdc analog output signals:
• Steamline Pressure
• Steamflow
• S/G Level
• PZR Level
• PZR Pressure
• Turbine Impulse Pressure
• Wide Range Pressure
For:
• Post Accident Monitoring
• Control Board Recorders & Indicators
• Control Systems
Isol
New PPS Prot Set I Racks 1-5
New PPS Prot Set II Racks 6-10
New PPS Prot Set III Racks 11-13
New PPS Prot Set IV Racks 14-16
Protection Set I Tricon
Protection Set I ALS
Protection Set I Tricon MWS Computer*
Protection Set I ALS MWS Computer*
KVM Switch*
Protection Set I KVM*
Protection Set II Tricon
Protection Set II ALS
Protection Set II Tricon MWS Computer*
Protection Set II ALS MWS Computer*
Protection Set II KVM*
Protection Set III Tricon
Protection Set III ALS
Protection Set III Tricon MWS Computer*
Protection Set III ALS MWS Computer*
Protection Set III KVM*
Protection Set IV Tricon
Protection Set IV ALS
Protection Set IV Tricon MWS Computer*
Protection Set IV ALS MWS Computer*
Protection Set IV KVM*
* Denotes Class II Component
Eagle 21 PPS Replacement Project Scope
Separately Isolated (Independent) 4-20 mAdc analog output signals for AMSAC:
• Narrow Range Steam Generator Level (4)
• Main Turbine First Stage Pressure (2)
Existing Diverse AMSAC
AMSAC "B Actuations
AMSAC "A" Actuations
To SSPS Train A Input Chassis I
To SSPS Train B Input Chassis I
To SSPS Train A Input Chassis II
To SSPS Train B Input Chassis II
To SSPS Train A Input Chassis III
To SSPS Train B Input Chassis III
To SSPS Train A Input Chassis IV
To SSPS Train B Input Chassis IV
NIS Inputs II "A"
NIS Inputs I "A"
NIS Inputs III "A"
NIS Inputs IV "A"
NIS Inputs II "B"
NIS Inputs I "B"
NIS Inputs III "B"
NIS Inputs IV "B"
Input Chassis I
Input Chassis II
Input Chassis III
Input Chassis IV
Man Trip "A"
Manual ESF "A"
Existing SSPS Logic Cabinet A (RNSLA)
SSPS Output Cabinet A
Reactor Trip Breaker RTA UV Coil
Bypass Breaker BYB UV Coil
Man Trip "B"
Manual ESF "B"
Existing SSPS Logic Cabinet B (RNSLB)
SSPS Output Cabinet B
Reactor Trip Breaker RTB UV Coil
Bypass Breaker BYA UV Coil
ESF "A" Actuators
ESF "B" Actuators
Existing Reactor Trip Breakers (to Rod Control Cabinets)
RNSLA
Man Trip "A" Shunt Trip
RTA
BYA
RNSLB
Man Trip "B" Shunt Trip
RNSLB
Man Trip "B" Shunt Trip
RTB
BYB
RNSLA
Man Trip "A" Shunt Trip
(from M-G Set)

Figure 4-4 Typical Replacement Protection Set

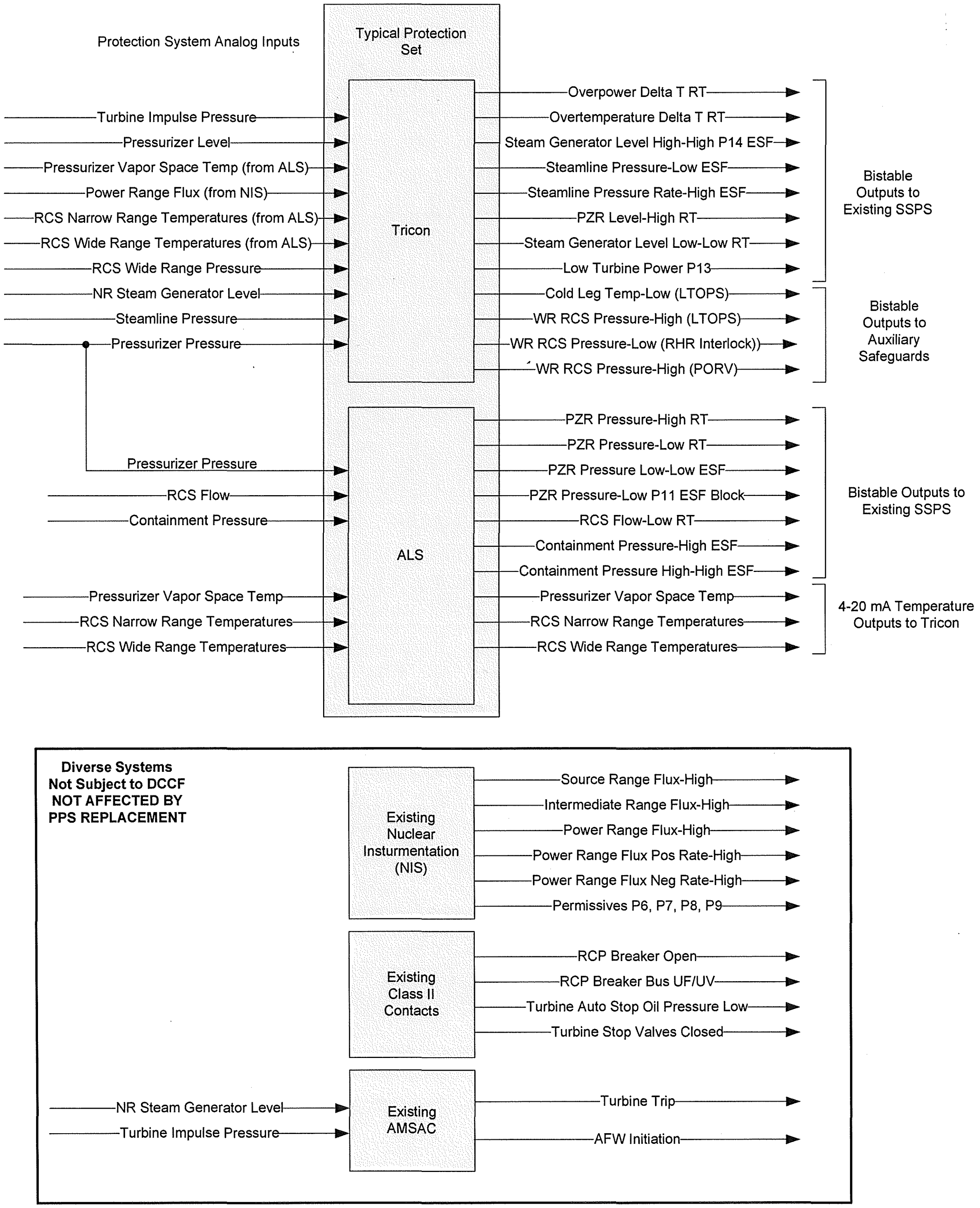

Protection System Analog Inputs
Typical Protection Set
Tricon
Turbine Impulse Pressure
Pressurizer Level
Pressurizer Vapor Space Temp (from ALS)
Power Range Flux (from NIS)
RCS Narrow Range Temperatures (from ALS)
RCS Wide Range Temperatures (from ALS)
RCS Wide Range Pressure
NR Steam Generator Level
Steamline Pressure
Pressurizer Pressure
Overpower Delta T RT
Overtemperature Delta T RT
Steam Generator Level High-High P14 ESF
Steamline Pressure-Low ESF
Steamline Pressure Rate-High ESF
PZR Level-High RT
Steam Generator Level Low-Low RT
Low Turbine Power P13
Bistable Outputs to Existing SSPS
Cold Leg Temp-Low (LTOPS)
WR RCS Pressure-High (LTOPS)
WR RCS Pressure-Low (RHR Interlock))
WR RCS Pressure-High (PORV)
Bistable Outputs to Auxiliary Safeguards
ALS
Pressurizer Pressure
RCS Flow
Containment Pressure
Pressurizer Vapor Space Temp
RCS Narrow Range Temperatures
RCS Wide Range Temperatures
PZR Pressure-High RT
PZR Pressure-Low RT
PZR Pressure Low-Low ESF
PZR Pressure-Low P11 ESF Block
RCS Flow-Low RT
Containment Pressure-High ESF
Containment Pressure High-High ESF
Bistable Outputs to Existing SSPS
Pressurizer Vapor Space Temp
RCS Narrow Range Temperatures
RCS Wide Range Temperatures
4-20 mA Temperature Outputs to Tricon
Diverse Systems Not Subject to DCCF NOT AFFECTED BY PPS REPLACEMENT
Existing Nuclear Instrumentation (NIS)
Source Range Flux-High
Intermediate Range Flux-High
Power Range Flux-High
Power Range Flux Pos Rate-High
Power Range Flux Neg Rate-High
Permissives P6, P7, P8, P9
Existing Class II Contacts
RCP Breaker Open
RCP Breaker Bus UF/UV
Turbine Auto Stop Oil Pressure Low
Turbine Stop Valves Closed
NR Steam Generator Level
Turbine Impulse Pressure
Existing AMSAC
Turbine Trip
AFW Initiation

Table 4-2 Process Variable Inputs to Tricon for RTS/ESFAS Functions

Process Variable	**Protection Functions**
Pressurizer (PZR) Level	Pressurizer High-Level RT
Power Range Neutron Flux	Input to Overtemperature Δ Temperature (OTDT) RT
	Input to Overpower Δ Temperature (OPDT) RT
RCS Narrow-Range Temperature	Input to OTDT RT
	Input to OPDT RT
	Input to Steam Generator Low-Low Level TTD
Steam Generator Level	Steam Generator Low-Low Level RT
	Hi-Hi Level Feedwater Isolation
	Hi-Hi Level Turbine Trip
	Hi-Hi Level MFW Pump Trip
	Low-Low Level AFW Actuation; process sense performed by PPS. AMSAC utilizes independently isolated level signals and independent turbine impulse pressure channels to provide diverse AFW initiation function
Steam Line Pressure	High-Negative Pressure Rate SLI
	Low-Pressure SI
	Low-Pressure SLI
Turbine Impulse Pressure	Permissive 13 (P-13) Low Turbine Power Permissive (Input to P-7 Low Power RT Permissive)

Table 4-3 Process Variable Inputs to ALS for RTS/ESFAS Functions

Process Variable	Protection Functions
Pressurizer Pressure	Pressurizer Low-Low Pressure SI
	Pressurizer SI Permissive (P-11)
	Pressurizer High-Pressure RT
	Pressurizer Low-Pressure RT
	Input to OTDT RT
Containment Pressure	High Pressure SI
	High Pressure (Phase A) Containment Isolation
	High Pressure (Phase B) Containment Isolation
	High-High Pressure Containment Spray
RCS Flow	RCS Low-Flow RT

Table 4-4 Diverse Protection Functions Not Affected by PPS Replacement

Process Variable	Protection Functions
Neutron Flux	Power-Range High-Flux (Low Setting) RT
	Power-Range High-Flux (High Setting) RT
	Power-Range Positive Flux Rate RT
	Power Range Flux Control Rod Stop
	Intermediate-Range High-Flux RT
	Source-Range High-Flux RT
	Input to OTDT RT (from Power Range)
AMSAC (Steam Generator Low Level)	Turbine Trip Above Control Interlock 20 (C-20) Permissive/RT Above Power Range Permissive P-9
Main Turbine Stop Valve Position	Turbine Trip/RT
Turbine Auto Stop Oil Pressure Low	
RCP Bus UV	RT
RCP Bus Underfrequency	RT
RCP Circuit Breaker Open	RT

4.2.1 Processor Subsystems (Platforms)

PPS replacement architecture components are discussed in this document as follows:

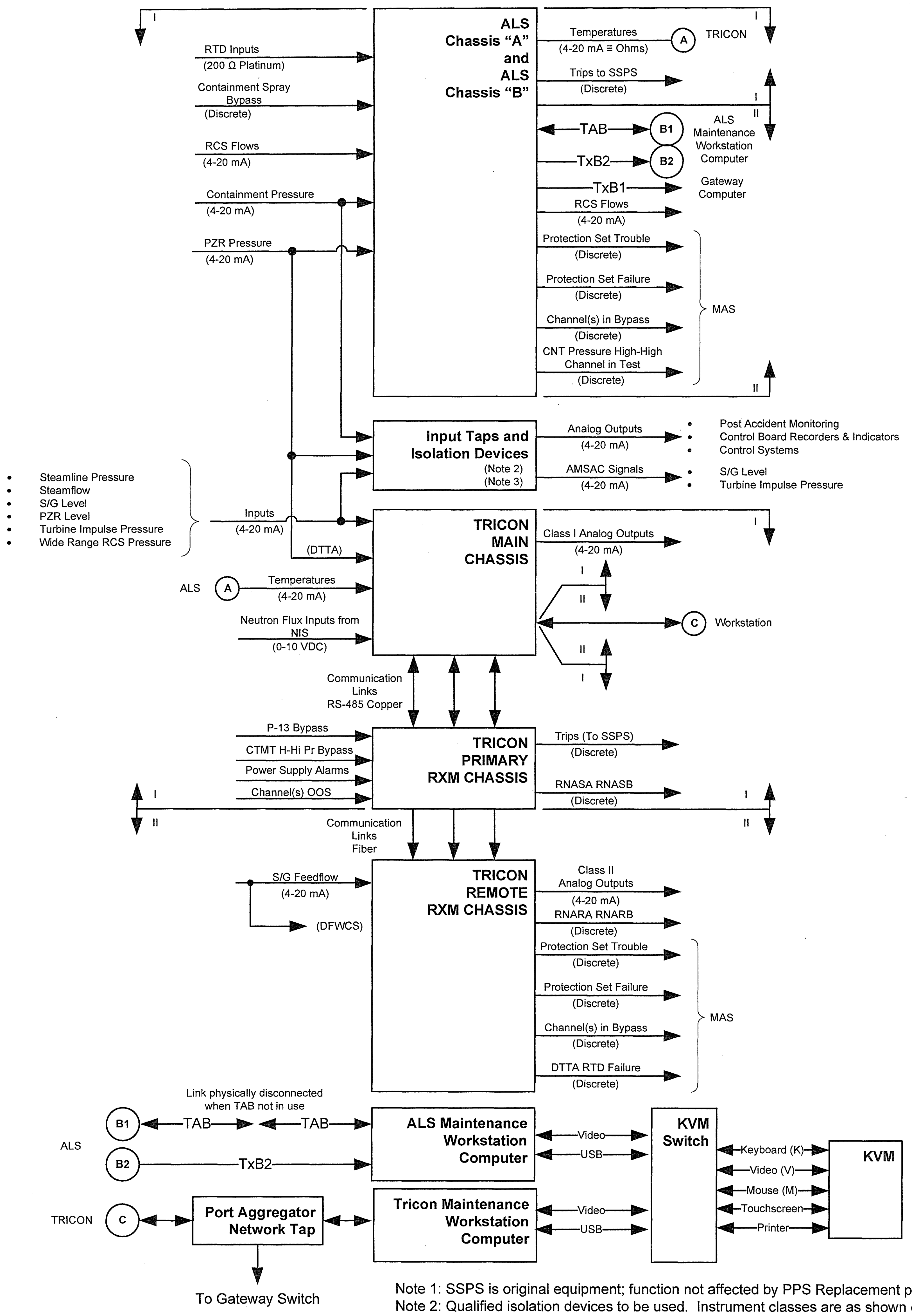
Table 4-5 Platform Cross-Reference

PPS Architecture Component	**LAR Section(s)**
FPGA-Based ALS Platform	4.2.1.2
ALS Processors	4.2.2.2
ALS Input/Output (I/O) Boards	4.2.3.2 Input 4.2.3.3 Output
ALS Power Supplies	4.2.7.2 Chassis Power Supplies 4.2.7.3 I/O Power Supplies 4.2.7.5 I/O Power Supplies
ALS Communications Modules	4.2.4.3
Tricon Platform • Main Chassis • Expansion Chassis • External Termination Assembly (ETA)	4.2.1.1
Tricon Processors	4.2.2.1
Tricon I/O Boards	4.2.3.1
Tricon Power Supplies	4.2.7.1 Chassis Power Supplies 4.2.7.3 Analog Inputs 4.2.7.4 I/O Power Supplies
TCMs	4.2.4.1 (TCM – External systems) 4.2.4.2 Remote Expander Module (RXM) – Interchassis)
MWS	4.2.9
Port Aggregator Network Tap and Media Converters	4.2.13

Figure 4-5 illustrates typical functional architecture for a single Eagle 21 replacement Protection Set.

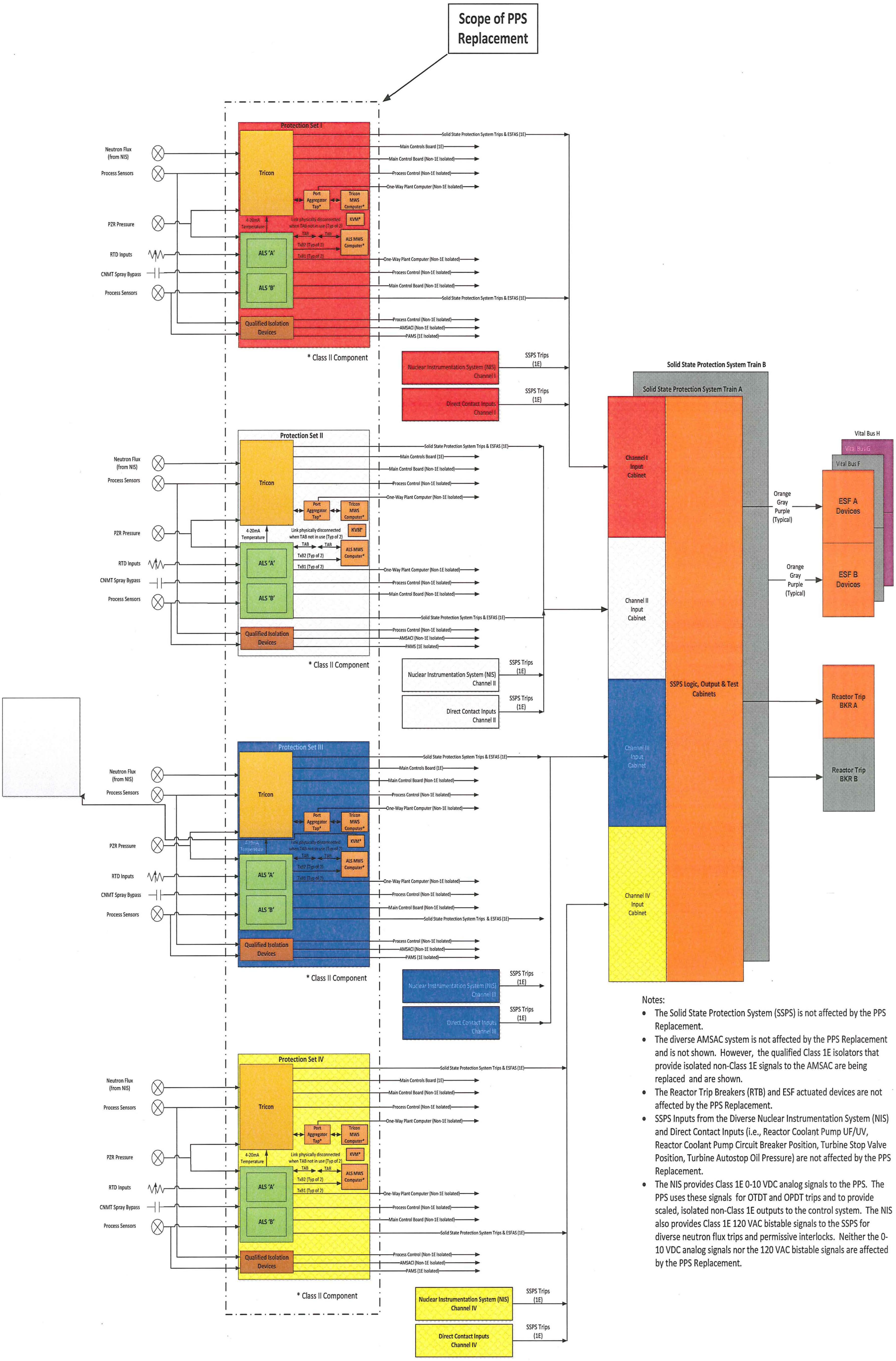
Figure 4-6 expands the shaded portion of Figure 4-3 to illustrate the relationship among the Protection Sets and interfacing systems.

Figure 4-5 Simplified Functional Architecture



Note 1: SSPS is original equipment; function not affected by PPS Replacement project
Note 2: Qualified isolation devices to be used. Instrument classes are as shown on Instrument Schematics.
Note 3: Several Class IB PAM functions obtain their signals directly from the Class I input loop. No isolation is necessary because the input loop is the correct classification. Details are provided in the IRS.

Figure 4-6 PPS Replacement Architecture


Scope of PPS Replacement
Protection Set I
Neutron Flux (from NIS)
Process Sensors
PZR Pressure
RTD Inputs
CNMT Spray Bypass
Process Sensors
Tricon
Port Aggregator Tap*
Tricon MWS Computer*
KVM*
4-20mA Temperature
Link physically disconnected when TAB not in use (Typ of 2)
TAB
TAB
ALS MWS Computer*
TxB2 (Typ of 2)
TxB1 (Typ of 2)
ALS 'A'
ALS 'B'
Qualified Isolation Devices
Solid State Protection System Trips & ESFAS (1E)
Main Controls Board (1E)
Main Control Board (Non-1E Isolated)
Process Control (Non-1E Isolated)
One-Way Plant Computer (Non-1E Isolated)
One-Way Plant Computer (Non-1E Isolated)
Process Control (Non-1E Isolated)
Main Control Board (Non-1E Isolated)
Solid State Protection System Trips & ESFAS (1E)
Process Control (Non-1E Isolated)
AMSACI (Non-1E Isolated)
PAMS (1E Isolated)
* Class II Component
Nuclear Instrumentation System (NIS) Channel I
SSPS Trips (1E)
Direct Contact Inputs Channel I
SSPS Trips (1E)
Protection Set II
* Class II Component
Nuclear Instrumentation System (NIS) Channel II
SSPS Trips (1E)
Direct Contact Inputs Channel II
SSPS Trips (1E)
Protection Set III
* Class II Component
Nuclear Instrumentation System (NIS) Channel III
SSPS Trips (1E)
Direct Contact Inputs Channel III
SSPS Trips (1E)
Protection Set IV
* Class II Component
Nuclear Instrumentation System (NIS) Channel IV
SSPS Trips (1E)
Direct Contact Inputs Channel IV
SSPS Trips (1E)
Solid State Protection System Train B
Solid State Protection System Train A
Channel I Input Cabinet
Channel II Input Cabinet
Channel III Input Cabinet
Channel IV Input Cabinet
SSPS Logic, Output & Test Cabinets
Vital Bus H
Vital Bus G
Vital Bus F
Orange Gray Purple (Typical)
ESF A Devices
Orange Gray Purple (Typical)
ESF B Devices
Reactor Trip BKR A
Reactor Trip BKR B

Notes:

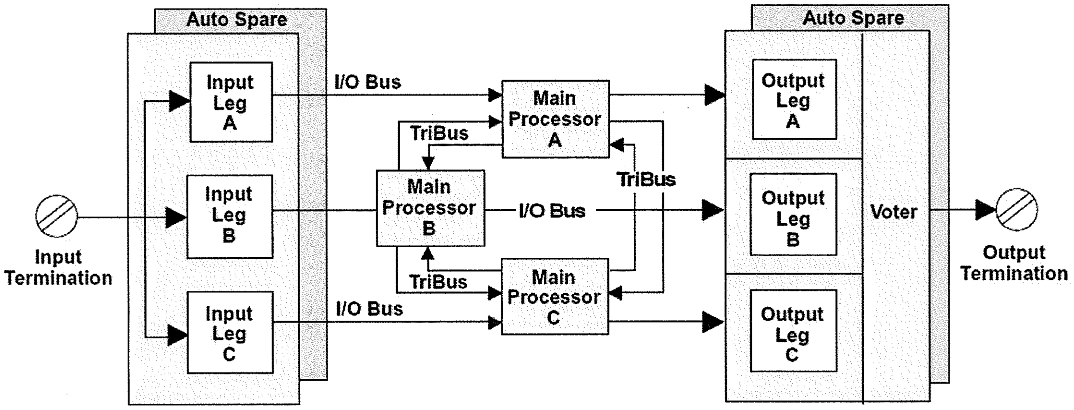
- The Solid State Protection System (SSPS) is not affected by the PPS Replacement.
- The diverse AMSAC system is not affected by the PPS Replacement and is not shown. However, the qualified Class 1E isolators that provide isolated non-Class 1E signals to the AMSAC are being replaced and are shown.
- The Reactor Trip Breakers (RTB) and ESF actuated devices are not affected by the PPS Replacement.
- SSPS Inputs from the Diverse Nuclear Instrumentation System (NIS) and Direct Contact Inputs (i.e., Reactor Coolant Pump UF/UV, Reactor Coolant Pump Circuit Breaker Position, Turbine Stop Valve Position, Turbine Autostop Oil Pressure) are not affected by the PPS Replacement.
- The NIS provides Class 1E 0-10 VDC analog signals to the PPS. The PPS uses these signals for OTDT and OPDT trips and to provide scaled, isolated non-Class 1E outputs to the control system. The NIS also provides Class 1E 120 VAC bistable signals to the SSPS for diverse neutron flux trips and permissive interlocks. Neither the 0-10 VDC analog signals nor the 120 VAC bistable signals are affected by the PPS Replacement.

4.2.1.1 Triconex Tricon-Based PPS Equipment

The Tricon is triple redundant from input terminal to output terminal, as shown in Figure 4-7. The TMR architecture allows continued system operation in the presence of any single point of failure within the system. The TMR architecture also allows the Tricon to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault, the Tricon alarms the condition, removes the affected portion of the faulted module from operation, and continues to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

Figure 4-7 shows the arrangement of the Tricon input, Main Processor, and output modules. As shown, each input and output module includes three separate and independent input or output circuits or legs. These legs communicate independently with the three Main Processor modules. Standard firmware is resident on the Main Processor modules for all three microprocessors as well as on the input and output modules and communication modules, which are not shown in Figure 4-7, but are described in subsequent sections.

Figure 4-7 Tricon Triple Modular Redundant Architecture



The main components of a Tricon system are the chassis, the termination panels, the power supply modules, and the Main Processor, input/output (I/O), and communication modules. Functional requirements for this hardware are specified in Section 4.3 of EPRI TR-107330 [122]. A brief description of this hardware is provided below.

1. Main Chassis

   A Tricon system consists of one main chassis and up to fourteen additional expansion chassis. The Tricon main chassis supports the following modules:

   - Two redundant power supply modules
   - Three Main Processors

- Communications modules
- I/O modules

The Tricon main chassis has a keyswitch (hereafter refered to as Tricon keyswitch) that sets the system operating mode:

- RUN – Normal operation with read-only capability by externally connected systems, including TriStation. Normally, the switch is set to this position and the key is removed and stored in a secure location.
- PROGRAM – Allows for control of the Tricon system using an externally connected personal computer running the TriStation software, including application program downloads.
- STOP – Stops application program execution.
- REMOTE – Allows writes to application program variables by a TriStation personal computer or by MODBUS masters and external hosts.

The STOP function is disabled in the application software configuration to prevent inadvertent application program halt [Triconex Application Guide [13] Appendix B, page 13].

The Tricon keyswitch will be in the RUN position when the Tricon is performing safety related functions and is not bypassed or manually tripped. If the Tricon keyswitch is not in the RUN position, an alarm is initiated on the control room Main Annunciator System (MAS) and the Tricon is considered inoperable [Triconex Application Guide [13] Appendix B, page 31]. Detailed information on the design and operation of the Tricon keyswitch is contained in Section 4.8.10.

Safety-related operation in REMOTE mode is permitted [Triconex Application Guide [13] Appendix B, page 31]. This mode will not be used in the PPS replacement.

The Tricon normally does not contain any disabled points unless there is a specific reason for disabling them, such as testing. To disable points, the Tricon keyswitch must be in PROGRAM mode rather than RUN or REMOTE mode. If the system does contain one or more disabled variables, an alarm on the Control Room MAS will be activated to indicate that disabled points are present. [Triconex Application Guide [13] Appendix B, page 52]. Disabling points for any reason will be under administrative control using an approved procedure.

A TriStation 1131 personal computer may be connected to an online Tricon with the Tricon keyswitch in the RUN position. In this mode, the TriStation cannot affect the program or variables and cannot pause or halt the application program. The TriStation 1131 includes password security features to lessen the chance of unauthorized access. For that reason, there are no restrictions to connecting a

TriStation personal computer to a Tricon [Triconex Application Guide [13] Appendix B, page 64].

The Tricon backplane is designed with dual independent power rails. Both power rails feed each of the three legs on each I/O module and each Main Processor module residing within the chassis. Power to each of the three legs is independently provided through dual voltage regulators on each module. Each power rail is fed from one of the two power supply modules residing in the chassis. Under normal circumstances, each of the three legs on each I/O module and each Main Processor module draw power from both power supplies through the dual power rails and the dual power regulators. If one of the power supplies or its supporting power line fails, the other power supply increases its power output to support the requirements of all modules in the chassis.

The Tricon has dual redundant batteries located on the main chassis backplane. If a total power failure occurs, these batteries maintain data and programs on the Main Processor modules for a period of six months. The system generates an alarm when the battery power is too low to support the system.

2. Expansion Chassis

   An Expansion Chassis is connected to the Main Chassis via three separate RS-485 data links, one for each of the three I/O legs. RXM, discussed in Section 4.2.4.2 are installed in the expansion chassis; therefore, three separate RS-485 data links are required for the three communications busses between the Primary RXM and the Remote RXM. The Tricon expansion chassis supports the following modules:

   - Two redundant power supply modules
   - Communications modules
   - I/O modules

3. ETA

   The ETAs are printed circuit board panels used for landing field wiring. The panels contain terminal blocks, resistors, fuses, and blown fuse indicators. The standard panels are configured for specific applications (e.g. digital input, analog input, etc.). Each termination panel includes an interface cable that connects the termination panel to the Tricon chassis backplane.

The Main Processor, I/O boards, the power supply modules and communication modules are discussed in subsequent sections. Additional detail regarding Triconex components can be found in Section 2.1 of the Tricon Version 10 PLC topical report [13] submittal to NRC.

In October of 2000 Triconex issued a topical report [8] to NRC as the basis for generic qualification of the TRICON PLC system for safety-related application in nuclear power plants for review by the staff of the NRC.

This document was also submitted to NRC by EPRI as a technical report entitled, "Generic Qualification of the Triconex Corporation Tricon Triple Modular Redundant Programmable Logic Controller System for Safety-Related Application in Nuclear Power Plants," document number 1000799, dated November 2000 [8].

By letter dated March 20, 2001, Triconex amended its original qualification summary report by submitting Topical Report 7286-546, "Amendment 1 to Qualification Summary Report," Revision 0, dated March 19, 2001 Agencywide Documents Access and Management System (ADAMS) Accession Number ML010810143) [9]. This amendment requested that NRC review and approve an update of the Triconex PLC from Version 9.3.1 to Version 9.5.3.

By letter dated June 26, 2001, Triconex again revised its qualification summary report by submitting Topical Report 7286-546, "Amendment 1 to Qualification Summary Report, Revision 1, dated June 25, 2001 (ADAMS Accession Number ML011790327) [10].

Based on these submittals, NRC issued a SER [11] for the platform on December 11, 2001 documenting staff findings that the platform possesses acceptable hardware and operating system software quality to be applied in safety-related RTS and ESFAS applications in nuclear power plants.

In September 2009, Triconex submitted a Topical Report [12] that was updated for the Version 10 Tricon as well as to address current regulatory issues. On May 15, 2012 IOM submitted the NRC approved Revision 4 to the Tricon Version 10 PLC topical report to NRC [13] as the basis for generic qualification of the system for safety-related application in nuclear power plants.

4.2.1.2 FPGA-Based ALS Platform

The diverse ALS portion of the PPS replacement [Figure 4-8] platform utilizes FPGA hardware logic rather than a microprocessor and therefore has no software component required for operation of the system. The built-in diversity of the ALS subsystem [16] ensures that the PPS replacement will perform the required safety functions automatically in the presence of a postulated CCF without an adverse impact on the operator's ability to diagnose the event or perform previously credited manual actuation activities.

Figure 4-8 does not illustrate the proprietary internal architecture of the ALS portion of the PPS replacement. Refer to the ALS Diversity Analysis [16] and Section 2 of the

ALS System Design Specification [19] as well as Section 4.7 of this LAR for description of the internal ALS architecture including diversity aspects and interfaces.

The ALS platform is designed as a universal safety system platform. The ALS provides advanced diagnostics and testability functions which improve the ability of plant I&C personnel to perform surveillance testing as well as diagnose failures should they occur. System integrity is greatly improved over existing systems by eliminating single point vulnerabilities while adding the capability to identify and address any failure within the system without causing a plant transient.

A typical safety application implemented using the ALS platform is comprised of one or more ALS chassis, and peripheral equipment consisting of Cabinets, Power Supplies, Control Panels, Assembly Panels and ASU. The Assembly Panels incorporate field terminal blocks, fuse holders, switches, and other application specific hardware. The ALS chassis is an industry standard 19" chassis. The ALS chassis contains ALS core logic, and I/O cards that are a CSI proprietary design.

Figure 4-8 Generic ALS FPGA Architecture

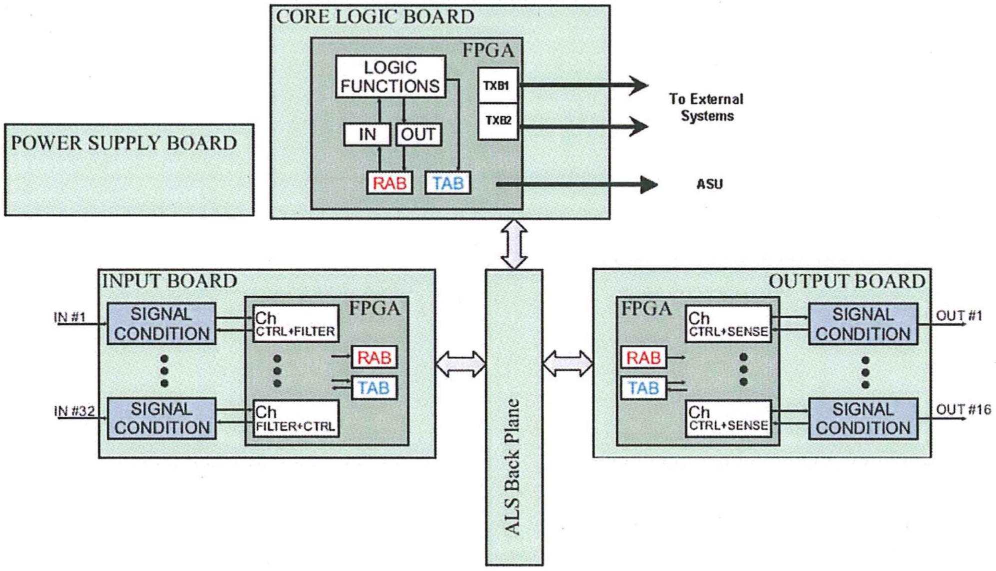


Table 4-3 identifies the PPS functions that are performed automatically by the ALS subsystem.

The ALS design practices and methodologies were first accepted by NRC in their review and approval of the much simpler Wolf Creek Main Steam and Feedwater Isolation System (MSFIS) [14]. However, the MSFIS safety evaluation [14] states that it is a unique application, and that future ALS applications, such as an RPS or ESFAS that receives input signals and makes trip decisions, may require additional design diversity. The PPS replacement receives input signals and makes trip decisions. Therefore, the proposed PPS Replacement Project provides additional design diversity, appropriate to its complexity, as discussed in Section 4.7, and in the ALS Diversity Analysis [16].

CSI submitted the ALS Topical Report Submittal [15] and supporting documentation, which describes generic qualification of the ALS for safety-related applications in nuclear power plants, for NRC approval .

The ALS Topical Report Submittal [15] and supporting documentation are currently being reviewed by NRC Staff. Therefore, this platform is referenced as a Tier 3 digital platform for application to the DCPP Eagle 21 PPS Replacement LAR and its approval is a prerequisite for NRC approval of this LAR.

4.2.2 Safety Function Processors

4.2.2.1 Triconex Main Processors

The Tricon subsystem of the PPS replacement utilizes three safety-related Model 3008N Main Processor modules to control the three separate legs of the system shown in Figure 4-7. Each Main Processor module operates independently with no shared clocks, power regulators, or circuitry. Each module owns and controls one of the three signal processing legs in the system, and each contains two 32-bit processors. One of the 32-bit processors is a dedicated, leg-specific I/O and communication (IOCCOM) microprocessor that processes all communication with the system I/O modules and communication modules. The processors operate asynchronously, sharing information by means of dual-ported memory that is dedicated exclusively to this exchange of information. Communications are discussed further in Section 4.8.

The second 32-bit primary processor manages execution of the control program and all system diagnostics at the Main Processor module level. Between the primary processors is a dedicated dual port random access memory (DPRAM) allowing for direct memory access data exchanges.

The dual microprocessor architecture structure described above thus complies with Position 4 of DI&C ISG-04 [2] by executing the communications process separately from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function.

Specific Tricon Main Processor and System Bus PPS Replacement Project compliance with ISG-04 [2] is addressed in Sections 3.1 and 5.0 of the Triconex DCPP PPS ISG-04 Conformance Report [25]. The Tricon subsystem of the PPS replacement has been designed to an alternative to ISG-04 [2], Section 1, “Interdivisional Communications,” Position 10 that states, in part, provisions that rely on software to effect the disconnection of maintenance and monitoring equipment are not acceptable. The Tricon keyswitch relies on software to effect the disconnection of the TriStation capability to modify the safety system software. The use of the Tricon keyswitch is acceptable for the PPS replacement design since failure of the Tricon keyswitch will not prevent performance of the PPS safety function. This is discussed in more detail in Section 4.8.10.

The operating system, run-time library, and fault analysis for the Main Processor is fully contained in flash memory on each module. The Main Processors communicate with one another through the TriBUS proprietary, high speed, voting, bi-directional serial channel. Each Main Processor has an I/O channel for communicating with one of the three legs of each I/O module. Each Main Processor has an independent clock circuit and selection mechanism that enables all three Main Processors to synchronize their operations each scan to allow voting of data and exchange of diagnostic information.

Technical details regarding the Tricon Main Processor modules, including discussion of Control and IOCCOM processor architecture, communications, speed, internal memories, word width, and bus interface are provided in Section 2.1.2.6 of Tricon V10 Topical Report Submittal [13].

4.2.2.2 ALS Core Logic Boards

The ALS-102 Core Logic Board (CLB) is the primary decision making board in the ALS FPGA system, and contains all the application specific logic circuits that define and control the operation of a given system. The ALS-102 is based on a generic ALS board that is configured with application specific logic. The ALS-102: (1) controls all sequencing within the ALS system; (2) issues requests to input boards to provide field input information as required; (3) makes decisions based on received inputs; and (4) commands the output boards to drive a specific output state to the field devices without using a microprocessor. The Design Specification for the ALS-102 is provided in [94].

A portion of the FPGA logic in the ALS-102 is customized by CSI for the PPS replacement application based on the DCPP Conceptual Design Document (CDD) [27], FRS [28], Interface Requirements Specification (IRS) [29] and Controller Transfer Function Requirements Specification [120]. These documents specify the overall functionality requirements of the PPS replacement. From this design input, CSI develops the application-specific ALS-102 FPGA Requirements Specification [20] and from this specification CSI creates the detailed application specific logic specification for the ALS-102.

The CSI FPGA design process is described in Section 4.5 of this LAR.

4.2.3 I/O Modules

4.2.3.1 Triconex I/O Modules

As shown in Figure 4-7, Tricon TMR input modules contain three separate, independent processing systems, referred to as legs, for signal processing (Input Legs A, B, and C). The legs receive signals from common field input termination points. The microprocessor in each leg continually polls the input points, and constantly updates a private input data table in each leg's local memory. Signal conditioning, isolation, or processing required for each leg is also performed independently. The I/O modules provide three complete signal paths in each leg for all boards used in the PPS replacement, except the Enhanced Relay Output (ERO) Module 3636T, which is simplex (one signal processing path per channel), thus providing data isolation and independence so that a component failure in one leg does not affect the signal processing in the other two legs. The ERO module provides discrete outputs to non-safety-related systems such as the MAS, hence loss of the single leg does not affect a safety function and TMR capability is not required.

Input data is sampled, conditioned, and sent to the main processors. Each main processor communicates via an individual I/O bus with one of the triplicated microprocessors on each I/O module. In each main processor, the I/O bus microprocessor reads the data and provides it to the main processor through a DPRAM interface. For analog inputs, the three values of each point are compared, and the middle ("median") value is selected. The median selection process functions continuously without dead band or hysteresis. The control algorithm is invoked only on known good data. All input modules include self-diagnostic functions designed to detect single failures within the module.

After the main processors complete the control algorithm, data is sent to the output modules. Outputs from the main processors are provided to the I/O bus microprocessors through DPRAM. The use of DPRAM allows separation of the control and communications functions of the Main Processor to comply with Position 4 of DI&C ISG-04 [2]. The I/O bus microprocessors transfer that data to the triplicated microprocessors on the output modules. The output modules set the output hardware appropriately on each of the triplicated sections and vote on the appropriate state and/or verify correct operation. Discrete outputs use a unique, patented, power output voter circuit. This voter circuitry is based on parallel-series paths that pass power if the driver for legs A and B, or legs B and C, or legs A and C command them to close (i.e. 2-out-of-3 vote). Analog outputs use a switching arrangement tying the three legs of digital to analog converters to a single point. All output modules include self-diagnostic functions designed to detect single failures within the module.

The Triconex I/O modules listed in Table 4-6, voting processes, and fault detection processes are described in Section 2.1.2.7 of the Tricon V10 Topical Report Submittal [13].

The following Triconex I/O Module types are used in the PPS replacement and are described in Reference 2.5.30 of the Tricon V10 Topical Report Submittal [13].

Table 4-6 Triconex I/O Modules

MODULE TYPE	MODEL NO.	MODULE TYPE/DESCRIPTION
Analog Input	3703EN	Enhanced Analog Input Module, Isolated
	3721N	Next Generation Analog Input Module, -5-5 V Direct Current (DC)
Analog Output	3805HN	Analog Output Module, 4-20 mA
	3805E	Analog Output Module, 4-20 mA
Digital Input	3501TN2	Enhanced Digital Input Module, 115V AC/DC
	3503EN2	Enhanced Digital Input Module, 24V AC/DC
Digital Output	3601TN	Enhanced Digital Output Module, 115 V AC
	3601E	Enhanced Digital Output Module, 115V AC/DC
Relay Output	3636T	Enhanced Relay Output Module, N.O., Simplex

4.2.3.2 ALS Input Modules

The ALS Input Boards perform sensor sampling, signal conditioning, filtering and analog-to-digital conversion of field input signals. Input Boards perform specific input functions, such as 24V or 48V digital contact sensing, 4-20 mA analog inputs, 0-10V analog inputs, resistance temperature detector (RTD) inputs, or thermocouple (TC) inputs.

The ALS input boards provide self-test capability that continuously verifies vital components within the channel are operational. Isolation between the channels and the ALS logic is maintained by utilizing galvanic isolators. The input channels are protected against electrostatic discharge (ESD) and surge voltages using transient voltage suppressors (TVS). Opto-isolator circuits are designed to maximize the life expectancy of the device. The input boards provide front panel light-emitting diode (LED) indicators which show the status of a particular input signal. Generally, all input channels are galvanically isolated from the ALS logic and the barriers can withstand more than 1500 Vrms difference between the field domain and the digital domain.

ALS Input Board scaling, range and calibration are configured during the system level design for the PPS replacement application.

The ALS Input Boards used in the PPS replacement are listed in Table 4-7 and described in Section 2.2 of the ALS Topical Report Submittal [15]. The design specifications listed in Table 4-7 describe input board fault detection, configuration and data validation processes.

4.2.3.3 ALS Output Modules

The ALS Output Boards provide signals to control field devices such as actuators, indicators, and relays. The ALS output boards used in the PPS replacement are listed in Table 4-7 and described in Section 2.2 of the ALS Topical Report Submittal [15].

The output channels on the ALS output boards are based on isolated solid-state devices, similar to the input channels. Output channels include self-test capability and other specialized test functions to ensure the channel is operational. The output channels are protected against ESD and surge voltages. The output boards provide front panel LED indicators that show the status of a specific output.

All output boards have galvanic isolation between the channels and the ALS logic, and can withstand a minimum of 1500 Vrms. Depending on the board type, the output boards can have individually isolated channels, or they can be located on a common isolation domain.

Digital output channels in the PPS replacement are configured in the Output Board non-volatile RAM to drive the output to a predefined state in case of board failure or lack of communication with the ALS-102. These predefined states are Open, Closed or As Is. The predefined states are determined as part of the system level design of the PPS replacement application.

The output modules, fault detection, configuration and data validation processes are described in Section 2.2 of the ALS Topical Report Submittal [15]. The design specifications listed in Table 4-7 describe input board fault detection, configuration and data validation processes.

Table 4-7 ALS I/O Modules

Type	Description	Function	Design Specification
ALS-302	Digital Input Board	32 Channel 48 V DC Contact Input	6002-30202 [106]
ALS-311	Analog Input Board	8 Channel RTD/TC Input	6002-31102 [107]
ALS-321	Analog Input Board	8 Channel Voltage/Current Input	6002-32102 [108]
ALS-402	Digital Output Board	16 Channel Contact Output	6002-40202 [109]
ALS-421	Analog Output Board	8Channel Voltage/Current Output	6002-42102 [110]

4.2.4 Communications Modules or Means

4.2.4.1 Triconex Communications Modules

The TCM have three separate communication busses and three separate communication bus interfaces, one for each of the three main processors. The three communication bus interfaces are merged into a single microprocessor. That microprocessor votes on the communications messages from the three main processors and transfers only one of them to an attached device or external system. If two-way communications are enabled, messages received from the attached device are triplicated and provided to the three main processors.

The communication paths to external systems utilize Cyclic Redundancy Checks (CRC), handshaking, and other protocol-based functions to ensure data communication integrity. These functions are supported in hardware and firmware. Firmware provides core functionality common to all the communication modules with additional coding to support the specific communication protocol.

The TCM allows the Tricon to communicate with other Tricons and with external hosts over fiber optic networks. The TCM provides two fiber optic port connectors labeled Net 1 and Net 2, which support Peer-to-Peer (P2P), time synchronization, and open networking to external systems. In addition, the TCM contains four serial ports allowing the Tricon to communicate with Modbus master and slaves.

Reference 2.5.35 [24] in the Tricon V10 Topical Report Submittal [13] describes the Tricon V10 conformance to ISG-04 [2]. The TCM handles all communications with external devices, and it has been qualified under the IOM Appendix B program for nuclear applications. Upon total loss of all TCMs, the main processors continue to function.

Specific PPS Replacement Project TCM compliance with ISG-04 is addressed in Section 4.1 and 5.0 of the Triconex DCPP PPS ISG-04 Conformance Report [25].

4.2.4.2 Triconex RXMs

The RXMs are single-mode fiber optic modules that allow expansion chasses to be located several kilometers away from the main chassis. An RXM connection consists of three identical modules, serving as repeaters/extenders of the Tricon I/O bus, and which also provide ground loop isolation. Refer to Figure 4-5.

Each RXM module has single channel transmit and receive cabling ports. Each of the three primary RXM modules is connected to the remote RXM modules housed in the remote chassis. Each pair of RXM modules is connected with two fiber optic cables operating at a communication rate of 375 KBaud. The interfacing cabling is unidirectional for each channel. One cable carries data transmitted from the primary

RXM to the remote RXM. The second cable carries data received by the primary RXM from the remote RXM. The RXM modules provide immunity against electrostatic and electromagnetic interference. Since the RXM modules are connected with fiber optic cables, they may be used as 1E-to-non 1E isolators between a safety-related main chassis and a non-safety-related expansion chassis. This isolation capability is utilized in the PPS Replacement Project for one-way non-safety-related outputs to external systems such as the MAS.

The RXM are described in Section 2.1.2.3 of the Tricon V10 Topical Report Submittal [13].

Specific PPS replacement Remote RXM compliance with ISG-04 [2] is addressed in Section 4.2 and 5.0 of the Triconex DCPP PPS ISG-04 Conformance Report [25].

4.2.4.3 ALS Communications Modules

The PPS replacement application does not utilize the ALS-601 Communications Board described in the ALS Topical Report Submittal [15]. Two (2) independent, dedicated, serial, transmit-only (no handshake) EIA-422 communication channels (TxB1 and TxB2) provided by the ALS-102 provides information to external systems [Figure 4-6]. RS-422 is the common short form title of American National Standards Institute (ANSI) standard ANSI/TIA/EIA-422-B, "Electrical Characteristics of Balanced Voltage Differential Interface Circuits." This technical standard specifies the electrical characteristics of the balanced voltage digital interface circuit. As used in this LAR, EIA-422 and RS-422 are equivalent and used interchangeably. The ALS-102 transmits application specific input and output states and values continuously to the MWS (which performs the function of the ASU via the one-way RS-422 communication channel TxB2 on the ALS-102. The second, one-way RS-422 communications channel TxB1 on the ALS-102 transmits application specific input and output states and values continuously to the non-safety PDN Gateway Switch that connects to the PDN Gateway Computer.

4.2.5 Voters

The PPS monitors plant parameters, compares them against setpoints and provides signals to the SSPS if operating limits are exceeded. The SSPS evaluates the signals and performs coincident logic functions at the RTS and ESFAS levels to mitigate the event that is in progress. This voting takes place among the four Protection Sets and is outside the scope of the PPS replacement, because the SSPS is not being replaced by this change.

The PPS subsystems also perform internal voting functions, as described below.

4.2.5.1 Triconex Voting

At the beginning of each scan, each main processor within a given Protection Set takes a snapshot of the input data table in DPRAM, and transmits the snapshots to the other main processor modules over the TriBUS described in Section 4.2.2.1 . Each processor module independently forms a voted input table based on respective input data points across the three snapshot data tables. If a main processor module receives corrupted data or loses communication with one of the other two processors in the same Protection Set, the local table representing that respective leg data defaults to the de-energized state. The voting scheme is designed for de-energize to trip applications, always defaulting to the de-energized state unless voted otherwise.

For digital inputs, the voted input table is formed by a 2-out–of-3 majority vote on respective inputs across the three data tables for each main processor within the same Protection Set. As above, the voting scheme is designed for de-energize to trip applications, and defaults to the de-energized state unless voted otherwise. Any single leg failure or corrupted signal feeding a main processor module is corrected or compensated at the main processor module level when the voted data table is formed.

For analog inputs, a mid-value selection algorithm chooses an analog input signal representation in the voted input table. The algorithm selects the median of the three signal values representing a particular input point for representation in the voted input tables. The median selection process takes place continuously and does not require configuration of dead band or hysteresis for operation. Any single leg failure or corrupted signal feeding a main processor module is compensated for at the main processor module level when the voted data table is formed. Significant errors between legs are alarmed. Refer to Section 2.1.2.6 of the Tricon V10 Topical Report Submittal [13] for additional information.

The main processors then execute the application program in parallel on the voted input table data and produce an output table of values in DPRAM. The voting schemes explained above for analog and digital input data ensure that the process control programs are executed on the same input data value representations. The IOCCOM processors generate output tables, each corresponding to an individual output module in the system. Each output table is transmitted to the appropriate leg of the corresponding output module over the I/O data bus.

The Triconex voting methodology is described in Sections 2.1.2.6 (Main Processor), 2.1.2.7 (I/O Modules), and 2.1.2.8 (TCM) of the Tricon V10 Topical Report Submittal [13].

4.2.5.2 ALS Voting

The ALS subsystem in each Protection Set in the PPS replacement provides two complete and diverse execution paths “A” and “B” comprised of the ALS-102 CLBs, input boards and output boards shown in Figure 4-9.

Section 2.2 of the ALS Diversity Analysis [16] describes the internal logic within an ALS FPGA, called the FPGA image, which consists of two redundant cores each containing all the logic necessary to perform the function of the ALS-102. The two cores independently perform the same function with an independent redundancy checker verifying the results. The redundancy checker compares all outputs and critical internal states from the two cores and will drive the board to a safe state if the outputs of the two cores do not agree. The redundancy multiplexer provides an additional diversity safety layer by performing simple voting on key outputs from the two cores to ensure that the desired outputs are generated if the two cores do not agree. This provides internal, or Core, diversity within an individual ALS-102.

Core Diversity is implemented for each of the FPGAs on all of the ALS boards to ensure there is sufficient diversity for simple applications. An additional level of design diversity is incorporated for more complex applications, such as the PPS replacement, which receives sensor signals and makes trip or actuation determinations. This additional level of diversity is called Embedded Design Diversity, and provides diverse “A” and “B” execution paths.

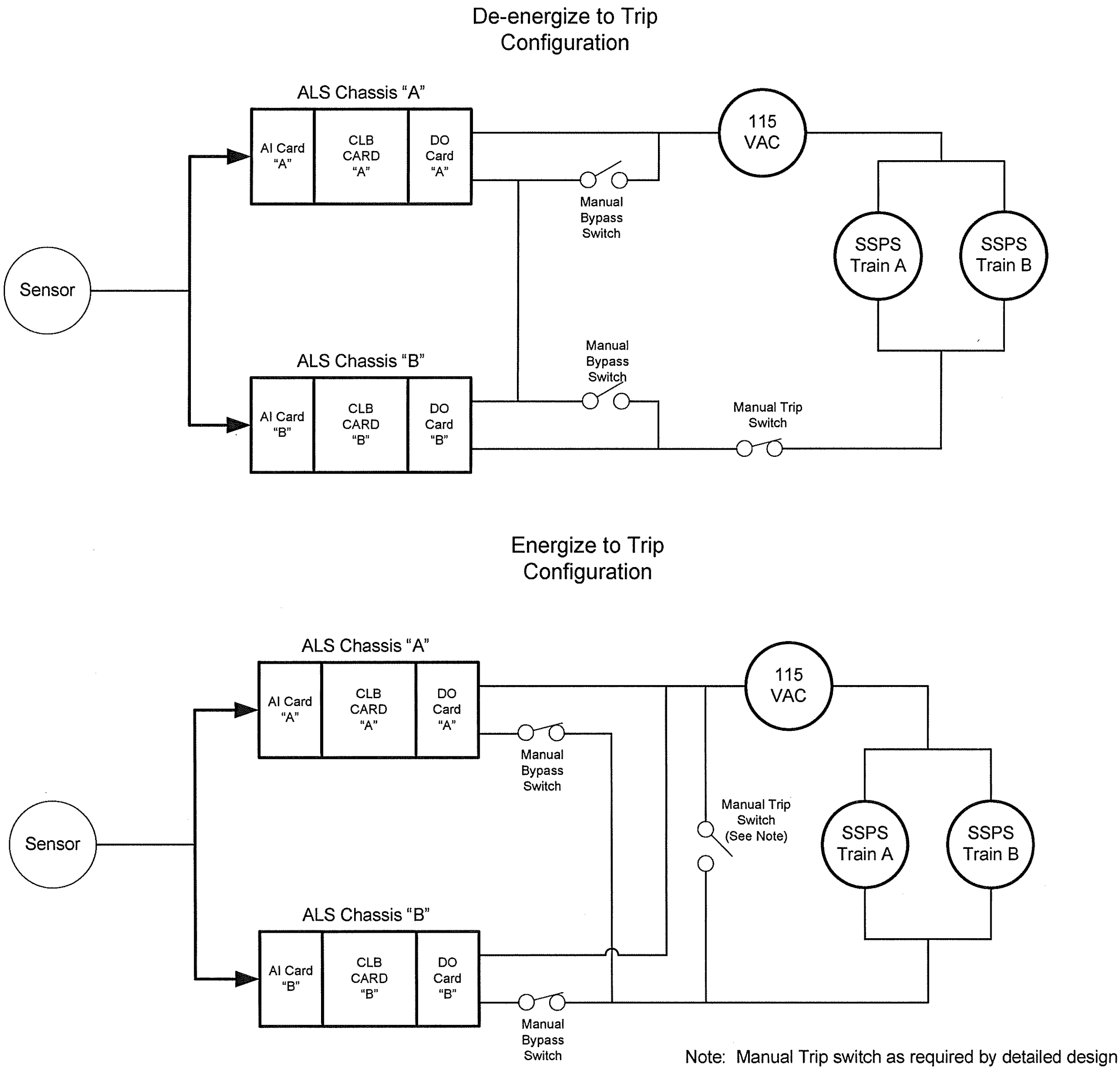
The diverse “A” and “B” execution path outputs are combined in hardwired logic as shown in Figure 4-9 to ensure that the protective action is taken if directed by either path. A single failed path cannot prevent a protective action. Either ALS-102 identifies itself as failed and sets its outputs to a fail-safe state before halting operation if it detects a mismatch between the outputs of its diverse logic cores.

The ALS-A and ALS-B voting arrangement is described in the ALS System Design Specification [19], Section 2.

Both logic cores within a diverse execution path have the same interface with field inputs and outputs and the TAB. It is not possible to bypass one core (i.e., “A1”) without bypassing the other core (i.e., “A2”) at the same time.

Figure 4-9 also illustrates the ALS manual trip and bypass switches discussed in Section 5.11.1.3.2 of this LAR.

Figure 4-9 ALS Diversity Architecture



De-energize to Trip Configuration

Energize to Trip Configuration

Note: Manual Trip switch as required by detailed design

4.2.6 Manual Channel Trip and Reset

The existing DCPP protection system design includes manual displays and controls in the control room for manual actuation and management of plant critical safety functions. Where necessary and practical, the indications are derived from the raw sensor signal and the indications are not processed by any digital system. The available displays and controls are listed in Table 3-5 and Table 3-6 of the approved DCPP D3 analysis [7] and include but are not limited to the following:

1. Reactivity Control

   RT may be initiated at any time by controls that are independent of the PPS. Independent indication of rod position is provided as well. The NIS provides Class IE protection functions indication of neutron flux diverse from the PPS as discussed in the PPS Replacement D3 Assessment [7].
2. Reactor Core Cooling and Heat Removal

   AFW may be initiated manually and monitored by controls that are independent of the PPS.
3. RCS Integrity

   SI may be initiated manually and monitored by controls that are independent of the PPS.
4. Containment Isolation and Integrity

   Containment Spray, Containment Isolation and CVI may be initiated manually and monitored by controls that are independent of the PPS.

The system level manual trip and actuation functions described above are hardwired and are not affected by the PPS replacement. Once initiated, protective actions run to completion. Reset of the protective action must be initiated manually after the initiating cause is no longer present.

4.2.7 Power Supply

The PPS is supplied vital uninterruptible AC power from four electrically independent and physically separated 120 V AC distribution panels. Each distribution panel is supplied from a separate, dedicated inverter and from a backup common 480 V AC vital bus. An inverter can be fed from the 125 V DC vital system or from the 480 V AC vital system. The 125 V DC system is designed with three vital batteries, with each battery having a dedicated charger supplied from a 480 V AC vital bus.

Protection Set	Vital Inst AC Bus
I	PY-11 (21)
II	PY-12 (22)
III	PY-13 (23)
IV	PY-14 (24)

Each 480 V AC vital bus is designed to be supplied from the main generator, from the two independent offsite sources and from the onsite diesel generators. Safety-related 480 volts AC from vital AC motor control center (MCC) is fed to an uniterruptible power supply and rectified. Rectifier output is fed to the inverter and converted to 120 V AC.

Safety related vital DC bus power is fed to an uninterruptible power supply as immediate backup supply. The vital DC bus is backed up by the safety-related 125 vital DC station battery, which is charged from vital 480 V AC. Inverter output is fed through a static switch with integral manual bypass switch to vital instrument AC power distribution panels. On loss of inverter output, the static switch will select backup regulating transformer output (120 V AC) to the distribution panels. The backup regulating transformer receives input from the 480 V AC supply. The backup regulating transformer may be aligned via a transfer switch to either of two 480 V AC busses; the normal supply or an alternate supply. The alternate supply circuit breaker is normally open to prevent interconnection of redundant power supplies due to a failed transfer switch. The transfer switch may not be used under load.

PG&E practices power supply quality monitoring per the guidance of NRC RG 1.180 [23] As-found and as-left Total Harmonic Distortion measurements will be performed at PPS 120 V AC power supply input terminals before and after installation of equipment powered from the 120 V AC vital instrument power supply. If needed, corrective measures will be implemented during installation.

4.2.7.1 Triconex Power Supply Modules

The Triconex PPS subsystem utilizes two Triconex power supply modules in each chassis. The power supply modules have been qualified by Triconex per the Tricon V10 Topical Report Submittal [13] and operate from the redundant uninterruptible 120 V AC safety-related instrument power supply used to power the existing Eagle 21 PPS. Power supplies in non-safety-related chasses are isolated from the safety-related primary power source by qualified circuit breakers or fuses.

All power supply modules are rated for 175 watts, which is sufficient to supply the power requirements of a fully populated chassis. Two different power supply modules can be used in a single chassis. The PPS replacement utilizes 120 V AC modules.

The power supply modules possess built in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator LEDs on the front face of each power module provide module status. The power supply modules also contain the system alarm contacts. The chassis backplane provides terminal strip interfaces for power and alarm connections. The alarm function operates independently for each power module. An AC line filter reduces incoming noise and suppresses conducted emissions and conducted susceptibility.

The alarm contacts on at least one of the chassis power supplies actuate when the following power conditions exist:

- A power module fails

- Primary power to a power module is lost
- Power module has a low battery or over temperature condition

The alarm contacts on both power modules of an expansion chassis actuate when a fault is detected on an I/O module.

The alarm contacts on both power supply modules in the main chassis actuate when system trouble such as a processor or I/O module fault is detected. The alarm contacts on both power modules of an expansion chassis actuate when a fault is detected on an I/O module. The alarm contacts on individual power supply modules actuate when trouble is detected within the module or if primary power is lost.

Each of the three legs on each I/O module and each Main Processor module normally draws power from both power supplies through the dual power rails and the dual power regulators. If one of the power supplies or its supporting power line fails, the other power supply increases its power output to support the requirements of all modules in the chassis.

The Triconex power supply modules are described in Section 2.1.2.5 of the Tricon V10 Topical Report Submittal [13].

4.2.7.2 FPGA-Based ALS Logic Power Supplies

The power supply system in each ALS safety system cabinet is comprised of two qualified, independent AC/DC power supplies. Each power supply is designed to provide 150 percent of the cabinet load, and operates in a redundant configuration. The power supplies are mounted in the same cabinet as the ALS chassis. Each ALS PPS subsystem chassis is powered via the Backplane Assembly from an external dual-redundant power supply system. The cabinet load consists of all ALS platform components and peripheral devices. Input/Output power is provided by separate power supplies as discussed below. Power supply failures (loss of output voltage) are alarmed. The ALS-A and ALS-B subchannels are supplied by the same 48 V DC power supplies (typical for each Protection Set).

Inside the PPS cabinet, an AC line filter reduces incoming noise and suppresses conducted emissions and conducted susceptibility. In addition to the power supplies and AC line filter the power distribution system consists of breakers and terminal blocks as necessary.

The individual 48 V DC chassis power supplies supplied by PG&E are redundant, hot swappable, and capable of being replaced while the system is operational without interruption of power to the ALS chassis or other safety system components. The 48 V DC from the redundant cabinet power supplies is fed to the ALS chassis, where they are diode auctioneered to provide a single local 48 V DC supply. Each ALS board contains DC/DC converters that generate stable local board power. All ALS boards are fused, filtered and over-voltage protected on the incoming cabinet 48 V DC supply voltage. The fuse ensures that local failures on an ALS board cannot disrupt the chassis power. The filtering prevents electrical noise propagation from the ALS backplane to the board itself and also prevents noise propagating from the ALS board to the ALS backplane.

The ALS power supply and distribution within the ALS chasses is described in Section 2.6.2 of the ALS Topical Report Submittal [15] and in Section 4.2.1 of the ALS Platform Specification [95].

4.2.7.3 Analog Input Power Supplies – Analog Inputs

The Tricon and the ALS subsystem in each Protection Set are provided with its own pair of safety-related adjustable redundant loop power supplies capable of powering all 4-20 mA instrument input loops associated with that subsystem. Operating voltage will be selected during detailed design to power instrument loops without exceeding voltage limitations of instrument loop sensors (transmitters). Separate I/O power supplies are provided and qualified by PG&E during detailed design for the Triconex and ALS subsystems.

4.2.7.4 Triconex Discrete I/O Power Supplies

De-energize to trip discrete Triconex outputs to the SSPS and auxiliary relays utilize the 120 V AC safety-related PPS instrument power supply. Energize to trip discrete Triconex outputs to the SSPS and auxiliary relays are powered by safety-related redundant 24 V DC power supplies. Other discrete Triconex outputs are powered by the external system.

Triconex discrete inputs are powered by redundant 24 V DC power supplies, except trip output loopback signals, which are powered by the 120 V AC discrete output (DO) [Figure 4-10]. Triconex analog 4-20 mA output loops are powered by redundant 24 V DC power supplies. The Triconex qualification requires that separate power supplies be used for analog and digital I/O.

4.2.7.5 ALS I/O Power Supplies

All discrete ALS outputs to the SSPS are powered by safety-related 120 V AC Protection Set power. Other discrete ALS outputs such as output signals to the MAS are powered by the external system. Discrete ALS inputs are powered by safety-related redundant 48 V DC power supplies. Analog ALS 4-20 mA outputs are powered by the ALS internal power supply. The feedback signals shown in Figure 4-9 are powered by the redundant, safety-related 48 V DC discrete input power supply.

Failure of any Tricon or ALS I/O power supply is alarmed on the control room MAS.

4.2.8 Test Subsystem

The PPS replacement permits any individual instrument channel to be maintained and calibrated in a bypassed condition, and when required, tested during power operation without initiating a protective action at the system level. This is accomplished without lifting electrical leads or installing temporary jumpers. The PPS replacement permits periodic testing during reactor power operation without initiating a protective action from the channel under test.

External hardwired switches are provided on all PPS replacement trip and actuation outputs. The switches may be used for SSPS input relay testing or to trip or actuate the channel manually if needed. Activation of the external trip switches is indicated in the control room through the SSPS partial trip indicators. Actuation of bypass switches (ALS) and out of service switches (Tricon) is indicated through the MAS.

Refer to Section 4.11.3.2 for test and bypass design details.

4.2.8.1 Tricon-Based PPS Equipment

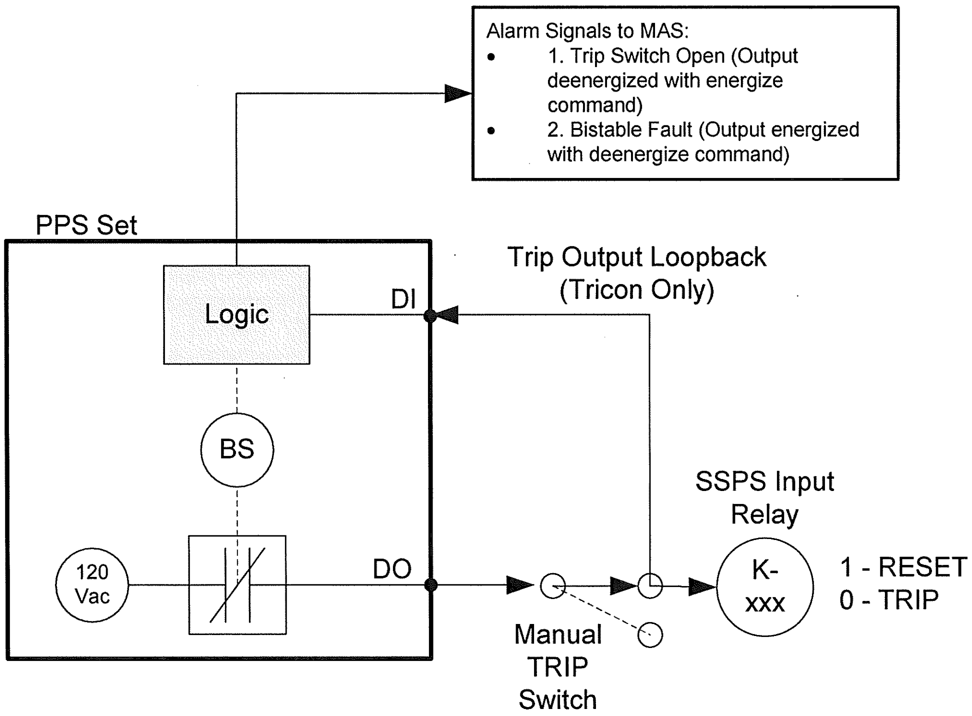
The Triconex portion of the PPS replacement continuously performs diagnostic functions as described in the Tricon V10 Topical Report Submittal [13]. The diagnostic functions within the main processor module monitor the status of each main processor as well as each I/O module and communication channel. The main processor modules process diagnostic information recorded within the main processor module and diagnostic information received from the diagnostics functions within the I/O module in order to make decisions about the health of the I/O modules in the system. All discrepancies are flagged and used by the built in fault analyzer routine to diagnose faults.

When a fault is detected on a main processor module, it is annunciated and voted out, and processing continues through the remaining two main processor modules. When the faulty main processor module is replaced, it runs a self-diagnostic to determine its basic health. When the self-diagnostic is successfully completed, the newly inserted main processor module then begins the process of "re-education" where the control program is transferred from each of the working units into the newly inserted main processor module. All three main processor modules then resynchronize data and voting, and the newly inserted main processor module is allowed back in service.

If one of the three legs within an I/O module fails to function, an alarm is raised to the main processor modules. If a standby I/O module is installed in the paired slot with the faulty I/O module, and standby I/O module is deemed healthy by the main processors, the system automatically switches over to the standby I/O module and takes the faulty I/O module off line. If no standby I/O module is in place, the faulty I/O module continues to operate on two of the three legs and protection and control is unaffected. The maintenance technician obtains a replacement I/O module and inserts it into the system at the logically paired slot associated with the failed I/O module. When the main processor modules detect the presence of a newly inserted I/O module, they initiate local health state diagnostics and, if the newly inserted I/O module is healthy, automatically switch over to the new I/O module. The faulty I/O module may then be removed and returned to the factory for repair.

Specific PPS replacement test and calibration functions and application diagnostics are supported by the platform but implemented in the application program. An example of such a diagnostic is a mismatch check that compares the trip demand from the PPS to a feedback signal. A mismatch occurs if the trip demand signal does not agree with the feedback signal, as shown in Figure 4-10:

Figure 4-10 Triconex Trip Output Diagnostic



Triconex self-test methodology is described in Sections 2.1.2.6 (Main Processor module), 2.1.2.7 (I/O Modules), and 2.1.2.8 (TCM) of the Tricon V10 Topical Report Submittal [13].

Specific testing provisions implemented in the PPS Triconex Software Application Program (TSAP) for compliance with 10 CFR 50 requirements, including IEEE 603 [21] and IEEE 7-4.3.2 [80] are discussed in later sections of this LAR.

4.2.8.2 FPGA-Based ALS PPS Equipment

The ALS platform incorporates self-diagnostic functions that provide a means to detect and alarm all significant failure(s) within the platform. Details of the ALS Board self-diagnostic functions are described in the design specification listed in Table 4-7 associated with each board. Additional ALS platform fault detection and self-diagnostics information is provided in the ALS Platform Specification [95].

The ALS platform is designed to support the elimination of manual periodic surveillance testing of an installed ALS safety system. In typical safety system applications the ALS platform is operating at steady state where it is monitoring plant conditions to initiate RT or ESF actuations. To verify operability, it is necessary to test these static commands on a regular basis. Historically this has been done with periodic surveillance testing which involves plant personnel placing the system into a bypassed or partial tripped state and then testing the critical functions. The ALS platform provides that facilitate extending the intervals for periodic surveillance testing. This can be done through a combination of redundancy and self-testing which automatically and transparently verifies critical system functions.

The ALS Platform uses a combination of implementation and test strategies in order to maintain its high integrity status. The four primary implementation and test strategies are described below. The testing is performed automatically by the ALS system without the need for interaction by plant personnel.

Redundancy All ALS FPGAs are implemented with redundant digital logic. This is to protect the ALS board against a type of failure which can potentially occur over time as a result of manufacturing defects, radiation damage or flash cell charge degradation. This section exclusively focuses on how the redundancy is implemented internal to the ALS FPGAs. Other levels of redundancy such as the redundant input or outputs, or application level redundancy are not covered in this section. Differences between the redundant circuits cause the ALS to take appropriate action. The redundancy implementation detects any deviation between the redundant circuits before a possible erroneous signal can propagate to the remainder of the system.

Diversity The diversity between the redundant logic modules has been achieved as a result of changing the Finite State Machine (FSM) encoding style and the module hierarchy between the two cores.

BIST The Built-In-Self-Test (BIST) is used for exercising all critical functions within a board. This is done to ensure that latent failures cannot build up in the system and make the system inoperable without the knowledge of plant personnel. The BIST typically applies input stimuli on the inputs to a sub-circuit and validates the correct response on the output.

Inherent Self-Test Inherent Self-Test is a method for implementing high integrity directly into the logic circuits by constructing it in a way that latent STUCK-AT or OPEN failures are instantly detected. An example of inherent self-testing is a serial communications link with CRC protection.

The ALS Platform self-test strategy is based on the following steps:

Detect The ALS Platform detects failures in its circuits or connected field devices either by running nonintrusive background tests on a regular interval, or by redundancy.

Mitigate The circuits causing the failure are isolated before the failure is allowed to propagate to other systems.

Announce The detected failure is announced using the ALS rack alarm which typically ties into a master control board alarm. Other application specific indicators may also be added to the system to give a more detailed status indication to the control room, such as indicating in which function the failure occurred and to show if the system remains operable.

React The failure is announced using the system alarm and by other application specific means. The ALS system is designed so a failure in a sub-circuit causes the system to enter a specific state, such as a partial trip or bypass. A critical function is the system's ability to drive its output channels to a predefined state when a specified set of inputs events occur, such as digital inputs being activated or analog input going beyond a threshold.

The ALS self-test functions are described in Section 3.0 of the ALS Topical Report Submittal [15].

4.2.9 Other Subsystems – Tricon MWS and ALS MWS

Each Protection Set in the PPS replacement is provided with a separate dedicated non-safety-related MWS for the Tricon subsystem and the ALS subsystem for the purpose of maintenance and calibration. The Tricon MWS and ALS MWS within a redundant Protection Set are connected to and communicate with the safety-related equipment in the associated Protection Set. The Tricon and ALS MWSs are not connected to and cannot communicate with safety-related equipment outside its associated Protection Set. Refer to Figure 4-12.

The two non-safety related MWSs in each Protection Set share common KVM and touchscreen equipment via a KVM switch as shown in Figure 4-2 and Figure 3-3. The Tricon MWS is dedicated to the Tricon PPS subsystem in the respective set; the ALS MWS is dedicated to the ALS PPS subsystem in that set. The two MWSs cannot communicate with each other nor can they communicate with the MWSs in redundant protection sets.

A MWS may access data only within its own Protection Set. Communication of any MWS with any other Protection Sets is not possible. There are no means of connecting any Protection Set to another MWS without reconfiguring the Protection Set controllers and communications cabling.

The non-safety-related Tricon MWS is used to mantain and configure the Tricon and also to view data from Tricon.

The Tricon MWS is connected to the Tricon PPS subsystem in read-only mode, except during testing and calibration, when two-way communication between the Tricon MWS and safety-related processors is required to perform the test or calibration function. The Tricon MWS is able to read, but not write, process instrumentation information for local display at the Tricon MWS during normal operation.

Using the MWS, the PPS replacement permits any individual instrument channel to be maintained in a bypassed condition, and when required, tested during power operation without initiating a protective action at the system level, and without lifting electrical leads or installing temporary jumpers.

On-line testing in the Tricon is controlled by the non-safety-related MWS and by safety related logic enabled via an external safety-related hardwired out of service switch. When the out of service switch is activated, the safety-related logic in the associated Protection Set allows the associated instrument channel to be taken out of service while maintaining the rest of the instrument channels in the Protection Set operable. The individual out of service switch only removes an individual instrument channel from service and no other instrument channel. If the out of service switch is returned to the normal position during test, the safety-related logic automatically restores the instrument channel to safety-related operation.

The non-safety ALS MWS is used to maintain and configure the ALS subsystem and also to view data from ALS subsystem. On-line testing in the ALS is controlled by the TAB as described in Section 2.3.2 of the ALS Topical Report Submittal [15]. The two-way connection between the ALS MWS and the ALS PPS is normally physically disconnected from the ALS subsystem. When on-line testing of the ALS subsystem is required, the non-safety-related ALS MWS is physically connected to the TAB and the TAB is placed in service allowing two-way communications between the ALS MWS and the ALS subsystem under bypass conditions as described in Section 5.3.3 of the ALS Topical Report Submittal [15].

Refer to Section 4.11.1.3.2 for discussion of Design for Test and Calibration.

4.2.10 Cabinets, Racks, and Mounting Hardware

The PPS is housed in existing process instrumentation cabinets numbered 1 through 16 (DCPP Electrical Location Numbers RNP1A, RNP1B, RNP1C, RNP1D, RNP1E, RNP2A, RNP2B, RNP2C, RNP2D, RNP2E, RNP3A, RNP3B, RNP3C, RNP4A, RNP4B, RNP4C) [Figure 4-11].

The cabinets provide the same degree of physical separation and electrical isolation between Protection Sets as the previously approved Eagle 21 PPS [5]. The cabinets will be evaluated for seismic considerations as part of the detailed PPS replacement design. Non-safety-related hardware mounted in the PPS cabinets will be evaluated for seismic interactions during the detailed design.

Protection set cabinet assignments are as follows:

Table 4-8 Protection Set Assignments

Protection Set	Cabinet	Electrical Location
I	1	RNP1A
	2	RNP1B
	3	RNP1C
	4	RNP1D
	5	RNP1E
II	6	RNP2A
	7	RNP2B
	8	RNP2C
	9	RNP2D
	10	RNP2E
III	11	RNP3A
	12	RNP3B
	13	RNP3C
IV	14	RNP4A
	15	RNP4B
	16	RNP4C

Figure 4-11 PPS Rack Locations

The PPS rack locations is security-related information per 10 CFR 2.390 [88] and were submitted to the NRC staff in PG&E Letter DCL-11-123, dated December 20, 2011 [164].

Parameters monitored by each Protection Set are shown in the following table:

Table 4-9 Protection Set Input Parameters

PARAMETER	PROTECTION SET
Rx Coolant Flow, Loops 1, 2, 3, 4	I, II, III
Wide Range Rx Coolant Temperature (hot and cold legs), Loops 1, 2	I
Wide Range Rx Coolant Temperature (hot and cold legs), Loops 3, 4	II
Wide Range Rx Coolant Pressure, Loop 3	IV
Wide Range Rx Coolant Pressure, Loop 4	III
Narrow Range Rx Coolant Temperature (hot and cold legs), Loop 1	I
Narrow Range Rx Coolant Temperature (hot and cold legs), Loop 2	II
Narrow Range Rx Coolant Temperature (hot and cold legs), Loop 3	III
Narrow Range Rx Coolant Temperature (hot and cold legs), Loop 4	IV
Neutron Flux (from Nuclear Instrument System)	I, II, III, IV
Pressurizer Level	I, II, III
Pressurizer Pressure	I, II, III, IV
Pressurizer Vapor Temperature	IV
Steamflow, Steamline Pressure, S/Gs 1, 2, 3, 4	I, II
Steamline Pressure, S/Gs 2, 3	III
Steamline Pressure, S/Gs 1, 4	IV
S/G Narrow Range Level, S/Gs 1, 2, 3, 4	III, IV
S/G Narrow Range Level, S/Gs 2, 3	I
S/G Narrow Range Level, S/Gs 1, 4	II
Turbine Impulse Chamber Pressure	I, II
Containment Pressure	I, II, III, IV

Each of the Protection Sets contains the following equipment that is dedicated to the specific Protection Set. There is no communication between the Protection Sets and no equipment is shared between Protection Sets, except for the PDN Gateway Switch, which is isolated from the Protection Sets via fiber-optic cable and a NetOptics port aggregator network tap for each Protection Set as described in Section 4.2.13.1 of this LAR. Tricon TCM cards provide functional isolation as described in Section 4.15.1 of this LAR.

The PPS replacement effectively consolidates the functions performed by the PPS such that more protective functions are implemented in fewer processors. The effects of this consolidation will be discussed in the system-level Phase 2 PPS replacement Failure Modes and Effects Analysis (FMEA).

a) Safety-Related Triconex Subsystem

Physical details of the Triconex PPS subsystem are provided in Section 2.1.2 of the Triconex Submittal [13].

b) Safety-Related ALS PPS Subsystem

Physical details of the ALS are provided in the ALS Topical Report Submittal [15], the ALS Platform Requirements Specification [68], and the ALS Platform Specification [95].

c) Non-safety-Related MWS

The non-safety-related Tricon MWS and ALS MWS is provided by PG&E and is described in Section 4.2.9 of this LAR.

4.2.11 Appendix B Compliance Section (D.2.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.3 states:

Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance (QA) program (See American Society of Mechanical Engineers (ASME) NQA-1 -1989).

This section describes compliance with IEEE 603-1991 [21], Section 5.3. The following subsections describe the PG&E, IOM and CSI QA Programs, and how each applies to the PPS Replacement Project.

Compliance with IEEE Standard 7-4.3.2-2003 [80], "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3 "Quality," is described below and in Section 4.11.1.1.

4.2.11.1 PG&E QA Program

PG&E maintains full responsibility for assuring that its nuclear power plants are designed, constructed, tested and operated in conformance with accepted engineering practices, applicable regulatory requirements and specified design bases and in a manner to protect the public health and safety. To this end PG&E has established and implemented a quality assurance program (QAP) [142], which conforms to the criteria established in 10 CFR, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power, Plants and Fuel Reprocessing Plants" [151]. The PG&E QAP [142] is contained in DCPP FSAR [26] Chapter 17, "Quality Assurance," and complies with Revision 1 of RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants - LWR Edition" [152] and subsequent NRC guidelines.

DCPP FSAR Chapter 17 [142] describes the QA requirements for those systems, components, items, and services which have been determined to be nuclear safety related (Design Class 1). PG&E's QAP [142] also provides a method of applying a graded QAP to certain non-safety related systems, components, items, and services.

The quality of systems, components, items, and services within the scope of the PG&E QAP is assured commensurate with the systems, components, items, or services importance to safety.

The affected RTS/ESFAS and associated components within the scope of this LAR are classified in accordance with the QAP [142]. Those systems and components that perform an active safety function are classified as Design Class I. Design Class I covers those systems "and their attendant components, items, and services which have been determined to be nuclear safety related."

Procedures and work instructions necessary to implement the requirements of the QAP [142] are developed and approved by the organization responsible for the activity. These procedures and instructions may be contained in manuals, station procedures and directives, administrative instructions and/or other documents. These documents identify the criteria to determine acceptable quality for the activity being performed. On-site implementation of procedures and work instructions is the responsibility of the Site Vice President.

In support of the oversight activities for the PPS Replacement Project, PG&E has developed a project specific "Quality Assurance Plan for the Diablo Canyon Process Protection System Replacement" that defines the oversight activities to be performed by the PG&E Quality Verification group for the project which in part supports meeting 10 CFR 50, Appendix B, including technical audits, cyber security audits, and software quality assurance audits. The "Quality Assurance Plan for the Diablo Canyon Process Protection System Replacement" was submitted to the NRC in Attachment 1 to the Enclosure of PG&E Letter DCL-12-069 [160]. The "Quality Assurance Plan for the Diablo Canyon Process Protection System Replacement" requires audit reports and an Audit Summary Report to be created.

The following sections describe the primary manuals, procedures and directives, by project phase, used in the course of the PPS Replacement Project.

4.2.11.1.1 Design Phase

The design phase is performed within the context of the plant engineering change program, governed by department directives and design change program directives. PG&E contracted with IOM and CSI to perform the I&C hardware and software portion of engineering change activities, following the PG&E owner requirements provided in [27], [28], and [29], and the individual PG&E contracts with each firm for their scope of supply. The contract includes Outside Contractor Interface Agreements that describe how IOM and CSI performs engineering change activities per the requirements of the PG&E engineering change program while doing so under the respective IOM or CSI QA Program (described in Section 4.2.11.2 and 4.2.11.3, below). The actual engineering change is prepared by contracted engineering services under a defined task engineering services contract from PG&E. The engineering services contractor maintains an engineering resource pool that is qualified to the PG&E engineering change program. PG&E is performing the Owner Acceptance function in accordance with the engineering change program documents.

4.2.11.1.2 Manufacturing

The manufacturing phase for the PPS replacement equipment is also contracted to IOM and CSI for their respective scope of supply. This phase includes basic hardware and software design, detailed hardware and software design, hardware manufacturing, software development, integration of the hardware and software, Factory Acceptance Test and Site Acceptance Test. These equipment activities are outsourced to IOM and CSI under the PG&E DCPP Procurement Control Program [153]. IOM and CSI are performing the contracted equipment scope under their QA program [31 and 33] and their implementing procedures (described in the following sections). Specifications describing the equipment requirements as well as the required development and manufacturing activities are included in the contract. IOM and CSI are approved suppliers, audited by PG&E, under the PG&E Nuclear Procurement Program and associated directives.

The PPS replacement chassis, cards, cables, ASU, and sensing modules are being procured from IOM and CSI as basic components, furnished with Certificates of Conformance to purchase order requirements.

4.2.11.1.3 Inspection

Inspection of equipment purchased for implementation as part of design changes to PG&E nuclear facilities is governed by the PG&E DCPP Procurement Control Program [153] and associated directives.

As part of the procurement process, inspections occur at various stages of the project. Prior to submittal of specifications for bidding and eventual contract award to the vendor(s), verification is made that IOM and CSI are qualified per industry QA processes to provide the equipment identified within the specification.

Once the contract is awarded for procurement of the specified equipment and/or services, project related inspections begin. The vendors manufacturing facilities and service organizations undergo a general engineering inspection and familiarization. More formalized inspections occur as the project progresses. Prior to shipment of the equipment, inspections occur at the vendor facilities with the purchaser to verify manufacture of the equipment to approved drawings, project documentation and perform pre-FAT assembly, hardware configuration, and if applicable, software configuration.

The equipment is then shipped to the DCPP site and upon arrival is inspected to verify the delivered materials are in general compliance with the equipment purchase specification(s) and the associated shipping documents. Additional detailed inspections occur by the engineering and implementation organizations to verify technical details of the received equipment as part of the staging for implementation. Various details such as material counts, wiring, mountings, arrangements, configurations, and physical packaging (cabinetry) are inspected by PG&E.

As mentioned above, these activities are performed using both specific and general guidance provided in PG&E Nuclear Procurement and PG&E Nuclear Engineering directives and procedures.

4.2.11.1.4 Testing

The PPS Replacement Project includes several testing activities. A complete description of the testing is included in Section 4.11.1.2.1.

A Modification Test Plan (MTP) will be developed for the project. The MTP specifies the necessary testing to be performed during and after installation of the PPS replacement systems and components. The actual test procedures used will be a combination of permanent operations procedures, permanent maintenance procedures, and temporary test procedures. These procedures are prepared, reviewed, approved, controlled, and performed under existing PG&E Project and Station programs.

4.2.11.1.5 Installation

Installation of the PPS replacement systems and components will be performed in accordance with written installation procedures and work orders. The scope of the installation procedures and work orders includes safety tagging requirements, demolition and removal of old components, modification of racks for seismic requirements, installation of new equipment,, modification of supporting structures, cabling, terminations, checkout, and system power up. The PPS replacement systems are not available or operable until all post modification testing is performed as required by the MTP and the implementation is accepted by the station staff in accordance with PG&E Project procedures.

Installation procedures are also prepared, reviewed, approved, controlled and performed under existing PG&E Project procedures. Work orders are planned, scheduled and controlled using the PG&E work process. PG&E is experienced in the installation of major engineering changes, and is solely responsible for the quality of installation activities.

4.2.11.1.6 Operations

Operability of the PPS replacement and components will be determined in accordance with TS 3.3.1 and 3.3.2.

Operation of the digital RPS/ESF and associated components is conducted under various department directives and procedures. Operations Procedures are used to perform operational tasks with plant systems and components. Periodic test procedures are used to perform surveillance tests on plant systems and components.

4.2.11.1.7 Maintenance

Maintenance of the PPS replacement and components will be conducted under the Preventive Maintenance Program described in Nuclear System Directives and the DCPP Maintenance Program.

The DCPP Maintenance Program provides policies and procedures which direct and support the conduct of work as it relates to the philosophy of the DCPP maintenance activities and other groups performing maintenance at DCPP.

Maintenance procedures are used to perform maintenance activities on plant systems and components. Instrument procedures are used to perform module checkouts, instrument and instrument loop calibrations and checks, system troubleshooting and corrective maintenance. Surveillance procedures are used to perform surveillance tests on plant systems and components. PG&E is solely responsible for the quality of maintenance on the RPS and ESF.

The procedures described above will be revised as needed for the PPS Replacement equipment in accordance with existing Nuclear System Directives.

4.2.11.2 Triconex QA Program

Section 5.3 of Standard Review Plan [47] Appendix 7.1.C, "Guidance for Evaluation of Conformance to IEEE Standard 603 [21]," notes that for digital computer-based systems, the quality requirements described in Clause 5.3 of IEEE Standard 7-4.3.2-2003 [80] should be addressed. Compliance with Clause 5.3 of IEEE Standard, 7-4.3.2-2003 [80] is addressed in the following discussion and in section 4.11.1.1.

The IOM Nuclear QA Program Manual (IOM-Q2) [31] is the upper tier corporate document that defines the quality requirements for the design, manufacturing and testing of the Tricon system and associated engineering services provided by IOM for the DCPP digital PPS Replacement Project. The IOM Corporate Nuclear Quality Assurance Manual (NQAM) (IOM-Q2) [31] commits to 10 CFR 50 Appendix B [151], 10 CFR 21 [154] and NQA-1-1994 [58] as governing regulations along with international QA standards as a basis for the IOM Nuclear QA Program Manual [31]. The program is implemented by QA procedure manuals for engineering (EDM), manufacturing (EDM), QA Program Manual (QPM), and project procedures manual (PPM). The IOM QAP has been reviewed by NRC in conjunction with the Tricon V10 Topical Report Submittal [13] and audited on numerous occasions at the Lake Forest, CA facilities.

The IOM QAP Manual (IOM-Q2) [31] associated with both Tricon operating software and project applications software was reviewed by NRC in conjunction with the Tricon V10 Topical Report Submittal [13], and IOM Document NTX-SER-09-021, Nuclear System Integration Program Manual (NSIPM) [32]. A description of the project processes and the basis for implementing project procedures is provided in the NSIPM. The NSIPM implements the requirements of the IOM NQAM [31], 10 CFR 50 Appendix B [151], NQA-1-1994 [58], and the applicable Regulatory Guides and industry standards.

Project procedures (i.e., the PPM) govern all quality-affecting Project activities performed by IOM personnel for the DCPP PPS Replacement Project. The PPM provides appropriate controls for project activities conducted at the Invensys Operations Management (Invensys) Lake Forest facility. These controls ensure that all nuclear Class 1E projects (or non Class-1E projects where the customer has specified certain 1E requirements) processes, project activities, and project documents will meet the requirements of 10 CFR 50, Appendix B, 10 CFR Part 21 and the Invensys Quality Management System. This procedures manual provides specific controls for Invensys organizations that perform nuclear safety-related system integration project activities. The PPM is a collection of different procedures, including referenced Forms, and is a controlled document. Each PPM procedure is intended to implement key areas of project activities. Each procedure within the PPM is assigned a unique document number and title.

4.2.11.3 CSI QA Program

All work at CS Innovations is performed in accordance with the "Westinghouse Quality Management System" [33], a QA program that is based on 10 CFR Part 50 [151], Appendix B.

The QA program used by CSI is described in the ALS System Topical Report Submittal [15], Section 10, "Quality."

Clause 5.3 of IEEE 7-4.3.2-2003 [80] states that hardware quality is addressed in IEEE 603-1991 [21], and that software quality is addressed in IEEE/EIA Standard 12207.0-1996 [127] and supporting standards. The "Westinghouse Quality Management System" [33] program described in the ALS System Topical Report, Section 10 [15] is based on 10 CFR Part 50, Appendix B [151]. The ALS platform Life Cycle Management Process is described in Section 6 of the ALS System Topical Report Submittal [15].

Clause 5.3.1 of IEEE 7-4.3.2-2003 [80] requires an approved QA plan consistent with the requirements of IEEE/EIA 12207.0-1996 [127] for all software that is resident at run time.

As described in Section 2, the ALS platform has no resident software. Software is, however, used to design the ALS boards. The QA plan used for this effort is described in the ALS System Topical Report, Section 10 [15].

4.2.12 System Response Time (Section D.9.4.2.4 of DI&C-ISG-06 [1])

In accordance with IEEE 603-1991 [21], Clause 6.1, Automatic Control, which is addressed in Section 4.10.3.1 of this Enclosure, the PPS replacement equipment for DCPP is designed to work in cooperation with plant specific functional logic to automatically initiate and execute protective actions, with precision and reliability for the range of conditions specified. In order to complete a plant specific design, an evaluation must be performed to identify the existing setpoints, margins, errors and response times to ensure that existing plant safety analysis assumptions are enveloped.

The response time for the current Eagle 21 PPS is 0.409 seconds based on Westinghouse WCAP-11082 [39]. The PPS replacement has been specified to have a response time that is less than or equal to the current Eagle 21 PPS. For the PPS replacement, relevant setpoints, margins, errors and response times required for input to the digital PPS design are provided in the DCPP Units 1 & 2 PPS Replacement FRS [28] and Westinghouse WCAP-11082 [39]. The PPS replacement is designed to operate within the bounds of the requirements provided in these documents so that the assumptions used in the existing safety analyses are not invalidated.

In accordance with DCPP Units 1 & 2 PPS Replacement FRS [28], the time response of the PPS processing instrumentation (from input signal conditioner to conditioned output signal) shall not exceed 0.409 seconds.

The analysis for response time for the V10 Tricon PPS replacement architecture is contained in IOM Document 993754-1-817, Revision 1, “Maximum TSAP Scan Time,” that was submitted by PG&E in PG&E Letter DCL-12-039 [163], and for the ALS PPS replacement architecture is contained in CSI Document 6116-00011, “Diablo Canyon Process Protection System, ALS System Design Specification,” [19]. For the (temperature) channels shared with the ALS FPGA-based system, the 0.409 seconds is allocated between the ALS and the Tricon as stated in Section 1.5.8 of the IRS [29].

Section 7.5 of document 6116-00011 [19] identifies the ALS board access sequence and provides an analysis associated with digital response time performance. The DCPP PPS ALS system is configured in accordance with the qualification requirements of the ALS platform topical report..

4.2.13 Communications (Section D.1.2 of DI&C-ISG-06 [1])

The PPS replacement consists of four (4) Protection Sets architected such that each Protection Set is independent of and protected from adverse influence from the other Protection Sets. The PPS replacement does not utilize interdivisional safety-to-safety communications. The PPS replacement does incorporate interdivisional safety-to-non safety communications. The PPS replacement architecture ensures that communications between a safety division and non-safety equipment that resides within the Protection Set adhere to the guidance described in the ISG 4 Staff Positions. Figure 4-12 illustrates the communications architecture for the PPS replacement that meets NRC DI&C ISG 4 Staff [2] Position 1, Interdivisional Communications, as discussed in Section 4.8 of this LAR.

Figure 4-13 illustrates the communication architecture for a single Protection Set. The sections below discuss the communications for the Tricon and ALS portions of the PPS replacement.

4.2.13.1 Tricon-Based PPS Equipment Communications

The Tricon portion of the PPS replacement does not communicate data between redundant safety divisions. The P2P communication capability provided by the TCM is not used for the PPS replacement. The non-safety-related MWS [Section 4.2.9] within a redundant safety division communicates only with the safety-related controllers within that division. Two-way communications between the MWS and TCM are necessary because the TCM must be polled by the MWS in order to provide data. Additional information is provided in Section 4.8.

The PPS replacement design incorporates the NetOptics Model PA-CU port aggregator tap device shown in Figure 4-13 to ensure that only one-way communication takes place between the Tricon processors and the PDN Gateway Switch. The port aggregator tap is a hardware device that is installed between the Tricon processor, the MWS, and the PDN Gateway Switch. Ports A and B of the NetOptics are respectively connected to the Tricon TCM fiber optic NET2 port through a fiber optic-to-copper media convertor and directly to the MWS associated with the Tricon via copper Ethernet. The data link protocol from the NetOptics to the MWS and to the TCM media converter is Triconex NET2. The port aggregator tap copies all information that is flowing between Ports A and B to Port 1. Neither Port A nor B can read data from Port 1, and Port 1 cannot transmit data to Port A or Port B.

The PDN Gateway Switch is connected to Port 1 of the NetOptics device, thus providing one-way communications from the PPS replacement system to the PDN Gateway Switch. This design ensures that no data or command messages can be sent from the PDN Gateway Switch to the MWS or the Tricon TCM. There is no transmitting capability from NetOptics Port 1 back to Ports A or B, which ensures security of the

Tricon safety function. This NetOptics device permits two-way communications between the Tricon TCM and the MWS, while permitting the PDN Gateway Switch and PDN Gateway Computer read-only access to the Tricon TCM and the MWS.

Figure 4-13 only shows one TCM installed in the Tricon Main Chassis (Slot 7L), the PPS replacement will utilize two TCM cards in each main chassis (Slots 7L and 7-R). This will provide two non-safety-related communication paths to the MWS and the PDN Gateway Switch from each Protection Set to ensure continued communications if a single TCM fails.

The NetOptics Model 96443, Model PA-CU, or PAD-CU[1] port aggregator network tap was approved previously by the NRC for use with the Tricon V10 in Section 3.7.2.1 of the Tricon V10 NRC SER [155] and in a similar non-Tricon application in the Oconee RPS SER Section 3.1.1.4.3 [18]. NetOptics has confirmed to PG&E that the model number "96443" is the same as model number "PA-CU." Model number "96443" is the old stock-keeping unit part number for the Model PA-CU port aggregator network tap. The NRC staff determined that due to the electrical isolation provided by use of fiber optic cables and the data isolation provided by the Port Tap and the Maintenance and Service Interface (MSI) in the Oconee RPS, there was reasonable assurance that a fault or failure within the Oconee Gateway computer or the Operator Aid Computer will not adversely affect the ability of the Oconee RPS to accomplish its safety functions.

During the FAT, Invensys Operations Management will test the Protection Set communications paths illustrated in Figure 4-13 to verify that there is no inbound communications path associated with port aggregator network tap Port 1. That is, Invensys Operations Management will verify that communications from Port 1 to either the TCM on Port A or the MWS on Port B of the port aggregator network tap are not permitted. Results of this test will be documented in the Invensys Operations Management FAT report. Port aggregator dual in-line package (DIP) switch positions will be controlled by DCPP configuration management processes. The Port aggregator DIP switch positions will be controlled by a plant procedure or a plan that will be developed as part of the design change for installation of the PPS replacement after NRC approval of the LAR.

[1] The NetOptics Model PAD-CU has two one-way output ports but is otherwise identical in function to the PA-CU.

Figure 4-12 PPS Replacement Communications – All Protection Sets

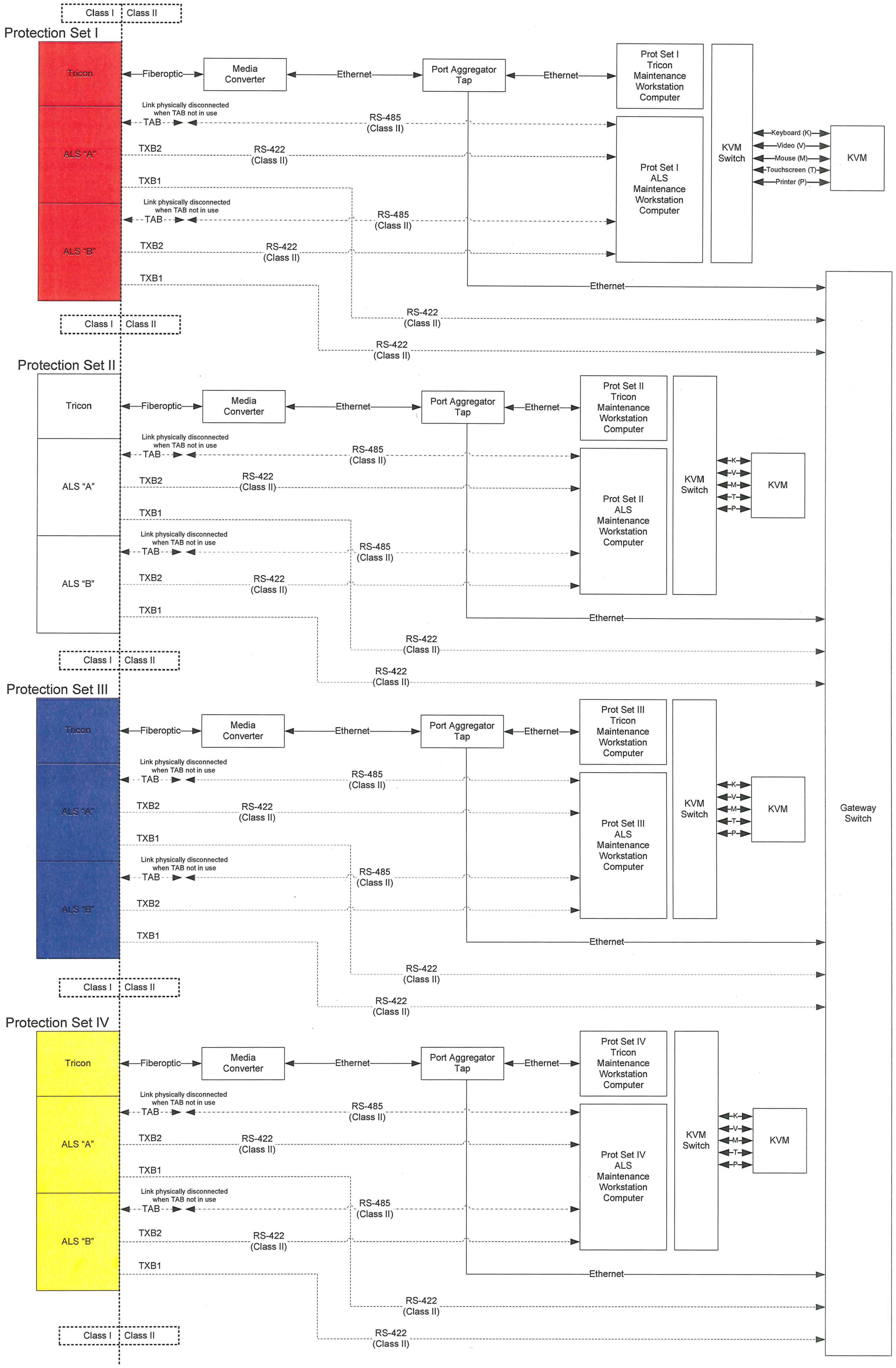
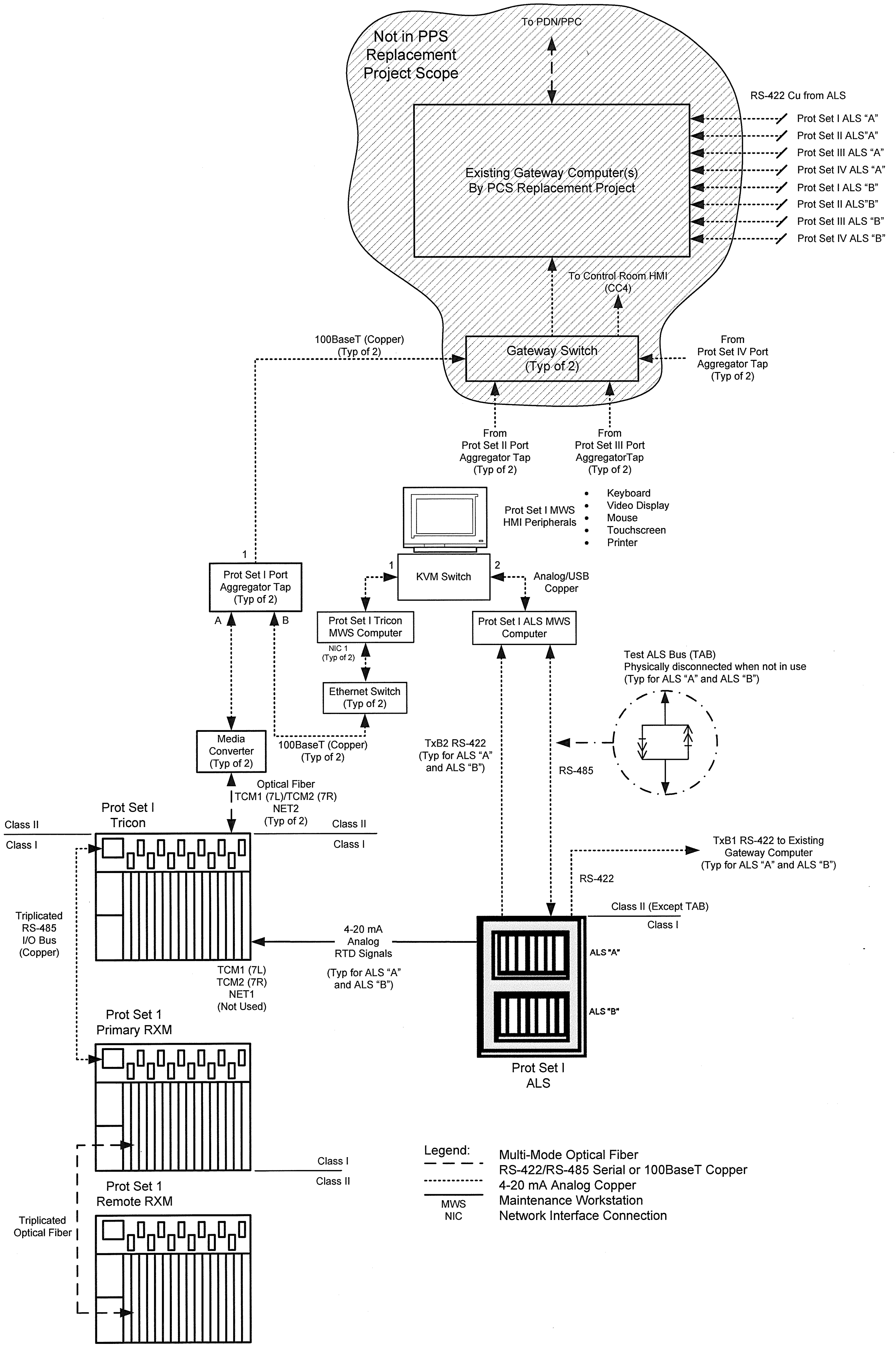


Figure 4-13 PPS Replacement Communications - Single Protection Set


Not in PPS Replacement Project Scope
To PDN/PPC
RS-422 Cu from ALS
Prot Set I ALS "A"
Prot Set II ALS"A"
Prot Set III ALS "A"
Prot Set IV ALS "A"
Prot Set I ALS "B"
Prot Set II ALS"B"
Prot Set III ALS "B"
Prot Set IV ALS "B"
Existing Gateway Computer(s) By PCS Replacement Project
To Control Room HMI (CC4)
100BaseT (Copper) (Typ of 2)
Gateway Switch (Typ of 2)
From Prot Set IV Port Aggregator Tap (Typ of 2)
From Prot Set II Port Aggregator Tap (Typ of 2)
From Prot Set III Port AggregatorTap (Typ of 2)
Prot Set I MWS HMI Peripherals
Keyboard
Video Display
Mouse
Touchscreen
Printer
1
2
KVM Switch
Analog/USB Copper
1
Prot Set I Port Aggregator Tap (Typ of 2)
A
B
Prot Set I Tricon MWS Computer
Prot Set I ALS MWS Computer
NIC 1 (Typ of 2)
Ethernet Switch (Typ of 2)
Test ALS Bus (TAB) Physically disconnected when not in use (Typ for ALS "A" and ALS "B")
Media Converter (Typ of 2)
100BaseT (Copper) (Typ of 2)
TxB2 RS-422 (Typ for ALS "A" and ALS "B")
RS-485
Optical Fiber TCM1 (7L)/TCM2 (7R) NET2 (Typ of 2)
Prot Set I Tricon
Class II
Class I
Class II
Class I
TxB1 RS-422 to Existing Gateway Computer (Typ for ALS "A" and ALS "B")
RS-422
Class II (Except TAB)
Class I
Triplicated RS-485 I/O Bus (Copper)
4-20 mA Analog RTD Signals
(Typ for ALS "A" and ALS "B")
ALS "A"
ALS "B"
TCM1 (7L) TCM2 (7R) NET1 (Not Used)
Prot Set 1 Primary RXM
Prot Set I ALS
Class I
Class II
Prot Set 1 Remote RXM
Triplicated Optical Fiber
Legend:
Multi-Mode Optical Fiber
RS-422/RS-485 Serial or 100BaseT Copper
4-20 mA Analog Copper
MWS Maintenance Workstation
NIC Network Interface Connection

4.2.13.2 FPGA-Based ALS Equipment Communications

There are no communication paths between redundant safety divisions in the ALS portion of the PPS replacement as shown in Figure 4-12 and Figure 4-13. The EIA-422 ALS communication channel from each ALS chassis to the Gateway computer is isolated, serial, one-way, as described in Section 2.2.1.3 of the ALS Topical Report Submittal [15] and Section 3.9 of the ALS 102 Design Specification [94]. The communication channel is provided by the ALS-102. Isolation of the ALS-102 communications channels is described in Section 3.9.1 of the 6002-10202 ALS-102 Design Specification [94]. The ALS-102B broadcasts data via communications channel TxB1 to the non-safety-related Gateway computer, which is common to all four Protection Sets. The TxB1 communications channel does not receive any data, handshaking, or instructions from the Gateway computer. The EIA-422 communications channels on the ALS-102 are inherently one-way. Thus, the ALS does not require use of the NetOptics device to prevent communication back to the ALS from the Gateway computer. The EIA-422 TxB2 communication channel that transmits data to the non-safety-related MWS is also serial, one-way with no handshaking.

The third ALS serial communications channel enables TAB functions between ASU maintenance software in the MWS and the ALS controller. This EIA-485 communication path is normally disabled, with two-way communications permitted only when the TAB communication link is physically connected between the TAB and the ALS MWS. Communications are not possible on the TAB if the communication link is physically disconnected. As explained in Section 2.2 of the ALS Platform Specification [95], the Protection Set containing the ALS chassis with TAB communications enabled remains functional during this action. The TAB is only allowed to monitor the state of internal registers and cannot affect safety-related data per ALS Requirements Specification [68] Section 7.2.

The two transmit-only EIA-422 communication channels, TxB1 and TxB2, and the TAB are described in Section 5 of the ALS Platform Specification [95], and Section 7 of the ALS Requirements Specification [68].

4.2.13.3 Non-safety-Related Tricon MWS and ALS MWS

The non-safety-related Tricon MWS shown in Figure 4-3, Figure 4-12, and Figure 4-13 is used to maintain and configure the Tricon and also to view the data from the Tricon . The non-safety-related ALS MWS shown in Figure 4-12 is used to view data from the ALS subsystem. Also, the ALS MWS, when physically connected to the TAB and when the TAB has been placed in service, is used to perform the maintenance functions associated with the ASU described in Section 2.6.3 of the ALS Topical Report Submittal [15].

A MWS may access data only within its own Protection Set. Communication with other Protection Sets is not implemented; that is, there are no means of connecting another Protection Set to another MWS without reconfiguring the Protection Set controllers and communications cabling. There are no communications switches in the architecture. Direct access to safety-related Protection Set communications from outside the Protection Set is prevented by the NetOptics port aggregator network tap.

The online non-safety communications, between the PPS controllers and their respective dedicated MWS units, improve the ability to maintain the PPS which improves the reliability of the PPS. In addition, the online Tricon and ALS non-safety communications enable on-line surveillance testing, calibration, and maintenance. The risk of challenging plant safety systems by inadvertent actuation is reduced through the ability to test when in bypass rather than requiring test in trip.

The online Tricon and ALS non-safety communications capability provide real-time, online data and status information on the PDN Gateway Computer and in the Control Room that are required to perform maintenance, calibration and testing. Without the online data links from the Tricon and ALS to the MWS and the PDN Gateway Computer, only the control board indicators and recorders would be available to provide "window" indicator information for the PPS. System trouble alarms would still be generated by the PPS on the Main Annunciator System, but without the alarm monitor and other data display capabilities provided by the MWS, there would be no direct means to remotely determine the specific cause of an alarm.

Lack of access to real-time, continuous, on-line PPS status data and diagnostic information would introduce a delay into PPS trouble identification and resolution, and substantially degrades the maintenance effectiveness and timeliness enabled by the diagnostic features built into the platforms and the application programs. The ability to make online use of the information provided by redundant, real-time data communications to the MWS and to the PPC improves PPS reliability and thus supports and enhances safety through providing timely diagnostic information and status details that assist performance of required trouble-shooting, maintenance, and surveillance activities.

4.2.13.4 Tricon-Based PPS Equipment Communications with Tricon MWS and PDN Gateway Switch

Communication between a safety-related Tricon controller and a non-safety device as shown in Figure 4-12 and Figure 4-13 is discussed in Sections 3.2 and 5.0 of the Triconex platform ISG-02 and ISG-04 compliance document [24] and Section 4.1 and 5.0 of the DCPP ISG-04 compliance document [25]. Under operating plant conditions the MWS displays plant parameters, perhaps including division diagnostic information. Access to functions beyond displaying data will be under administrative and physical controls. During plant on-line operation and during outages, the MWS will be used for performing the COT surveillance and modifying trip setpoints. Use of the MWS is in accordance with site-specific administrative (procedural) and physical-access controls to set and/or change Tricon safety system parameters while the channels are out of service (i.e., in bypass or partial trip mode).

The Tricon MWS is being designed to use Microsoft Windows™ XP Service Pack 3 operating system. The Tricon MWS is being designed to implement five Microsoft Windows™ based application programs: (1) Invensys WonderWare™ InTouch™ PPS application; (2) TriLogger; (3) Tricon Diagnostic Monitor; (4) Startup Delayer Application; and (5) TriStation 1131 (TS1131) Developers Workbench.

WonderWare™ InTouch™ Application

The WonderWare™ InTouch™ application provides on-line display of selected PPS internal parameters and trouble alarm details. The WonderWare InTouch application also is used for maintenance of individual PPS instrument channels in conjunction with the hardwired out of service (OOS) switches. The MWS WonderWare™ InTouch™ application will be the tool normally used to determine the specific cause of an alarm. The Main Annunciator System only displays system level alarms. The MWS InTouch application contains an alarm monitor, which is a troubleshooting aid that provides a detailed, specific display of the alarms generated by the Tricon PPS application.

Triconex TriLogger Application

The TriLogger software provides the ability to record, display, play back and analyze data from the Tricon system. Data can be viewed in real-time on the MWS. The TriLogger provides data trending and analysis capabilities and can be configured to trigger on specific events to log detailed data to aid technicians in isolating, diagnosing, and troubleshooting problems. The TriLogger must be connected and running at all times to perform these functions.

Tricon Diagnostic Monitor Utility Application

The Tricon Diagnostic Monitor utility displays Tricon system and module status by mimicking the actual Tricon chassis and slots, so that the user can find the exact location (chassis number and slot number) of a module that may be experiencing a fault or other problem. The Tricon Diagnostic Monitor Utility improves reliability by aiding rapid troubleshooting and fault location at the Tricon system level.

Startup Delayer Application

Startup Delayer delays WonderWare startup until the DDE Server has initialized. Otherwise, WindowViewer may startup first and never connect to DDE Server.

TriStation 1131 (TS1131) Developers Workbench Application

TriStation 1131 is a PC-based application development workstation tool that provides a comprehensive set of development, test, monitor, validation and diagnostic tools for Triconex PLC. The TS1131 program is utilized to maintain the PPS application program and may also be used for monitoring and troubleshooting purposes. The TS1131 program is described in Section 3.1.3.2 of the Tricon V10 SER [158].

The TS1131 tool will not normally be running while the Tricon is performing its safety function as described in Section 3.10.2.9 of the Tricon V10 SER [158]. If the TS1131 workstation is connected during online safety operation for maintenance or troubleshooting purposes, its use will be controlled via administrative controls and qualified maintenance personnel.

Write access to the operating Tricon is governed by the Tricon keyswitch. With the Tricon keyswitch in the RUN position, use of the TS1131 program is limited to read only access to the Tricon. Parameters may be examined, and application program logic operation may be observed in real time, but changes are not possible. The TS1131 program can only write to the Tricon when the Tricon keyswitch is in the PROGRAM position. With the keyswitch not in RUN, the PPS application will initiate an alarm on the MAS and the channel for each function processed by the Tricon subsystem protection set within the safety division will be declared inoperable with respect to its safety function.

Regardless of whether the Tricon keyswitch has been deliberately manipulated or whether the condition is the result of Tricon hardware or software failure, the internal Tricon diagnostics will detect a “keyswitch not in RUN” condition and the PPS application program will initiate a PPS Trouble alarm on the MAS. When the “keyswitch not in RUN” condition exists, the affected Tricon is considered to be INOPERABLE with respect to its safety function. The operator would enter the appropriate Technical Specification actions upon determination that the PPS trouble alarm was caused by the “keyswitch not in RUN” condition.

Even with the “keyswitch not in RUN” condition existing in multiple protection sets, negative impact is limited because on-line maintenance will normally be performed in one protection set at a time, and each Tricon protection set has its own dedicated, independent MWS. Therefore, only one Tricon protection set at a time would be configured physically to make software changes. If the TS1131 is not connected and running, changes cannot occur even if the “keyswitch not in RUN” condition exists. That is, the mere existence of the “keyswitch not in RUN condition” does not initiate changes. Intentional action by a trained, knowledgeable individual is also required. Given the PPS trouble alarms that would be active in all affected protection sets, it is highly unlikely that unintended changes could occur.

If a PPS Trouble alarm were to occur on the MAS due to the "keyswitch not in RUN" condition, regardless of the cause, the operator would notify DCPP Maintenance. In the absence of the detailed alarm monitoring provided by an on-line MWS (via the TCM NET2 interface), the maintenance technicians would be required to obtain work orders, gain access to the affected protection set, connect and boot the MWS, and only then could begin to determine the cause of the alarm. The alarm information would not be available if the alarm were due to a transient condition that cleared between the time the condition initiated and when the MWS was operational. Diagnosis of the condition could be delayed for several hours. With the on-line MWS and the alarm monitor function, the condition – whether caused by intentional manipulation of the Tricon controller keyswitch or by a hardware or software failure involving the keyswitch – would be identified immediately.

The capability for an on-line Tricon MWS is essential to maintain the Tricon safety function, including surveillance testing per the Technical Specifications and other required maintenance and is equivalent to the existing, approved Eagle 21 test in bypass capability. The MWS is required to bypass channels for testing. Removing a Tricon from service during such routine maintenance would require tripping all the channels in that protection set, which would make up one channel in the coincidence logic for all channels in the protection set. This condition increases the risk of challenging plant safety systems by inadvertent actuation should another channel trip inadvertently with the protection set out of service.

The application software utilizes the safety-critical Tricon library functions "GATENB" and "GATEDIS" to control MWS access to the Tricon in RUN mode. To update a parameter, the technician places the safety-related instrument-loop-specific out of service switch in the closed position. The Tricon will activate the pre-programmed "GATENB" and "GATDIS" functions to open a data window of limited range. Prior to updating the parameter in the Tricon control program, the new value will be staged on the MWS screen for acknowledgement. After the changes have been made and the maintenance technician has placed the switch in the open position, the safety-related control logic will close the data window to prevent further changes. The MWS interface will also have protective measures built in, such as password-protected log-on, role-based security functions to ensure only authorized individuals have the ability to update tuning parameters. If the out of service switch is de-activated before the change is made, the safety-related control logic will return the instrument loop to normal operation automatically. A similar series of request/confirm actions is used to direct maintenance and test functions from the MWS, always under control by the safety-related Tricon application program.

Section 4.0 of Appendix 1 to the Triconex platform conformance to DI&C ISG-02 and ISG-04 [24], "Non-safety VDU Communication To TRICON Example", discusses the use of the MWS and "GATENB/GATDIS". The GATENB/GATDIS functions are also discussed in Section 4.1 and Section 5.0, Point 3 of the DCPP specific evaluation of conformance to DI&C ISG-04 [25].

Communications from the Tricon to external non-safety systems are functionally isolated by the TCM and NetOptics Model PA-CU network port aggregator tap.

The PPS replacement design incorporates the NetOptics Model PA-CU port aggregator device described in Section 4.2.13.1 to ensure that only one-way communication takes place between the Tricon processors and the PDN Gateway Switch that transmits data to the PDN Gateway Computer. The NetOptics Model PA-CU port aggregator prevents inbound communications from external devices or systems connected to Port 1 of the port aggregator from being sent to interactive Ports A and B. Port 1 is a transmit-only port for external devices or systems connected to Port 1, and it does not listen to and is not affected by the communications protocol (or lack thereof) of the external device or system to which it is connected. The NetOptics device permits two-way communications between the Triconex TCM and the MWS, while permitting the PDN Gateway Switch and PDN Gateway Computer read-only access to the Tricon TCM and the MWS. Two-way communications between the TCM are necessary because the TCM must be polled by the MWS in order to provide data. The network switches between the port aggregator taps and the MWS ensure that Tricon multicast operation will continue if the Tricon MWS were to cease communications. The network switches are redundant to ensure continued Tricon multicast operation on failure of a single Tricon network link.

Data isolation between the safety-related Tricon control processor and the non-safety MWS is performed by the safety-related TCM. Fiber optic cable electrically isolates the Tricon from external non-safety-related devices such as the NetOptics port aggregator network tap. DCPP PPS replacement specific TCM compliance with ISG-04 [2] is discussed in Sections 4.1 and 5.0 of the Triconex DCPP PPS ISG-04 Conformance Report [25].

4.2.13.5 FPGA-Based ALS PPS Equipment Communication with ALS MWS and PDN Gateway Computer

The ALS MWS (containing the ASU maintenance software) is the primary tool used when accessing a particular ALS system in operation. The ALS MWS provides plant personnel access to advanced features of the ALS system such as system diagnostics, post-trip analysis, monitoring real-time operation, and assistance in performing user-initiated test, calibration and maintenance operations.

The on-line ALS MWS is required to maintain the ALS, including surveillance testing and calibrations per the Technical Specifications and other required maintenance. This function is similar to the existing approved Test in Bypass capability for Eagle 21. The diversity design of the ALS enables either (but not both) Chassis "A" or Chassis "B" in a protection set to be bypassed for maintenance or testing while the other chassis remains fully operational (although, in the bypassed condition, certain post-accident monitoring functions may not be available and need to be controlled administratively).

Without the flexibility provided by the ALS diversity design, the Technical Specifications actions would require tripping all the channels associated with the ALS chassis when removing a given protection set ALS chassis from service. In turn, this would make up one channel in the coincidence logic for all channels in the affected ALS protection set. Such an action increases the risk of inadvertently actuating plant safety systems were another channel to trip with the ALS protection set out of service.

The ALS MWS is being designed to use a Microsoft Windows™ XP Service Pack 3 operating system and to utilize Microsoft Windows™ based CSI ALS Service Unit (ASU) software that is described in Section 2.6.3 of the ALS Topical Report [15].

The DCPP PPS Replacement MWS is being mounted permanently in the PPS rack containing the PPS in a manner similar to that shown in Figure 2.6-1 of ALS Topical Report [15]; however, the MWS functions that use interactive TAB communications will be available: (1) only when the TAB is physically connected to the ALS MWS by qualified personnel under administrative controls; and (2) only on one ALS "A" or "B" subsystem at a time.

The TAB from ALS-102 Chassis "A" and Chassis "B" is provided with individual EIA-485 ports on the ALS MWS. The ASU software ensures that the correct TAB is connected to the respective EIA-485 port when the TAB is enabled.

ALS MWS Features

The main features of the ALS MWS are:

State Information – Provides monitoring of real-time operation, including all I/O signals as well as detailed status information from debugging registers. The advanced monitoring capabilities enable fast system diagnostics and troubleshooting.

System and Board Information – Provides detailed information about the configuration of an ALS system, including board FPGA programming, board build information, and board configuration.

Blackbox – The ASU software includes a so-called "blackbox" functionality where all events of an ALS system are transmitted by the ALS-102 CLB Transmit Bus TxB2 to the MWS for storage and subsequent retrieval. This allows plant personnel to inspect the ALS system's reaction to a past event. The blackbox function enhances ALS reliability and therefore safety by helping to reduce the time required to pinpoint the cause of a series of events. The MWS must be connected to the ALS via the Transmit Bus TxB2 during an event in order to capture and store the event data via the blackbox function. The MWS needs to be connected to the ALS chassis via Transmit Bus TxB2 and receiving data during online operation in order to provide data on events that may occur at any time.

Test – Application specific periodic surveillance tests can be implemented through the MWS. Based on the needs of the application features, tests may be implemented in the CLB that allow surveillance testing to be performed and/or monitored through the MWS.

Calibration – The MWS is used to readout and change application setpoints and channel calibration coefficients. The CLB holds the application setpoints and according to the application, it will allow the MWS to modify these setpoints. The MWS is also used during I/O channel calibration where it is used for selecting the board and board channel to be calibrated and to change calibration coefficients based on the readings received on an external calibrator.

Operation of the MWS is passive and non-intrusive, i.e., it can only modify the safety system tunable parameters stored in nonvolatile memory (NVM) for which it is designed (i.e., I/O calibration coefficients, setpoints and tuning constants). It is not possible to modify the safety algorithm or logic using the MWS. All communications initiated by the MWS take place on the TAB, and only when the TAB is physically connected between a ALS protection set and its dedicated ALS MWS. No reliable ALS bus (RAB) interruption is possible, effectively isolating the ALS MWS from ALS safety functions.

ALS Parameter Display

The MWS also provides a passive parameter display function using one-way ALS-102 CLB EIA-422 Transmit Bus TxB2. The ALS parameter display function allows the MWS to display parameters transmitted to it online by the one-way TxB2 transmit bus described in Section 2.2.1.3 of the ALS Topical Report [15]. The parameter display function does not require the TAB to be connected.

The ASU parameter display function is a Visual C++ based application developed for the Microsoft Windows API using Microsoft Foundation Class (MFC) libraries to provide graphical user interfaces for displaying ALS system status on the MWS and for providing user controlled access to the ALS controllers for performing maintenance operations such as calibration.

Upon start-up, the application establishes a dedicated serial port connection to the MWS RS-422 serial communication card port that is connected to the ALS-102 CLB unidirectional one-way TxB2 output in each ALS chassis “A” and “B.” These dedicated MWS serial ports receive ALS system status at a rate of 10 Hz (i.e., once every 100 ms).

Upon establishing the dedicated serial port connection on the MWS, the ASU parameter display function spawns a software thread to receive, validate, and store the data received from the respective ALS-102 TxB2. Validation of the received data consists of checking the packet header contents, checking packet length, performing a CRC check on the packet contents, and then comparing the calculated CRC with the CRC inside the TxB2 packet. If the data received by the parameter display application is invalid (i.e. invalid CRC), the application indicates the issue on its graphical user interface (GUI) and an entry is made in the application status log. If the data received by the parameter display application is valid, the application records the ALS system status in a data class which contains methods that are called by different GUI to extract and display the specific ALS system status.

Malfunctions of the ASU parameter display function cannot adversely affect ALS safety system operation because EIA-422 communications between the ALS and the ALS MWS via TxB2 are strictly one-way from the ALS-102 to the ALS MWS and the EIA-485 TAB is physically disconnected except for brief periods when the TAB for either ALS “A” OR “B” is connected to the MWS for maintenance under administrative control by trained technicians.

ALS to ALS MWS Communications

The ASU application software communications from the ALS chassis “A” and “B” ALS-102 CLB to the ALS MWS are via the transmit-only (no handshake) ALS-102 communication channel TxB2. The TxB2 channel is a dedicated and independent serial communications channel which transmits application specific input and output states and values continuously to the ASU application implemented in the MWS. The TxB2 communications channel does not receive any data, handshaking, or instructions from the MWS. The EIA-422 communications channels on the ALS-102, as discussed in Section 3.9 and Section 4.6 of the 6002-10202 ALS 102 Design Specification [94], are electrically isolated and inherently one-way; therefore the use of the NetOptics device is not required.

Two-way TAB communications between ASU application software in the MWS and the ALS chassis are used to perform ALS maintenance and calibration functions. This EIA-485 communication path is normally disabled, with two-way communications permitted only when the TAB communication link is physically connected between the TAB and the respective ALS MWS EIA-485 port under administrative control by trained technicians. TAB communications are disabled when not needed by physically disconnecting the TAB from the MWS. Communications are not possible on the TAB if the communication link is physically disconnected. The ALS MWS is connected to and communicates with the ALS via the TAB only when required to calibrate the ALS, update tuning constants, perform surveillances required by Technical Specifications, as well as to troubleshoot and otherwise maintain the ALS. The diverse ALS subsystem whose TAB has not been enabled will continue to perform its safety function without impact. An ALS trouble alarm is initiated on the MAS when the TAB is enabled. The non-safety communications provided by the Transmit busses will allow the operator to ascertain quickly the cause of the alarm, if the operator is not already aware of the maintenance activity being performed under procedural control. There are no interdivisional communications between the MWS and the ALS.

The ALS transmit bus TxB1 transmits data from each ALS "A" and "B" ALS-102 CLB to the PDN Gateway Computer. The ALS-102 CLB communication channel TxB1 is a EIA-422 communication link where the receive capability is physically disabled by hardware as described in the CSI document 6002-10202, "ALS-102 Design Specification" [94]. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 CLB is electrically incapable of receiving information from outside the ALS-102 via the Transmit Busses TxB1 and TxB2. Therefore, messages are not disregarded or rejected by the ALS-102 CLB. In effect, this is the same as the data isolation achieved by a "broken wire." TxB communications are described in Section 5.3 of the ALS Topical Report [15].

The Class 1E/ non-1E data communication for the ALS-102 CLB is described in Sections 2.2.1.3 and 5.3.2 of the ALS Topical Report [15], and in Position 2 of CSI document 6116-00054 [164]. The electrical isolation of the transmit busses is performed by magnetic couplers located on the ALS-102 CLB. The TxB isolators are described in Section 3.9.1 of CSI document 6002-10202, "ALS-102 Hardware Design Specification" [94]. Fault isolation occurs by way of board mounted transient voltage suppressors, board mounted fuses, and external fuses. The electrical isolation qualification of the Class 1E/non-1E data communication will be qualified with an isolation fault test that will be conducted per IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" [92] and Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems." This will be documented in a supplemental test report to be issued by November 15, 2013.

4.2.14 KVM Switch

The two MWSs in each Protection Set share common peripheral devices such as the keyboard, video display, mouse, touchscreen interface, and printer through a KVM switch. The Tricon MWS is dedicated to the Tricon PPS subsystem in the respective set; the ALS MWS is dedicated to the ALS PPS subsystem in that set. The KVM switch is being designed to be continuously on-line for monitoring data from either the Tricon or ALS platform via their respective MWSs. An AV4PRO-VGA KVM switch is being specified for the PPS replacemement. This KVM switch has ports for four computers (VGA video port, USB port, and audio port for each computer), a user console with a VGA video port, a USB keyboard port, and a USB mouse port), a user console with two switched USB ports (one for touchscreen and one for printer), and an options port.

The IRS [29] includes specifications to control the type of connection and operation modes of the KVM switch. Section 2.3.7of the IRS [29] states the KVM switch shall permit only connections between a single computer and the selected video display and peripheral devices. Connection between the computers shall not be permitted. In addition Section 2.3.7of the IRS [29] states the AV4PRO-VGA KVM switch shall utilize the default switching mode, in which the video display, keyboard and mouse and the enumerated USB ports are all switched simultaneously. This specification prevents the enumerated ports from being switched separately from the KVM. The user console's two switched USB ports, which use enumerated switching, pass data straight through the KVM switch without interpretation. With operation of the KVM switch utilizing the default switching mode, if a keyboard is connected to the USB1 or USB2 port, the hotkeys cannot be used to perform switching, and USB1 and USB2 traffic cannot cause an inadvertent switch. The keyboard and mouse are being designed to use the emulated switching function, not the enumerated switching function, and thus only the keyboard, mouse, and the button on the KVM switch can control the switch. A user console switched USB port is being used by the local printer for each protection set.

The unused MWS and KVM switch ports will be addressed in accordance with the DCPP CSP [48]. The local printer for each protection set will also be controlled by the PG&E SCMP [159]. Remote control KVM switching or KVM firmware update requires a custom serial cable. The KVM firmware update requires specialized software on the computer being used to perform the update. KVM firmware update will only be done by procedure. The MWS and KVM switch are being located inside a locked cabinet inside a vital area inside the protected area, which will minimize the possibility of the inadvertent actions. In addition, administrative and PG&E SCMP [159] configuration controls prevents inadvertent loading of an EPROM image that could corrupt operation of the KVM switch.

During normal, non-maintenance operation, the ALS communicates one-way to its dedicated MWS via Transmit Bus TxB2. Safety to non-safety communications using a TxB2 communications channel is addressed in Section 5.3.2 of the ALS Topical Report [15]. The TxB2 data communication paths from the ALS-102 CLB to the ALS MWS is a EIA-422 communication link in which receive capability is physically disabled by hardware as described in 6002-10202, the ALS-102 Design Specification. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 is electrically incapable of receiving information from outside the ALS-102. Therefore, the ALS cannot be affected by a malfunction in the dedicated, MWS associated with an ALS protection set regardless of whether the malfunction is caused by KVM switch malfunction or by malfunction of the MWS itself. If the KVM switch is somehow manipulated, the ALS will not be affected even if the KVM switch fails because the ALS communicates only one-way with the MWS, except for short periods when the TAB communications are enabled by physically connecting the TAB communication link. Connection of the TAB is performed as directed by a trained technician using an approved procedure. Therefore, if the KVM switch failed in some way to connect the ALS MWS and the Tricon MWS together, the ALS subsystem would not be affected. The Tricon subsystem may be affected, but the D3 analysis [106] evaluates the common cause failure of the Tricon and concludes the required protection system function can be performed.

4.3 Hardware Development Process (Section D.2 of DI&C-ISG-06 [1])

The hardware development process for the digital portions of the PPS replacement is discussed in the following sections for both the Tricon and the ALS. All safety-related digital hardware for the PPS replacement is being developed by IOM and CSI for their respective equipment, under PG&E contract.

Compliance with IEEE Standard 603-1991[21] Clause 5.3 Clause 5.3 "Quality," is described in Sections 4.2.11 and 4.10.2.3 of this Enclosure. Compliance with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3 "Quality," is described in Sections 4.2.11 and 4.11.1.1.

a) Tricon-Based PPS Equipment

Section 5.1.2 of the 7286-545-1 Tricon V10 Topical Report Submittal [13] describes the product development process for the Tricon platform. IOM document NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System" [146] discusses the differences between the previously approved Tricon V9.5.3 and the Tricon V10.2.1. One of the key differences between the V9.5.3 and the V10.2.1 is the fact that Triconex has added additional processes distinctively tailored to development of software used in designing and maintaining PLDs. Details of this process are provided in NTX-SER-09-06, "Triconex Development Processes for PLDs in Nuclear Qualified Products" [145].

b) FPGA-Based ALS PPS Equipment

The "Westinghouse Quality Management System," a QA program is based on 10 CFR Part 50, Appendix B, is used for the development of all electrical and electronics assemblies.

The ALS is a FPGA-based hardware logic system that does not execute software. This was discussed in Section 3.0 of Docket 50-482, Amendment 181 to License No. NPF 42 [14]. The FPGA is however configured by using software tools. Therefore the development of the configuration for the FPGA is similar to a traditional microprocessor based software development program. Section 4.5 of this LAR describes the configuration portion of the FPGA development. The process for the final hardware result of the FPGA configuration is discussed in FPGA Development Procedure NA 4.51 [61].

4.4 Software Architecture (Section D.3 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Software Architecture for IOM and CSI in support of the PPS replacement project following the guidance in BTP-7-14 [4], Section B.3.3.2 is described in the following sections.

a) Tricon-Based PPS Equipment

The software architecture for the Tricon portion of the PPS Replacement Project is described in the Tricon V10 Topical Report Submittal [13] Section 2.1.3. Triconex Document No. 993754-11-914, Protection System Replacement DCPP PPS System Architecture Description [144], provides further information regarding the Triconex platform operating system software and also provides an overview of the application software architecture and function. More detailed information regarding the PPS application is provided in the SRS [75].

b) FPGA-Based ALS PPS Equipment

The ALS is a FPGA-based hardware logic system that does not utilize executable software. It instead incorporates a collection of logic elements such as “and” gates, “or” gates, bistable flip-flops, registers, inverters, adders, and other digital logic. Some logic elements are combinations of individual gates. The field programmable portion of the name refers to the ability to determine the functionality of the FPGA by the end user.

The FPGA logic elements are arranged in an array of open connections. This could be compared to a series of similar but unconnected discrete logic elements on a breadboard, where the functionality of the overall circuit is undetermined until the connections are made. The FPGA also contains a series of reconfigurable interconnects that allow the logic elements to be "wired together.” An FPGA configured for a particular application results in a fixed piece of hardware comprised of basic logic and FSMs. A fixed hardware device comprised of basic logic and FSMs results in a completely deterministic circuit capable of realizing multiple aspects of the particular application functionality in a discrete non-sequential evaluation manner.

Further information regarding the generic ALS architecture is provided in 6002-00011 ALS Platform Specification [95] and the ALS Topical Report Submittal [15]. Further information regarding the PPS replacement specific software architecture is provided in section 2 of 6116-00011 Diablo Canyon PPS System Design Specification [19] and the ALS-102 FPGA Requirements Specification [20].

4.5 Software Development Process (Section D.4 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 states:

Computer software shall be developed, modified, or accepted in accordance with an approved software QA plan consistent with the requirements of IEEE/EIA 12207.0-1996. The software QA plan shall address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can be found in International Electrotechnical Commission (IEC) 60880 (1986-09) [128] and IEEE Std 730TM-1998 [129].

The software plans and specifications addressing software development for the DCPP PPS replacement are addressed in the following sections for both the Tricon and the ALS. All safety-related software for the PPS replacement is being developed by these two organizations for their respective equipment, under PG&E contract.

The following sections provide a description of each of the software plans associated with life cycle development for the respective platform applications for the DCPP PPS replacement. The PG&E PPS Replacement Project also has developed a project specific System Quality Assurance Plan (SyQAP) [52] and System Software Verification and Validation Plan [53], as described in the following sections, to address PG&E responsibilities after turnover from the vendors.

a) IOM

Section 2.3 and 2.4 of the Tricon V10 Topical Report Submittal [13] describe the QA program and software life cycle processes for the design and qualification of the Tricon platform software (operating system software, application and software development tools). Section 2.3.2 of Reference [13] describes the software life cycle planning processes of the design and qualification of the Tricon platform.

The IOM NQAM Manual [31] describes the program measures incorporated by IOM to ensure the Tricon application software attains a level of quality commensurate with its importance to safety functions and required by 10 CFR 50 Appendix B [151], performs the required safety functions correctly, and conforms to established technical and documentation requirements, conventions, rules, and industry standards. The Triconex QPM applies to application software developed for all Tricon projects in the U.S., including the PPS Replacement Project.

b) CSI

Section 6 of the ALS Topical Report Submittal [15] describes the QA and software life cycle processes for the development of ALS boards and systems. Section 6.2 of Reference [15] describes the software life cycle planning documentation required for software development on the ALS digital platform. A listing of the specific software planning documents described in the following sections is included in Section 12 of Reference [15].

The "Westinghouse Quality Management System" [33] used by CSI describes the program measures to ensure all 10 CFR 50 Appendix B [151] requirements are met in the development of ALS boards and systems.

4.5.1 Software Management Plan (Section D.4.4.1.1 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], software management for PG&E and the Software Management Plan (SMP) for both IOM and CSI in support of the PPS replacement project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1and BTP-7-14 [4], are described in the following sections.

4.5.1.1 PG&E

PG&E will not develop software for the PPS replacement. DCPP Program Directive CF2 [49] and procedures CF2.ID2 [50] and CF2.ID9 [51] control software development throughout the remaining life cycle phases (i.e., Operations, Maintenance, Retirement) under the control of PG&E after development and delivery of software and/or systems to PG&E from the 10 CFR 50 Appendix B Suppliers.

4.5.1.2 IOM

Triconex Document No. 993754-1-905, PPS Replacement DCPP Project Management Plan (PMP) [69], meets the guidance of BTP 7-14 Section B 3.1.1 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and describes the management process for the PPS Replacement Project to ensure adherence to the IOM quality and process requirements for the development of nuclear safety-related software and hardware.

This plan addresses the following areas:

- Project Organization
- Management Oversight
- Organizational and Personnel Responsibilities
- Project Risks
- Development Environment and Product Security

4.5.1.3 CSI

CSI Document No. 6002-00000, ALS Management Plan [59], meets the guidance of BTP 7-14 Section B3.1.1 [4] and defines the process used to manage the ALS Platform development project and overall project life-cycle. The Management Plan follows the QA program used by CSI as defined in the "Westinghouse Quality Management

System" [33]. This management plan addresses two aspects of ALS platform management: 1) development project management and 2) overall product life-cycle management.

CSI Document No. 6116-00000, DCPP ALS Management Plan [60], meets the guidance of BTP 7-14 Section B3.1.1 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the process used to manage the PPS Replacement project and overall product life-cycle. This plan follows the QA program used by CSI as defined in the the "Westinghouse Quality Management System" [33] and defines the set of unique activities as defined in IEEE Standard 1058-1998 "IEEE Standard for Software Project Management Plans" [137], for delivery of the ALS-based chassis portion of the PPS replacement system.

4.5.2 Software Development Plan (Section D.4.4.1.2 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Software Development Plans (SDP) for both IOM and CSI in support of the PPS Replacement Project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.2.1 PG&E

PG&E will not develop software for the PPS replacement.

4.5.2.2 IOM

Triconex Document No. 993754-1-905, PPS Replacement DCPP PMP [69], meets the guidance of BTP 7-14 Section B 3.1.2 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the development processes for the PPS Replacement Project to ensure adherence to the IOM quality and process requirements for the development of nuclear safety-related software and hardware.

This plan addresses the following areas:

- Project Organization
- Management Oversight
- Organizational and Personnel Responsibilities
- Project Risks
- Development Environment and Product Security

Triconex uses a standardized project management process to assess risks, as described in Section 3.4 and 3.5 of the Triconex DCPP Software PMP [69]. This methodology is used to identify, assess, monitor, and control areas of risk that arise during the software development project. In the course of project execution, the project risks are monitored, and the current assessment is reviewed to determine if it needs to be modified.

4.5.2.3 CSI

CSI Document No. 6002-00000, ALS Management Plan [59], meets the guidance of BTP 7-14 Section B3.1.2 [4] and defines the process used to manage the ALS Platform development project and overall project life-cycle. The Management Plan follows the QA program used by CSI as defined in the “Westinghouse Quality Management System” [33]. This management plan addresses two aspects of ALS platform management: 1) development project management and 2) overall product life-cycle management.

CSI Document No. 6116-0000, DCPP ALS Management Plan [60], meets the guidance of BTP 7-14 Section B3.1.2 [4] and NRC RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” [136] and defines the process used to manage the PPS Replacement project and overall product life-cycle. This plan follows the QA program used by CSI as defined in the “Westinghouse Quality Management System” [33] and defines the set of unique activities as defined in IEEE Standard 1058-1998 “IEEE Standard for Software Project Management Plans” [137], for delivery of the ALS-based chassis portion of the PPS replacement system.

As described in the ALS Topical Report Submittal [15], Section 12, risk management for the ALS platform is a part of the SVP. This is included as part of the Life Cycle and is documented in the DCPP ALS Management Plan [60]. The ALS Life Cycle Management Process is described in Section 6 of ALS Topical Report Submittal [15].

4.5.3 Software QA Plan (Section D.4.4.1.3 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Software QA Plan (SQAP) for IOM, CSI and PG&E in support of the PPS replacement project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.3.1 PG&E

The DCPP SyQAP for the PPS Replacement Project [52] meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” [136] and defines the activities to be followed in the design, development, review and testing for the PPS Replacement project, by PG&E, IOM and CSI. This plan establishes the goals, processes, and responsibilities required to implement effective software quality management for the PPS replacement software, ensure any required software performs correctly, and that the required software functions conform to established regulatory requirements, technical requirements, conventions, rules and standards. To achieve these goals, software development will proceed in a traceable, planned and orderly manner. Throughout this plan, "software" is used when referring to firmware and logic developed from software based development systems.

4.5.3.2 IOM

Triconex Document No. 993754-1-801, PPS Replacement DCPP SQAP [71], meets the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the activities to be followed in the design, development, review, and testing for the IOM scope of supply in the PPS Replacement Project.

4.5.3.3 CSI

CSI Document No. 6002-00001 ALS QA Plan [63], meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the techniques, procedures, and methodologies that will be used by CSI to assure quality in the design and test developments of the ALS platform, and in particular in the FPGA design and test activities performed as part of the platform development and implementation for the PPS Replacement Project.

4.5.4 Software Integration Plan (Section D.4.4.1.4 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Software Integration Plans for IOM and CSI in support of the PPS replacement project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.4.1 The PPS replacement design uses separate MWSs for the ALS and the Tricon subsystems for each protection set. This provides physical separation of the MWSs which ensures that the ALS and Tricon subsystems are completely separate and independent.

4.5.4.2 Triconex Document No. 993754-1-910 DCPP Tricon PPS Software Integration Plan [76], meets the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital

Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and describes the system integration strategy for integrating the V10 Tricon Protection Set software functions together into a TSAP, integrating the TSAP with the hardware, and the steps involved in the software integration process.

4.5.4.3 CSI

The FPGA Development Procedure NA 4.51 and the Westinghouse Level 3 Quality Management System Procedure Electronics Development Procedure NA 4.50 [61], meets the guidance of BTP 7-14 Section B3.1.4 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the FPGA Development Procedure for all phases of FPGA development for the ALS scope of supply in the PPS Replacement Project.

The Westinghouse Level 3 Westinghouse Quality Management System Procedure, Electronics Development Procedure NA 4.50 [62], meets the guidance of BTP 7-14 Section B3.1.4 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the ALS procedure for development of all electrical and electronics assemblies. This plan includes specifying and designing electronics circuit designs, mechanical packaging, tests procedures and test equipment in the ALS scope of supply for the PPS Replacement Project.

4.5.5 Software Safety Plan (Section D.4.4.1.9 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Software Safety Plan (SSP) for IOM and CSI in support of the PPS replacement project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.5.1 PG&E

PG&E will not develop software for the PPS replacement. Control of 10 CFR 50 Appendix B supplier software products while it is in PG&E's possession during the SAT and Design Verification Test are prescribed by the PG&E SyQAP and SVVP.

4.5.5.2 IOM

Triconex Document No. 993754-1-911, PPS Replacement DCPP SSP [72], meets the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and addresses the process and activities intended to improve software safety throughout the PPS software development lifecycle. The SSP for the

IOM portion of the PPS Replacement is written based on the guidance provided by ISG-6 [1], IEEE Standard 1228-1994 [138] and NUREG/CR-6101 [139].

4.5.5.3 CSI

CSI Document No. 6116-00000 Diablo Canyon PPS Management Plan Section 5.11 [60], meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and establishes the approach to addressing software safety in the FPGA design and test activities performed as part of the platform development and implementation for the PPS Replacement Project.

4.5.6 Software V&V Plan (Section D.4.4.1.10 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the SVVP for IOM, CSI and PG&E in support of the PPS Replacement Project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.6.1 PG&E

DCPP Project Procedure, System Verification and Validation Plan (SyVVP) for the PPS Replacement Project [53] meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the activities to be followed in the verification and validation for the PPS Replacement project, by PG&E, IOM and CSI.

The PG&E SCMP [159] has been developed to establish and document a process of change control and software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility and for the remainder of its life cycle following installation at DCPP, including the Operation Phase and Maintenance Phase. The change management process includes software changes and aspects of PPS replacement component configuration necessary to meet SDOE and cyber security requirements. Modification to the PPS Replacement components produced by the vendors, CS Innovations and Invensys Operations Management, will be performed by the vendors and verification and validation will be controlled by the vendor's verification and validation plans created for the PPS Replacement Project (CSI Document No. 6116-00003, "DCPP ALS V&V Plan," [54] for CS Innovations and Triconex Document No. 993754-1-802, "PPS Replacement DCPP SVVP" [73] for Invensys Operations Management).

4.5.6.2 IOM

Triconex Document No. 993754-1-802, PPS Replacement DCPP SVVP [73], meets the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and establishes the requirements for the V&V process to be applied to the TSAP software developed for the PPS Replacement Project, running on the safety-related V10 Tricon platform hardware. This SVVP also defines when, how, and by whom specific V&V activities are to be performed. The SVVP contains a IEEE-1012 compliance table to describe how IOM implements the criteria of the 1998 version of IEEE-1012.

For compliance with RG 1.168 [131], the PPS Replacement Triconex Document No. 993754-1-905, "PPS Replacement DCPP PMP" [69] and the SVVP [73] both describe the organizational structure and interfaces of the PPS Replacement Project. The documents describe the Invensys Operations Management Nuclear Delivery design team structure and responsibilities, the Nuclear IV&V team structure and responsibilities, the interfaces between Nuclear Delivery and Nuclear IV&V, lines of reporting, and degree of independence between Nuclear Delivery and Nuclear IV&V. In addition, the PMP [69] describes organizational boundaries between Invensys Operations Management and the other external entities involved in the PPS Replacement project: PG&E, Altran, Westinghouse, and Invensys Operations Management suppliers. The combination of the PMP [69] and SVVP [73] demonstrate compliance of the Invensys Operations Management organization with RG 1.168 [131].

4.5.6.3 CSI

CSI Document No. 6002-00003 DCPP ALS V&V Plan [54], meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the techniques, procedures, and methodologies that will be used by CSI to provide independent Verification and Validation (IV&V) in the design and test development of the ALS platform, and in particular in the FPGA design and test activities performed as part of the platform development and implementation for the PPS Replacement Project. The ALS V&V Plan, Appendix A Table A-1, contains a IEEE-1012 compliance table to describe how CSI implements the criteria of the 1998 version of IEEE-1012.

For compliance with RG 1.168 [131], the CS Innovations 6116-00000, "Diablo Canyon PPS Management Plan" [60] includes details on how the IV&V team has an independent organizational reporting structure from the design and implementation team. The IV&V team that has an independent organizational reporting structure from the design and implementation team.

4.5.7 SCMP (Section D.4.4.1.11 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the SCMP for IOM and CSI in support of the PPS Replacement Project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.7.1 PG&E

DCPP Procedure CF2.ID2, Software Configuration Management for Plant Operations and Operations Support [50], meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines the activities to be followed in the Operations and Operations Support software configuration management.

PG&E document SCM 36-01, "Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Software Configuration Management Plan (SCMP)" [159] has been developed using DCPP Procedure CF2.ID2 to establish and document a process of change control and for software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility and for the remainder of its life cycle following installation at DCPP. The change management process includes software changes and aspects of PPS replacement component configuration necessary to meet SDOE and cyber security requirements. Document SCM 36-01 addresses in part ISG-06, Enclosure B, Item 1.10, Software Configuration Management Plan.

4.5.7.2 IOM

Triconex Document No. 993754-1-909, PPS Replacement DCPP CMP [77], meets the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136]. This CMP defines how Software Configuration Management is to be applied within the IOM scope according to RG1.169 132] which endorses IEEE Standard 828-1998 [140]. IEEE Standard 828-1998 (Standard for Software Configuration Management Plans) establishes the minimum required content of the SCMP. These standards are supplemented by IEEE Standard 1042-1998 [141] that provides approaches to good software configuration management planning.

4.5.7.3 CSI

CSI Document No. 6002-00002 ALS CMP [66], meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and describes the Configuration Management organization and practices used for baseline control of ALS related configuration items.

PG&E will not have the capability to alter the ALS FPGA or the nonvolatile RAM (NVRAM) configuration itself. Therefore, any change to the ALS FPGA must be made by CS Innovations, including the ALS-102 board configured specifically for PG&E, and the ALS-102 FPGA configuration management activities are covered by the ALS CMP [66]. PG&E capability to change an ALS board configuration, including the ALS-102 board, is limited to board-level replacement.

PGE will have limited capability to change the NVRAM configuration for a specific ALS I/O board to support board replacement (such as to replace a failed board) by loading NVRAM images that are under CS Innovations configuration control and that have been previously verified and validated at the system level by CS Innovations. Configuring the NVRAM in order to replace an ALS I/O board will be performed by PG&E under an approved plant maintenance procedure.

4.5.8 Software Test Plan (Section D.4.4.1.12 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Software Test Plan (STP) for IOM and CSI in support of the PPS Replacement Project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.8.1 IOM

Triconex Document No. 993754-1-813, PPS Replacement DCPP STP [74], meets the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” [136]. This STP defines the scope, approach, and resources of the testing activities that are required to be performed for the V10 Tricon portion of the DCPP PPS replacement to support the following:

- To detail the activities required to prepare for and conduct the system integration tests.
- To identify the tasks for responsible teams to perform and the schedule to be followed in performing the tasks.
- To define the sources of the information used to prepare the plan.
- To define the test tools and environment needed to conduct the system test.

4.5.8.2 CSI

CSI Document No. 6116-00005 DCPP PPS System Test Plan [67], meets the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power

Plants," [136] and covers the design verification, acceptance and release testing of the ALS portion of the PPS Replacement Project.

4.5.9 Software Requirement Specification (Section D.4.4.3.1 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the SRS for IOM and CSI in support of the PPS replacement project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

These are developed based on the owner requirements identified in the following PG&E Documents:

- DCPP Units 1 & 2 PPS Replacement FRS [28]
- DCPP Units 1 & 2 PPS Replacement Interface Requirements Specification [29]

4.5.9.1 IOM

Triconex has developed the SRS for the PPS Replacement Project in four documents, with one applicable to each Protection Set as follows:

- Triconex Document No. 993754-11-809, PPS Replacement DCPP SRS Protection Set I [75]
- Triconex Document No. 993754-12-809, PPS Replacement DCPP SRS Protection Set II [75]
- Triconex Document No. 993754-13-809, PPS Replacement DCPP SRS Protection Set III [75]
- Triconex Document No. 993754-14-809, PPS Replacement DCPP SRS Protection Set IV [75]

Each of these documents meet the guidance of BTP 7-14 Section B 3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136] and defines how the conformed software design specifications (SDS) are to be satisfied by the project-specific design for the IOM scope of supply in the PPS Replacement Project. Each of these documents meets the guidance provided in NRC RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [135] which endorses IEEE Standard 830-1993, "IEEE Recommended Practice for Software Requirements Specifications." [143]

Each SRS address the following for the associated Protection Set:

- Functionality to describe what the software is supposed to do
- External interfaces to describe how the software interacts with people, the system's hardware, other hardware, and other software
- Performance in describing the speed, availability, response time, and recovery time of the software functions
- Attributes. What are the portability, correctness, maintainability, security, etc.
- Design constraints imposed on an implementation listing any required standards in effect, implementation language, policies for database integrity, resource limits, or operating environment(s).

4.5.9.2 Westinghouse/CSI

Westinghouse/CSI has developed the SRS documentation for both the platform and also for the specific PPS Replacement Project requirements as follows:

- CSI Document No. 6002-00010, ALS Platform Requirements Specification, R7 [68]
- Westinghouse Document No. WNA-DS-02442-PGE, Revision 2, ALS System Requirements Specification [17]

Each of these documents meet the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136]. Each of these documents meets the guidance provided in NRC RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [135] which endorses IEEE Standard 830-1993, "IEEE Recommended Practice for Software Requirements Specifications" [143].

CSI Document No. 6002-00010, ALS Platform Requirements Specification [68], establishes the performance, design, manufacture, test and acceptance requirements for the ALS platform in support of the ALS Topical Report Submittal [15] submitted to the NRC.

Westinghouse ALS System Requirements Specification [17], establishes the specific performance, design, manufacture, test and acceptance requirements for the DCPP Replacement Project using the ALS platform. It identifies design and test requirements and criteria and references functional requirements which are applicable to the system design. It also provides requirements for functional features, defines normal and abnormal plant conditions during which the ALS must operate, and identifies applicable QA and verification and validation programs.

4.5.10 Software Design Specification (Section D.4.4.3 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the SDS for IOM and CSI in support of the PPS replacement project and complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.1 and BTP-7-14 [4], are described in the following sections.

4.5.10.1 IOM

In the IOM software development process, the SRS is equivalent to the Software Design Description (SDD) in DI&C-ISG-06 [1] Section D.4.4.3.3.

The SRS for the PPS Replacement Project is made up of four documents, with one applicable to each Protection Set as follows:

- Triconex Document No. 993754-11-809, PPS Replacement DCPP SRS Protection Set I [75]
- Triconex Document No. 993754-12-809, PPS Replacement DCPP SRS Protection Set II [75]
- Triconex Document No. 993754-13-809, PPS Replacement DCPP SRS Protection Set III [75]
- Triconex Document No. 993754-14-809, PPS Replacement DCPP SRS Protection Set IV [75]

The SDD for the IOM scope of the PPS Replacement Project will be submitted to the NRC for review in Phase 2.

4.5.10.2 CSI

CSI has developed the System Design Specification documentation for both the platform and also for the specific PPS Replacement Project requirements as follows:

- CSI Document No. 6002-00011, ALS Platform Specification [95]
- CSI Document No. 6116-00011, DCPP PPS ALS System Design Specification [19]

Each of these documents meet the guidance of BTP 7-14 Section B3.1.3 [4] and NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [136]. Each of these documents meets the guidance provided in NRC RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," [135] which endorses IEEE Standard 830-1993, "IEEE Recommended Practice for Software Requirements Specifications" [143].

CSI Document No. 6002-00011, ALS Platform Specification [95], is the highest level specification for the ALS platform and describes the general philosophy and functionality in support of the ALS Topical Report Submittal [15].

CSI Document No. 6116-00011, DCPP PPS ALS System Design Specification [19], provides the specification for the ALS component as part of the PPS Replacement Project. CSI is responsible for the ALS subsystem portion of the PPS system for Protection Sets 1-4. The ALS PPS subsystem includes ALS chassis hardware, ALS I/O cards (A & B), ALS CLBs with programmed functional logic (A & B), MWS software, standard cabling for terminating to ALS I/O boards, and logic validation and testing to verify the Protection Set safety functions.

4.6 Environmental Equipment Qualification (Section D.5.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.4 states:

Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.

Refer to Section 4.11.1.2 of this Enclosure for details regarding compliance with the additional requirements of IEEE Standard 7-4.3.2-2003 [80].

To address environmental factors, the physical requirements for the DCPP PPS replacement equipment are specified to the vendors in Section 3.1 of the DCPP FRS [28]. Physical requirements specified include temperature, relative humidity, pressure, radiation, seismic, electromagnetic capability, and emissions. The CS Innovations and Invensys Operations Management vendors are required to confirm the equipment meets the physical requirements in the DCPP FRS [28]. The vendors requirements traceability matrix (RTM) documents contain the basis for how the equipment meets the physical requirements in the DCPP FRS [28] in accordance with ISG-06.

4.6.1 Triconex Qualification

The Tricon portion of the PPS replacement incorporates the standard Tricon platform described in the Triconex Tricon V10 Topical Report Submittal [13], which was submitted to the NRC on May 15, 2012.

Section 2 of the Tricon V10 Topical Report [13] for the Tricon provides a summary of the equipment testing and analysis performed to meet the requirements of IEEE 603-1991 [21], IEEE Standard 323-1983 [65], EPRI TR-107330 [81], EPRI TR-102323 Revision 1 [79] and RG 1.180 Revision 1 [23]. This report addresses the specific required environmental conditions and testing/analysis performed to qualify this equipment. This testing/analysis confirmed that the Tricon safety system is fully qualified and capable of performing its designated safety functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions, as required.

Analysis of all components being installed as part of the Tricon portion of the PPS replacement to PG&E Environmental Quality (EQ) requirements will be provided in Phase 2.

4.6.2 ALS Qualification

The ALS portion of the PPS replacement incorporates the standard ALS platform described in the ALS Topical Report Submittal [15].

The ALS Topical Report Submittal Section 4 [15], for the ALS platform provides a summary of the equipment testing and analysis performed to meet the requirements of IEEE 603-1991, IEEE Standard 323-1983 [65], EPRI TR-107330, EPRI TR-102323 Revision 1 [79] and RG 1.180 Revision 1 [23]. This report addresses the specific required environmental conditions and testing/analysis performed to qualify this equipment. This testing/analysis confirmed that the ALS safety system is fully qualified and capable of performing its designated safety functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions, as required.

Analysis of all components being installed as part of the ALS portion of the PPS replacement to PG&E EQ requirements will be provided in Phase 2.

4.6.3 Ancillary Safety-Related Equipment Utilized In the PPS Replacement Project

Components that were not included in either the Triconex or ALS qualification testing program but are utilized in the PPS replacement were either purchased as 1E or qualified in accordance with the DCPP QAP [142], regulatory requirements, and standards provided by EPRI TR-107330 [122], RG. 1.180 R1 [23], 10 CFR 50 Appendix B [151], RG 1.100 Revision 2 [118], IEEE Standard 344-1975, IEEE Standard 381-1977, and Section 5.4 of IEEE Standard 603-1991 [21]. This equipment includes, but is not limited to:

- Rack power supplies
- Isolators
- Bypass switches
- Trip switches
- Termination modules
- Fuses

4.7 Defense-in-Depth & Diversity (Section D.6 of DI&C-ISG-06 [1])

The PPS replacement was designed to address diversity through use of Tricon and ALS subsystems and the diversity provided by the existing NIS, Class II contacts, and AMSAC.

PG&E submitted the D3 topical report for the PPS replacement to the NRC for approval ([6], ADAMS Accession No. ML102580726) and the NRC has issued a SER for the D3 topical report ([7], ADAMS Accession No. ML110480845). The staff evaluated the PPS replacement D3 topical report in accordance with the guidance in NUREG-0800 [4], BTP 7-19, "Guidance for Evaluation of D3 in Digital Computer Based Instrumentation and Control Systems," Revision 5, March 2007, as well as the supplemental guidance provided by DI&C-ISG-02, "Task Working Group #2: D3 Issues, Interim Staff Guidance," Revision 2, dated June 5,2009 ([3], ADAMS Accession No. ML091590268). The SER for the D3 topical report concluded that the PPS replacement changes will not adversely impact the safety determination that was made for the Eagle 21 digital PPS and that there is adequate D3 within the PPS replacement such that plant responses to the design basis events concurrent with potential software CCF meet the acceptance criteria specified in BTP 7-19 [4].

In the SER for the D3 topical report, for NRC Staff Position 4, “Effects of CCF,” in DI&C-ISG-02, the staff stated partial losses of the Tricon and the ALS portions of the PPS due to software CCF was not addressed, and therefore, the licensee will be required to develop and submit a FMEA Analysis to address this issue. The FMEA for the Tricon and ALS is addressed in Section 4.10.2.1.1.

In the SER for the D3 topical report, for NRC Staff Position 7, “Single Failure,” in DI&C-ISG-02 [3], the staff stated because the PPS system design was not complete, it was not possible for the NRC staff to confirm that the documented basis for diversity is included in the overall system design. The single failure evaluation for the Tricon and ALS is addressed in Section 4.10.2.1. In the SER for the D3 topical report, for NRC Staff Position 7, “Single Failure,” the staff also stated the displays and controls used should be independent and diverse from the computer-based PPS system. The information displays are addressed in Section 4.10.2.8 and the independence of the design is addressed in Section 4.10.2.6.

The Tricon portion of the PPS replacement uses the same processors, programming language and function blocks within redundant Protection Sets. However, the redundant Protection Set application programs are different from each other in the same manner that the Eagle 21 application programs in different redundant Protection Sets are different from each other.

Safety-related information (i.e., Pressurizer vapor space and RCS narrow and wide range temperature) transmitted from the logic-based ALS to the software-based Tricon is via analog signals. There is no communication of safety-related information from the software-based Tricon to the logic-based ALS. There is no software-based communication between or among redundant or diverse Protection Sets. No database information or equipment that uses software is shared between the Tricon and the diverse ALS or between redundant Protection Sets within Tricon or ALS portions of the replacement PPS.

Concern for ALS software CCF is addressed through incorporating additional design diversity in the FPGA-based hardware system as described in Section 4.1.1 and using qualified design practices and methodologies to develop and implement the hardware as described in Section 4.2.

As documented in the PPS replacement D3 topical report and determined by the D3 SER [7], the diverse ALS cannot be affected by a software CCF that affects the Tricon. The PPS replacement provides sufficient design diversity to automatically mitigate the DCPP FSAR [26] Chapter 15 events should a software CCF occur in the PPS replacement concurrent with the event. The ability of the ALS portion of the PPS to perform credited automatic protective functions is not adversely affected by a software CCF as described in Section 3 of the ALS Diversity Analysis [16] and Section 9 of the CSI Topical Report Submittal [15].

As shown in Figure 4-7, the ALS provides Class IE signal conditioning for the Pressurizer Vapor Space temperature, RCS wide range temperature and narrow range RTD inputs to the OPDT and OTDT thermal trip functions. These temperature signals are passed from the ALS to the Tricon for processing by the Tricon portion of the PPS replacement. The NIS provides diverse automatic protection should a failure in either the ALS or Tricon disable the OPDT and OTDT trip functions.

The Tricon-based portion of the PPS replacement shares the Pressurizer Pressure analog signals with the ALS portion of the PPS replacement. The shared signals are not processed by software upstream of either the Tricon or ALS. The Pressurizer Pressure signal is used by the ALS to generate the diverse Pressurizer pressure-high and -low trips and the pressure-low safeguards functions. It is also used in the Tricon to calculate the OPDT and OTDT trip setpoints. Since the signal is shared at the transmitter (4-20 mA analog) output, a failure in either ALS or Tricon cannot affect the other subsystem. AMSAC shares steam generator level and turbine impulse pressure with the Tricon. The signals are shared at the transmitter (4-20 mA analog) outputs and isolated to meet 10 CFR 50.62 [22] diversity requirements. A Tricon failure cannot affect the AMSAC and an AMSAC failure cannot affect the Tricon. Each ALS instrument channel retains its identity from sensor through processing to coincident logic. Isolated signals from the ALS to other systems are analog.

The NRC SER determined that the design addresses Staff Position 1 of ISG-02 [3] adequately.

Thus, the replacement PPS:

1. Replaces the entire Eagle 21 PPS with a system that is Class 1E, nuclear safety-related and which automatically performs all the automatic protection functions approved by NRC in the SER for the Eagle 21 PPS [7].

2. Provides Class IE safety-related automatic mitigation functions, which address CCF as described in the previously approved DCPP D3 Analysis [6], where previous evaluations relied upon manual operator action to mitigate events that occurred with a concurrent postulated CCF to the PPS.

3. Provides an architecture in which a CCF in the software-based TRICON portion of the replacement PPS cannot adversely affect the safety function of the logic-based ALS.

4. Provides an architecture in which a single failure of the diverse ALS cannot adversely affect the safety function of the TRICON.

5. Provides an architecture in which failure of either the Tricon or the ALS cannot adversely affect the ability of the operator to initiate RT or ESFAS functions.

4.8 Communications (Section D.7 of DI&C-ISG-06 [1])

The DI&C-ISG-04, Task Working Group #4, Highly Integrated Control Rooms – Communications Issues (HICRs) [2] has provided ISG on the review of communications issues. DI&C ISG-04 [2] contains three sections: (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations.

Sections 4.8.1 through 4.8.20 of this enclosure provide details of the PPS replacement compliance to ISG-04 for interdivisional communications. Figures 4-12 and 4-13 in Section 4.2.13 of this enclosure provide additional detail for interconnections of the PPS replacement communications architecture.

Command Prioritization and Multidivisional Control and Display Stations are not applicable to the PPS replacement.

4.8.1 ISG-04 Interdivisional Communications Staff Position No. 1

ISG-04 Interdivisional Communications, Staff Position No. 1 States:

A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE 603. It is recognized that division voting logic must receive inputs from multiple safety divisions.

The PPS replacement conforms to this Staff Position.

The PPS replacement consists of four (4) Protection Sets with architecture such that each safety channel within a given Protection Set is not dependent upon any information or resource originating outside the Protection Set which the channel is a member. The details for the Tricon and ALS conformance to this staff position No. 1 are provided in the sections below.

a) Tricon-Based PPS Equipment

The Tricon portion of the PPS replacement architecture does not depend on any information or resource originating or residing outside its own Protection Set to accomplish its safety function because the Tricon does not receive any information originating or residing outside its own Protection Set while online and performing its safety function. Each PPS division sends data from the safety TCM to the non-safety MWS within the division, and through a dedicated one-way NetOptics port aggregator network tap [Section 4.2.13] of this LAR, to the common Gateway Network Switch. The only time data is allowed to be received by the TCM is when the channel is out of service. The channel is taken out of service by taking multiple deliberate actions: 1) activating a safety-related hardware out of service switch locked in a cabinet and 2) activating a software switch on the Workstation requiring password access. The sensors connected to the Tricon are dedicated sensors and operate completely independent of other Tricon divisions. The Protection Set architecture includes a Remote RXM non-safety chassis which provides outputs to non-safety indicators and alarms. Further technical detail on the V10 Tricon, including RXM isolation functions, can be found in the NTX-SER-09-10, Tricon Applications in Nuclear RPSs - Compliance with NRC ISG-2 & ISG-4 [24].

b) FPGA-Based ALS Equipment

The ALS portion of the PPS replacement does not depend on any information or resource originating outside its own Protection Set to accomplish its safety function because the ALS does not receive any information originating or residing outside its own Protection Set while online and performing its safety function. The ALS inputs, conditioning and outputs do not depend on data/information from any divisional input outside its own division. Further technical detail regarding the conformance of the ALS platform to ISG-04 Interdivisional Communication staff position No. 1 is located in Section 2.2 of CSI Document No. 6116-00054, Revision 0, "Diablo Canyon Process Protection System ISG-04 Matrix" [165].

4.8.2 ISG-04 Interdivisional Communications Staff Position No. 2

ISG-04 Interdivisional Communications, Staff Position No. 2 states:

The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

The PPS replacement conforms to this Staff Position.

The PPS replacement consists of four (4) Protection Sets and is architected such that each safety channel within a given Protection Set is protected from adverse influence from outside the Protection Set which the channel is a member. The details for the Tricon and ALS conformance to this staff position No. 2 are provided in the sections below.

a) Tricon-Based PPS Equipment

The Tricon portion of the PPS replacement is protected from adverse influence from outside its own division by the TCM and the Primary RXM Chassis. Design of the system precludes dependence on any information or resource originating outside its own Protection Set.

Section 5, Staff position No. 2 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25] provides additional details regarding the conformance of the Tricon portion of the PPS replacement to ISG-04 Interdivisional Communication Staff Position No. 2. Further details regarding the conformance of the Tricon platform to ISG-04 Interdivisional Communication staff position No. 2 are located in section 5, Staff position No. 2 of NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24].

b) FPGA-Based ALS PPS Equipment

The ALS portion of the PPS replacement is protected from adverse influence from outside its own division. This is accomplished by the design on the communications interface of the ALS. The ALS portion of the PPS replacement has no continuous two-way communication signals outside the division. The connection to the non-safety ALS MWS is normally a one-way transmit only from the ALS via a serial data stream from the TxB2. The receive capabilities of the TxB channels on the ALS-102 CLB are physically disabled by hardware on the ALS board. The receive lines on the TxB channels of the ALS-102 are not externalized to any connector and are instead terminated as described in the 6002-10202 ALS-102 Design Specification [94].

Two-way communications via the TAB is permitted only when the TAB communication link is physically connected between the TAB and the ALS MWS. The two-way communications is provided via the TAB, as described in Section 5.2 of the ALS Platform Specification [95]. Communications are not possible on the TAB if the communication link is physically disconnected. As explained in Section 2.2 of the ALS Platform Specification [95], the Protection Set containing the ALS chassis with TAB communications enabled remains functional during this action. All other communication to non-safety equipment, i.e., Plant Computer, is via continuous one-way communication channels on the ALS-102. Further technical detail regarding the conformance of the ALS platform to ISG-04 Interdivisional Communication staff position No. 2 is located in section 2.2 of CSI Document No. 6116-00054, Revision 0, "Diablo Canyon Process Protection System ISG-04 Matrix" [165].

4.8.3 ISG-04 Interdivisional Communications Staff Position No. 3

ISG-04 Interdivisional Communications, Staff Position No. 3 States:

A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.

The PPS replacement conforms to this Staff Position.

The PPS replacement consists of four (4) Protection Sets and is architected such that each safety channel within a given Protection Set is protected from adverse influence from outside the Protection Set which the channel is a member. The details for the Tricon and ALS conformance to this staff position No. 3 are provided in the sections below.

a) Tricon-Based PPS Equipment

The Tricon portion of the PPS replacement does not receive any communication from outside its own division. Each PPS division sends data from the safety TCM to the non-safety MWS within the division, and through a dedicated one-way NetOptics port aggregator network tap [Section 4.2.13] of this LAR, to the common Gateway Switch. The only time data is allowed to be received by the TCM is when the channel is out of service. The channel is taken out of service by taking multiple deliberate actions: 1) activating a safety-related hardware out of service switch locked in a cabinet and 2) activating a software switch on the Workstation requiring password access. This added complexity is justified due to the added safety obtained by testing in bypass mode. The sensors connected to the Tricon are dedicated sensors and operate completely independent of other Tricon Protection Sets. There is no data exchange between RXM chassis in different Protection Sets. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 3 can be found in section 5, Point No. 3 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

Further technical detail on the Remote RXM non-safety chassis can be found in the Appendix 2 NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24].

b) FPGA-Based ALS PPS Equipment

The ALS portion of the PPS replacement does not receive any communication from outside its own division. The ALS platform does not make any comparisons of information between divisions including the sensors. All communication from the ALS chassis to non-safety related equipment is via transmit only one way communication with the exception of the normally disconnected TAB connection to the non-safety ALS MWS for the associated Protection Set. The receive capabilities of the TxB channels on the ALS-102 CLB are physically disabled by hardware on the ALS board. The receive lines on the TxB channels of the ALS-102 are not externalized to any connector and are instead terminated as described in the 6002-10202 ALS-102 Design Specification [94].

The ALS MWS is used for changing certain plant parameters such as setpoints during surveillance and maintenance. This communication is enabled through physical connection of the communication link from the TAB on the ALS chassis to the ALS MSW during bypass conditions. The TAB communication is enabled through the use of the TAB access connector. Activation of the TAB access is alarmed both locally and in the control room. Further details regarding the MWS interface to the ALS and the separation of the RAB and TAB, and conformance of the ALS platform to ISG-04 Interdivisional Communication staff position No. 3 is located in section 2.2 of CSI Document No. 6116-00054, Revision 0, "Diablo Canyon Process Protection System ISG-04 Matrix" [165].

4.8.4 ISG-04 Interdivisional Communications Staff Position No. 4

ISG-04 Interdivisional Communications, Staff Position No. 4 States:

The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

The PPS replacement conforms to this Staff Position.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement, communication with external devices is conducted and supervised by the TCM. The TCM operate asynchronously, sharing information only at end of the application processor scan. The TCM and the application processor are bridged with DPRAM. The DPRAM prevents direct communication between the application processor and the TCM interface with the MWS. When the host device requests data, the communication processor forwards the data from the application processor that was received at end of the previous scan. When a host device writes data, the communication processor passes the data to the application processor at next end of scan exchange. If there are any remaining communications tasks to be performed they are communicated in the next scan cycle(s). Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 4 can be found in section 5, Point No. 4 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

The ALS does not contain processors. Instead, it contains FPGAs which are firmware based. The communication hardware is located on the CLB. Further details regarding the FPGA-based communication hardware are provided in section 5, Table 5-2, Item 4 of the ALS Topical Report Submittal [15].

The ALS PPS subsystem contains three communication types: RAB, TAB, and Transmit Bus (TxB1/TxB2). The RAB is used for all data transfers between ALS boards. Communication related to performing the ALS PPS safety function is performed using the RAB. The TAB is bidirectional, when physically connected and enabled, and is used for diagnostics, calibration and system information gathering. The TAB is only connected and enabled during surveillance testing and maintenance periods via the ALS MWS. The TxB1/TxB2 transmit buses reside on the ALS-102 CLB only. The TxB1/TxB2 buses are used for sending ALS status information to remote computers or data loggers. The CLB communication functions for the TxB1/TxB2 and TAB are accomplished by logic that is independent from the FPGA logic performing the safety logic function via the RAB. The ALS-102 CLB uses dedicated logic to handle TxB1/TxB2 and TAB communications that is separate from the logic that is used to handle RAB communications and to perform the ALS PPS safety function. This prevents communication errors and malfunctions from interfering with the execution of the safety function. The ALS uses different registers (i.e., not shared) for separating communication functions. TxB1/TxB2 communications are controlled and sequenced through communication channel registers. The PPS safety logic is sequenced on separate registers and transmitted on separate buses. Further technical detail regarding the conformance of the ALS platform to ISG-04 Interdivisional Communication staff position No. 4 is located in Section 2.2 of CSI Document No. 6116-00054, Revision 0, "Diablo Canyon Process Protection System ISG-04 Matrix" [165].

4.8.5 ISG-04 Interdivisional Communications Staff Position No. 5

ISG-04 Interdivisional Communications, Staff Position No. 5 States:

The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for *the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.*

The PPS replacement conforms to this Staff Position.

The PPS Replacement does not utilize communications among the four Protection Sets (i.e., interdivisional communications). The details for the Tricon and ALS conformance to this staff position No. 5 are provided in the sections below.

a) Tricon-Based PPS Equipment

The application processors and the IOCCOM process operate asynchronously . Communication between the two processors takes place via DPRAM. The DPRAM prevents reads or writes from the IOCCOM communication processor from delaying access to the DPRAM by the safety processors. Similarly, the application processors and the TCM also communicate via DPRAM. The DPRAM prevents reads or writes from the TCM communication processor from delaying access to the DPRAM by the safety processors.

Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 5 can be found in section 5, Point No. 5 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

The ALS does not use processors and, therefore, the access time of memory is not a consideration with the FPGA design. The response time for the ALS platform is deterministic and variances are accounted for during the design phase. The cycle time of the ALS platform is set to be less than or equal to the required plant response time to account for the longest possible delay associated with the function of the ALS platform. This is verified during factory acceptance testing. Further details regarding the FPGA-based communication hardware is provided in section 5, Table 5.3-1 of the ALS Topical Report Submittal [15].

4.8.6 ISG-04 Interdivisional Communications Staff Position No. 6

ISG-04 Interdivisional Communications, Staff Position No. 6 States:

The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

The PPS replacement conforms to this Staff Position.

a) Tricon-Based PPS Equipment

The safety function processors do not perform any communications tasks as these tasks are handled by the TCM processor and the RXM processors. (IOCCOM). The safety function processors do not perform any communication handshaking and do not accept any interrupts from outside their own safety division.

Tricon controllers are not dependent upon interdivisional communications or external systems to perform the safety function. This would include interrupts from external systems. The Tricon application processors are isolated from non-safety I/O data communications by the combination of the DPRAM, the IOCCOM, and the safety-related Primary RXM. There is no handshaking on the I/O bus.

Further information can be found in NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24].

b) FPGA-Based ALS PPS Equipment

The ALS does not use a processor and the ALS subsystem in each Protection Set does not communicate with the ALS subsystem in the other three Protection Sets. Communication related to performing the ALS PPS safety function is carried out using the RAB. RAB communications between boards in the ALS PPS subsystem are deterministic and do not perform communication handshaking, nor do they accept any interrupts.

The ALS-102 CLB TxB1/TxB2 communication functions are one-way, transmit only, and do not perform communication handshaking, nor do they accept any interrupts from any communication devices.

The TAB is bidirectional and used for diagnostics, calibration and system information gathering. The TAB is only connected to the ALS MWS and enabled during surveillance testing and maintenance when the ALS subsystem instrument channel is declared out of service,

4.8.7 ISG-04 Interdivisional Communications Staff Position No. 7

ISG-04 Interdivisional Communications, Staff Position No. 7 States:

Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

The PPS replacement conforms to this Staff Position.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement all host communications are limited to Tricon-compatible protocols. Each protocol is well-defined and well-ordered, e.g., number of start and stop bits, timing, data frame format, number of data fields, and check sum or CRC field. Should an error occur, the communication processor rejects the message.

Data sets are pre-defined by the request sent by the receiving system; therefore, message length may vary, as a host device may request a different number of data points within each request. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 7 can be found in section 5, Point No. 7 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25]. Further details regarding the Tricon compatible protocols are provided in section 4 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

Further information can be found in NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement the ALS-102 CLB validates the data being received. With this validation unrecognized messages are not accepted or used. All ALS data is transmitted at each cycle whether changes have occurred or not. No handshaking is required by the ALS-102.

The ALS-102 TxB1/TxB2 communication functions are one-way, transmit only. The TxB receive channels on the ALS-102 CLB are physically disabled by hardware on the ALS board, therefore data is not accepted in the TxB1/TxB2 communication path. Further details regarding the FPGA-based communication hardware is provided in section 5 of the ALS Topical Report Submittal [15].

4.8.8 ISG-04 Interdivisional Communications Staff Position No. 8

ISG-04 Interdivisional Communications, Staff Position No. 8 States:

Data exchanged between redundant safety divisions or between safety and non-safety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

The PPS replacement conforms to this Staff Position.

The PPS replacement architecture does not perform data exchange between redundant safety divisions. Data exchange between safety and non-safety divisions are discussed in Sections 4.8.8.a and 4.8.8.b. The details for the Tricon and ALS conformance to this staff position No. 8 are provided in the sections below.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement the data communications with non-safety systems such as the MWS are handled by the TCM. The non-safety system may request data points, and the TCM replies if the request is valid and error free.

The TCM accepts data "writes" from the non-safety system to the Tricon only if:

- The data is valid and error free;
- The Tricon keyswitch is in the correct position; and
- The specific memory tag name attribute is configured as 'writeable'.

If the Tricon keyswitch is not in the RUN position, an alarm is initiated on the Control Room MAS and the Tricon is considered inoperable.

Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 8 can be found in section 5, Point No. 8 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement the TAB is used for communication of information to and from the ALS chassis and the non-safety MWS. This communication process is independent from the safety function logic. To enable the TAB to the interface to the MWS requires the setting of a hardware key-lock switch which, when enabled, is alarmed locally and in the control room. This process is done while in the bypass mode under plant administrative controls. The TAB and its interfaces are designed such the buses are nonintrusive in that the bus cannot interfere with processing of any information or data on the RAB.

The ALS-102 TxB communication channels provide safety information to the non-safety related plant computer. This communication path is one way and isolated from the safety related ALS Platform. The receive capabilities of the TxB channels on the ALS-102 are physically disabled by hardware on the ALS board, therefore incoming data is not accepted in the TxB1/TxB2 communication path. The receive lines on the TxB channels of the ALS-102 are not externalized to any connector and are instead terminated as described in the 6002-10202 ALS-102 Design Specification [94]. The communication logic is independent from the ALS-102 safety function logic and, as a result, cannot adversely affect the safety function of the transmitting division as described in Section 2.2 of CSI Document No. 6002-00011, "ALS Platform

Specification" [95]. Further details regarding the ALS communication with a non-safety MWS is provided in section 5 of the ALS Topical Report Submittal [15].

4.8.9 ISG-04 Interdivisional Communications Staff Position No. 9

ISG-04 Interdivisional Communications, Staff Position No. 9 States:

Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

The PPS replacement conforms to this Staff Position.

a) Tricon-Based PPS Equipment

Tricon received data is stored in fixed memory locations, which are utilized by the application processor when executing application logic. Input data is segregated from output data within memory. All communication messages are conducted by and stored in separate communication processors. Data is exchanged with the application processors at the end of each application program scan. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 9 can be found in Section 5, Point No. 9 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

The FPGA architecture does not utilize the architecture guidance given in this criterion since processors are not part of the design. However, for the ALS, messages are stored in two distinct buffer areas for receive and transmit data. These areas are allocated in the FPGA, according to the configuration of the ALS design. Further details regarding the ALS communication messages and memory organization are provided in section 5.6 of 6002-00011 ALS Specification [95] and the memory organization for the PPS replacement ALS subsystem is found in CSI Document No. 6116-10201, "Diablo Canyon Units 1 and 2 Process Protection System, ALS-102 FPGA Requirements Specification" [20].

4.8.10 ISG-04 Interdivisional Communications Staff Position No. 10

ISG-04 Interdivisional Communications, Staff Position No. 10 States:

Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

For the PPS replacement architecture there are four MWS (total of eight) for each ALS and Tricon subsystem. One MWS is dedicated to each subsystem in its own Protection Set. A MWS within a given Protection Set cannot communicate with or modify a MWS from another Protection Set.

The PG&E PPS Replacement design does not fully meet Position 10 but justification to an alternative to Position 10 is provided and is based on the combination of redundancy within the Tricon subsystem and both redundancy and diversity in the ALS subsystem, along with conservative administrative controls. Work may be performed on the Tricon portion of a Protection Set (safety division) without affecting operability of the ALS portion of the safety division, and work may be performed on one safety function within one ALS subsystem (chassis) without affecting the operability of the other safety functions within the ALS subsystem or the Tricon in that Protection Set.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement there are several layers of protection to prevent inadvertent application program changes. These include the Tricon keyswitch.

Additional reliability gains are realized by the TCM design itself (reliable design) and configuration features to prevent access from unknown network nodes. Additional protection is provided by features in the TriStation 1131 programming interface, including password access.

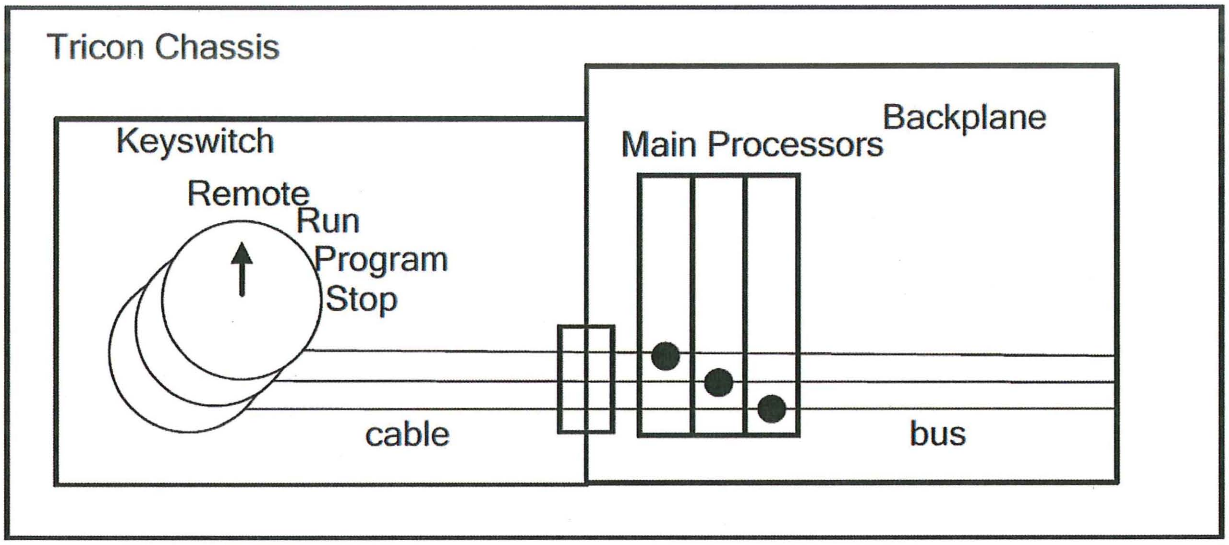
The Tricon keyswitch is a physical interlock that controls the mode of the 3008N MPs. It prevents the 3008N MPs from accepting “write” messages when placed in the RUN position. The Tricon keyswitch is implemented by a three-gang, four-position switch. Each of the gangs is connected to one of the 3008N MPs. The Tricon keyswitch position is voted between the three 3008N MPs and the voted value is used to perform keyswitch functions.

The Tricon keyswitch design mitigates against any single hardware fault. If one of the gangs on the switch goes bad or an input to a 3008N MP fails (e.g., a single bit flip), the error would affect only the 3008N MPP that is attached to the failed gang. The other two 3008N MPs would continue to receive good input values and out vote the 3008N MP with the bad input. This protects against any single fault in the Tricon keyswitch or on the 3008N MP.

The TCM and the application processors communicate via DPRAM. The DPRAM prevents reads or writes from the TCM communication processor from delaying access to the DPRAM by the safety processors.

The Tricon replacement design does not fully meet Position 10 but justification to an alternative to Position 10 is provided and is based on the combination of redundancy within the Tricon subsystem, along with conservative administrative controls. Position 10 states in part that provisions that rely on software to effect the disconnection of maintenance and monitoring equipment are not acceptable. The deviation to this postion is that the Tricon keyswitch relies on software to effect the disconnection of the TriStation capability to modify the safety system software. However, the use of the Tricon keyswitch is acceptable for the PPS replacement design since failure of the Tricon keyswitch will not prevent performance of the PPS safety function. There is no credible single failure on the V10 Tricon that would allow the safety-related application program to be inadvertently programmed (e.g., as a result of unexpected operation of the connected MWS with TS1131 installed on it).

A Tricon keyswitch on the main chassis selects the operating mode of the Tricon. The Tricon keyswitch is implemented with a three-gang switch and each of the gangs is connected to one of the Tricon 3008N MPs as represented in the diagram below:



The values are read by each of the main processors as a two bit value based on position as follows:

Position	Value
Stop	0
Program	1
Run	2
Remote	3

The Tricon keyswitch position is voted among the three MPs and the voted value is used to perform Tricon keyswitch functions. The Tricon application program has access to the voted Tricon keyswitch position and can perform a specified action depending on the position of the Tricon keyswitch. For example, the PPS Replacement application program is designed to provide an alarm output to the Main Annunciator System when the Tricon keyswitch position is not in RUN.

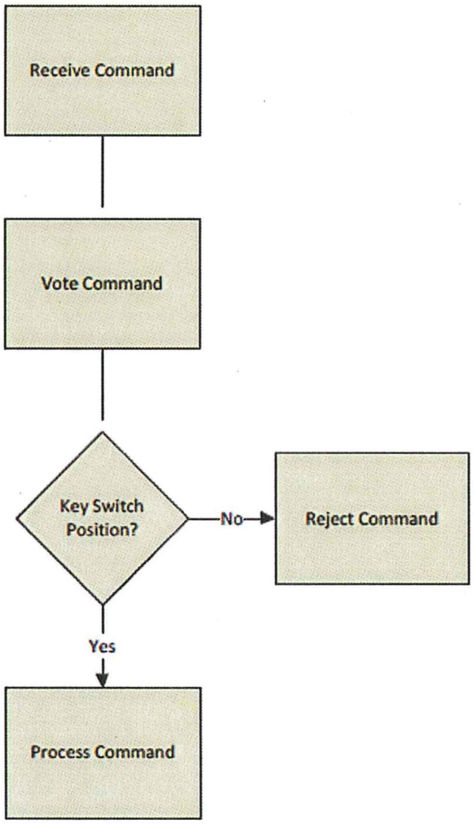
The Tricon keyswitch is designed to mitigate any single hardware fault. If one of the gangs on the Tricon keyswitch fails or the inputs to the MPs fail, it only affects the MP that is attached to that gang. The other two MPs will continue to receive good input values and out vote the MP with the bad input(s). This protects against any single fault in the physical Tricon keyswitch or on the MP.

The MP is responsible for handling commands from external devices (i.e., the MWS for the PPS Replacement) through the Tricon Communication Module. The software function, or the software "handler," inside the MP validates that the Tricon keyswitch is in the correct position before executing a command from the external device.

The required Tricon keyswitch setting for a subset of the categories of commands is as follows:

Command Category	Required Key Switch Setting
Application Changes	Program
Writes of Point Values	Remote or Program
Reads of Point Values	Any
Disabling of Points	Program
Read of Maintenance Information	Any

The MP checks whether the Tricon keyswitch is in the correct position before processing any command as depicted in the flow chart below:



The implementation in the MP firmware prevents any command from being executed when the Tricon keyswitch is not in the correct position. Below is an example of the code for halting the execution of the application:

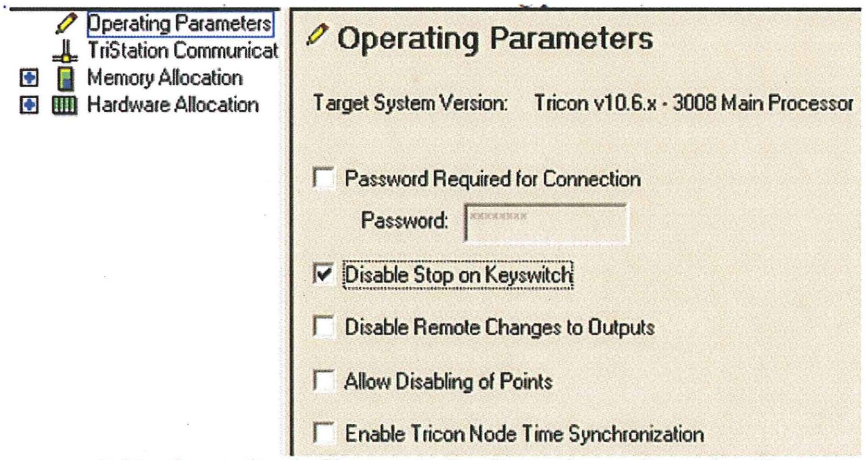
```
GLOBAL void
haltProgram (int connNum)
```

```
{
        /*
        * Make sure the keyswitch is in a position that allows this command.
        */

        if (!KEY_PROGRAM) {
                reject (WRONG_KEY_SETTING, connNum);
                return;
        }
        my_diagbuf.rll_status.cpRunState = CP_HALTED;    /* Note that we are halted. */
        respond (PROGRAM_HALTED, connNum);               /* Respond to the TRISTATION */
        return;
}
```

Every command has an appropriate check for the Tricon keyswitch position at the beginning of the function. For the above example, the STOP position of the keyswitch stops reading inputs, forces nonretentive digital and analog outputs to 0, and halts the application program. Retentive outputs remain at the value they had before the keyswitch was turned to STOP.

TriStation 1131 is configured during development to prevent the application from halting when the keyswitch is turned to STOP. A property named "Disable Stop on Keyswitch" determines whether the STOP position is disabled, as shown in the following graphic:



Operating Parameters
TriStation Communicat
⊞ Memory Allocation
⊞ Hardware Allocation

Operating Parameters

Target System Version: Tricon v10.6.x - 3008 Main Processor

□ Password Required for Connection

Password: xxxxxxxx

☑ Disable Stop on Keyswitch

□ Disable Remote Changes to Outputs

□ Allow Disabling of Points

□ Enable Tricon Node Time Synchronization

TriStation > Controller tree > Configuration > Operating Parameters

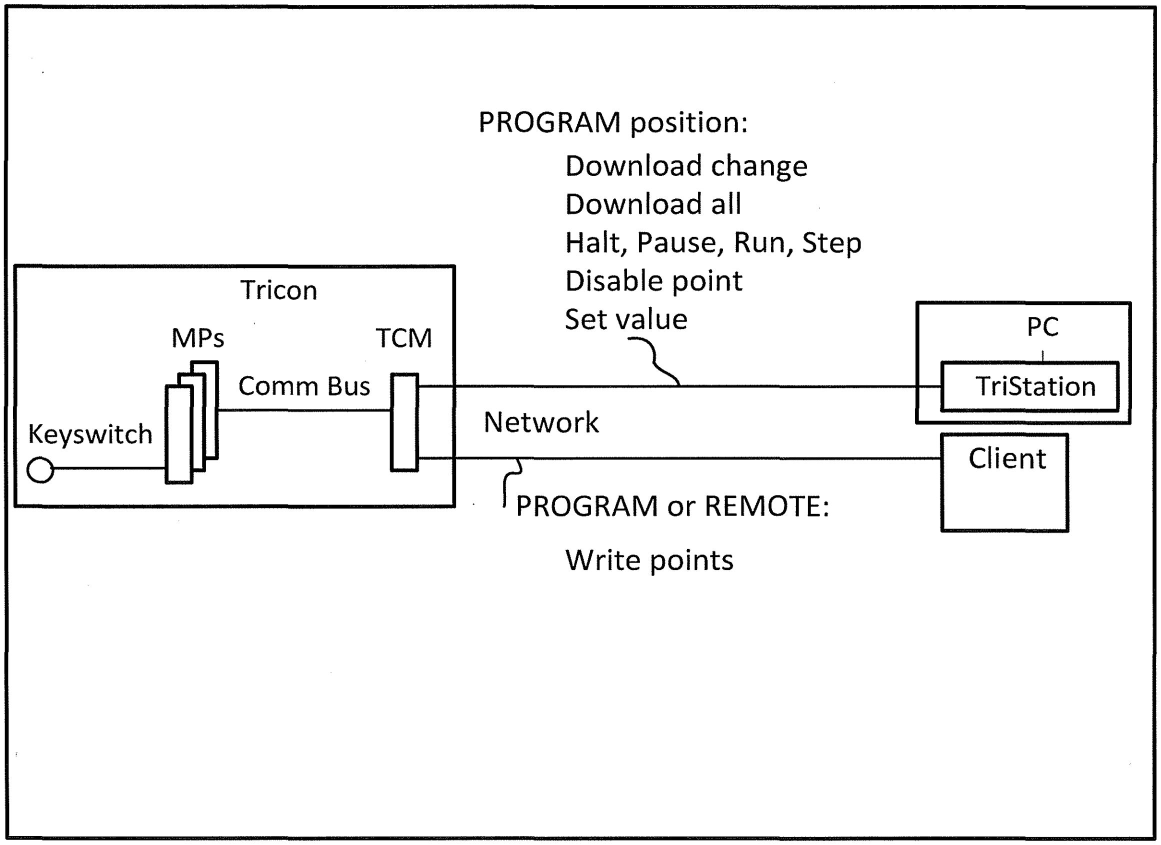
If the checkbox is selected, setting the Tricon keyswitch to STOP does not halt the application. If not selected, then setting the Tricon keyswitch to STOP does halt the application. The checkbox is selected by default. The default setting is used for the DCPP PPS replacement, which means turning the Tricon keyswitch to STOP will not halt the application program.

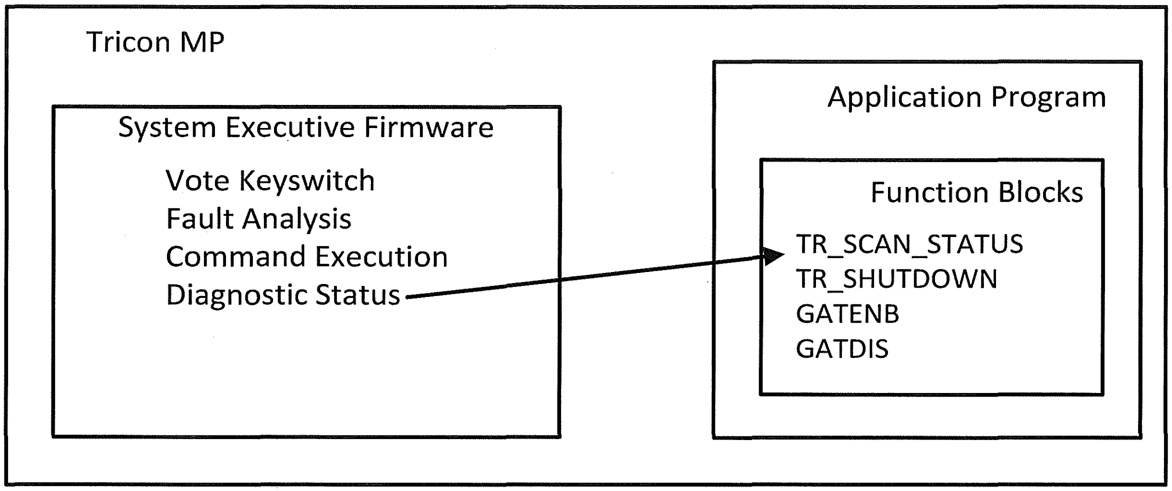
Software Affected by the Tricon Keyswitch

The Tricon keyswitch affects the firmware and application program executing on the MPs, commands from TS1131 software, and access by external devices (via the TCM):

The Tricon keyswitch must be in the PROGRAM position to accept commands from TS1131 to allow modifying the application program executing on the MPs. The Tricon keyswitch must be in the PROGRAM position or the REMOTE position to allow writing of points by an external device, except as permitted by the GATENB function described below.

The application program executing on each MP includes the system executive firmware and the application program as shown in the diagrams below:





The firmware includes Tricon keyswitch voting, fault analysis, command execution, and a diagnostic status structure. The application can call function blocks affected by the Tricon keyswitch.

Vote Keyswitch – Keyswitch voting starts when the keyswitch values have stopped changing for three seconds. If all voting legs agree on one value, the voted value is the agreed value. For a single failure, if one leg disagrees, that leg is reset, failed, and taken out of the voting. For multiple failures, if all voting legs mismatch, then an error message is logged without reset, and the voted value is 0 (STOP). When the voted value changes to STOP, if key stop is enabled, then the application program is halted, otherwise the change is logged.

Fault Analysis – Resets the main processor for a single failure, logs keyswitch errors, and logs changes in keyswitch position.

Command Execution – The firmware executes commands depending on the voted position of the keyswitch.

Diagnostic Status – Diagnostic status is a data structure with a keyswitch member that holds the voted keyswitch position. The keyswitch member is a system variable that can be read (i.e., a read-only value) by an external device or by a TR_SCAN_STATUS function block in the application program.

An application can call any of the following four function blocks:

TR_SCAN_STATUS – The KEYSWITCH output provides the keyswitch position.

TR_SHUTDOWN – Provides ALARM_PROGRAMMING_PERMITTED and ALARM_REMOTE_ACCESS outputs that can be used to alert an operator as described in the V10 Tricon Topical Report. The Tricon is designed so that an application program output can be provided to activate an annunciator window in the control room when the Tricon keyswitch is not in the RUN position. The TR_SHUTDOWN function block is not used in the DCPP PPS replacement.

GATENB and GATDIS – Can be used to temporarily allow writes to specified points even when the Tricon keyswitch is in the RUN position. The GATENB and GATDIS function blocks are used in the DCPP PPS replacement On-Line Maintenance and Test feature for adjusting tunable parameters and modifying setpoints.

Tricon Keyswitch Tests

The Tricon System Functional Validation, Invensys Operations Management document 9600158-002, tests the enable and disable application programs enabled by the Tricon keyswitch. The Tricon System Test Procedure, document 9600127-004, includes the following tests:

- Stopping and starting the application – turning active LEDs on and off.
- Ability to disable points.
- Disable of the STOP position of the keyswitch.
- RUN mode inhibits the ability to:
  - Disable variables
  - Change variable values
  - Download change
  - Halt
  - Download All
  - Change clock/calendar
  - Other commands in the command menu
- REMOTE mode inhibits similar to RUN mode.
- Test the ALARM_PROGRAMMING_PERMITTED and ALARM_REMOTE_ACCESS outputs of the TR_SHUTDOWN function block.
- Operation of the GATENB and GATDIS function blocks.
- Test the KEYSWITCH output of the TR_SCAN_STATUS function block.

The analysis of the failure modes, i.e., list of failures, their severity, and potential impact, of the Tricon keyswitch is contained in Invensys Operations Management document 9600164-531, "Tricon V10 Failure Modes and Effects Analysis," Revision 1, submitted for the Tricon Approved Topical Report [13]. The effects of failures in the V10 Tricon portion of the PPS Replacement are contained in Invensys Operation Management document 993754-1-811, "Failure Modes and Effects Analysis."

Administrative Controls

Normally, the Tricon keyswitch is set to the RUN position and the key is removed and stored in a secure location. The TriStation 1131 includes password security features to lessen the chance of unauthorized access. Control of operation of the Tricon keyswitch will be included in a procedure to ensure the protection set is declared inoperable when the Tricon keyswitch is not in the RUN position. A Trouble Alarm is initated on the MAS in the Control Room if the keyswitch is not in the RUN positin.

The PPS replacement contains design features that provide means to control physical access to safety related equipment. This includes access to PPS replacement equipment which encompasses the test points and the capabilities for changing setpoints. The PPS replacement equipment is located in a controlled area secured by the plant security system in a manner that only allows authorized personnel access. This limits the means to bypass safety system functions, via access controls, to authorized plant personnel. Keys to the cabinet doors, for the cabinets that contain the TriStation 1131 PC, will be maintained under the administrative control of DCPP operating staff.

Additional security controls that apply to the Tricon MWS that contains the TriStation 1131 are security-related information per 10 CFR 2.390 and have been previously submitted to the NRC staff in PG&E Letter DCL-11-123, dated December 20, 2011 [164].

ISG-04 Position 10 states: *Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment.*

The Tricon PPS design complies with the goal of this portion of the position, which refers to the alteration protection of theTricon application software (i.e., the safety division software), through a combination of system design and administrative controls. Modifications to addressable constants, setpoints, parameters, and other settings associated with a safety function are addressed in the response to the next portion of the position.

Each Tricon protection set within a safety division is provided with its own, dedicated MWS. Tricon applications are developed and downloaded to the Tricon using the TS1131 Developer's Workbench software tool, which resides on the MWS hard drive, but is not normally running. Tricon design requires that the controller keyswitch be placed in the PROGRAM position in order to download software from the TS1131 to the Tricon. The controller keyswitch is dependent upon software for its operation. However, the keyswitch hardware and software are safety-related and TMR, which preclude all but Tricon operating system CCF from inadvertently enabling software download.

Safeguards are provided to prevent inadvertent modification of Tricon safety division application software. First, any time a controller "keyswitch not in RUN" condition exists, whether intentionally or due to hardware or software failure, an alarm will be initiated on the MAS in the control room. Upon the operator determining cause of the alarm, the channel for each of the functions processed by the affected Tricon protection set within the safety division will need to be declared inoperable immediately. Second, the software cannot change spontaneously; multiple actions are necessary by a knowledgeable individual. The TS1131 program must be started, configured, and logically connected to the Tricon using an approved DCPP procedure in order to make changes. Should a "keyswitch not in RUN" condition occur in multiple divisions due to Tricon hardware or software malfunction or failure, changes cannot occur to Tricon software unless the TS1131 is in operation, configured specifically to perform the download, and the download is initiated.

Modification of Tricon application software will always be performed using approved DCPP procedures and will normally not be done with the plant online. The safety application software is protected from alteration during Main Processor Unit (MPU) replacement by the hot swap capability inherent in the TMR Tricon design. Hot swap capability enables any MPU or I/O module to be replaced on-line without affecting system operation. Should one of the three MPUs fail, the system will continue normal operation with the two remaining MPUs. Using an approved procedure, the technician will remove the failed MPU on-line and insert the replacement MPU. Upon completion of system diagnostics, the application software will be loaded automatically by the operating system from the functional MPUs to the replacement MPU without intervention or connection of any external equipment. When the loading is complete, the operating system will place the replacement MPU in service automatically. There is no opportunity to inadvertently load incorrect safety application software during MPU replacement. In the extremely unlikely event of failure of all three MPUs, the current safety application software will be downloaded from a verified backup source per a DCPP approved procedure. Such a download operation can only be performed with the Tricon offline and the keyswitch in the PROGRAM position.

Similarly, hot swap capability also allows Tricon I/O and communication modules to be replaced online without affecting system operation. Tricon chassis provide logical slots for I/O and communication modules, each slot comprising two physical slots. In the DCPP application, only one physical slot will be occupied by a given module. Should a fault occur in one of the three redundant legs in the module, the Tricon is designed to initiate a system trouble alarm locally and on the MAS. Using an approved DCPP procedure, the maintenance technician will gain access to the system and insert a spare module of the correct type into the physical slot adjacent to the faulted module. Upon completing Tricon system diagnostics, the replacement module will become the active module and the faulted module will become the spare module and no longer active. The faulted spare can then be removed from the chassis without any interruption in Tricon safety operation.

ISG-04 Position 10 states: *A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable.*

The Tricon portion of the DCPP PPS complies with this position through the TCM, which provides functional data isolation by utilizing the dual processor/shared memory scheme described in ISG-04 to provide communications between external systems/devices and the Tricon controller. The Tricon portion of the DCPP PPS includes functions controlled by the safety related logic to supplement the functional data isolation provided by the TCM and allow tunable parameters to be adjusted from the non-safety MWS without having an adverse effect on Tricon safety operation. Only the affected instrument channel need be declared inoperable when altering tunable parameters. It is not necessary to declare the non-associated instrument channels inoperable.

The MWS is used by maintenance and engineering personnel to view and change a limited set of addressable constants, setpoints, parameters, and other settings utilized in the Tricon portion of the PPS. The Tricon supports a limited access ("gated access") function that enables the MWS to write to internal tagnames whose "write" attribute is set when the Main Chassis key remains in the RUN position. Using approved DCPP procedures, addressable constants, setpoints, parameters, and other settings utilized in the Tricon portion of the PPS will be changed in one Tricon protection set at a time. The affected instrument channels will be out of service for a very short time while parameters are being changed. The other protection sets are unaffected and will continue to perform their safety function.

Within the locked Tricon Protection Set cabinets, the technicians can access individual channel safety-related OOS switches, each of which has a contact wired to a Tricon digital input (DI), as well as a second dedicated contact that activates a window on the MAS to notify the operator that the OOS switch has been activated. The Tricon safety-related logic continuously monitors the status of the DI and upon detecting that point "ON," allows the MWS screens associated with that instrument loop to be activated for the parameters to be changed.

Further request/confirm dialog action by the maintenance technician action is required from the MWS screen before the Tricon gate access for those values can be enabled and the values manually changed from the MWS. As a minimum, the dialog requires the technician to login with a specific access level privilege, select a "software switch" and then acknowledge the selection before addressable tagnames with write access can be modified. Another MAS window is activated when the channel is confirmed

OOS. Changes can then be made to that particular function's addressable tagnames, or the instrument channel bistable, as applicable, may be tested from the MWS in Trip and Bypass modes. The tagnames to which values are being written from the Workstation page remain writable (and the bistable trip or bypass test mode remains active) only so long as the OOS switch for that process is activated AND the Workstation page for that function is active. The function is out of service until the OOS switch for that function is returned to its normal position. Upon returning the OOS switch to the normal position, the gated access function is disabled, the annunciator window extinguishes and MWS status windows return to normal. The technician may print tuning constants and setpoints to comply with procedures. Multiple protective functions within a Protection Set can be removed from service following the steps detailed above, yet modifications can be made to only one instrument channel at a time.

The TS1131 may be connected to the Tricon in monitor-only mode during safety operation when required for trouble-shooting or maintenance using an approved procedure. If trouble-shooting requires parameters to be altered that cannot be modified via the MWS as described above, the keyswitch must be placed in the REMOTE (i.e., not in RUN) position in order for TS1131 to modify parameters and the instrument channel for each of the functions processed by the Tricon subsystem will be declared inoperable with respect to its safety function.

ISG-04 Position 10 states: *Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of a keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.*

The PPS replacement complies with this portion of ISG-04 Position 10, which restricts connections from a workstation to more than one safety division at a time. The PPS replacement architecture provides two individual MWSs in each Protection Set. One of the two MWSs is dedicated to the Tricon and the other MWS is dedicated to the ALS. A MWS within a given Protection Set communicates only with the controllers to which it is connected in its own Protection Set. A MWS cannot communicate with, modify, or affect the operation of the MWS from another Protection Set, nor can a MWS within a given Protection Set communicate with, modify, or affect the operation of a safety controller in another Protection Set.

Within a Protection Set, the video display, keyboard, mouse, touchscreen interface, and printer are shared between the Tricon and ALS MWS via a KVM switch. The KVM switch enables the Tricon MWS and the ALS MWS to be controlled from one single high resolution KVM console. The KVM switch permits only connections between the video display and USB interface devices and the single selected computer. The KVM switch cannot connect the ALS and Tricon MWSs to each other.

Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 10 can be found in section 5, Point No. 10 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement the safety firmware for the FPGAs is installed such that it can only be modified using special tools available to CSI and only upon board removal. Certain data parameters can be modified by the utility either during plant operation (Bypass mode) or while the plant is shutdown. These modifications are to tunable parameters. The non-safety ALS MWS is used to perform these functions when physically connected to the TAB, which is alarmed at the ALS chassis and in the control room.

Each ALS PPS rack within a protection set provides one bi-directional communication link named the TAB for the purpose of performing surveillance testing, calibration, and parameter updates. Activation of the TAB communication link is monitored by the ALS subsystem and administratively controlled through physically disconnecting the communication link when the TAB is not in use. Communication between the ALS MWS and the ALS via the TAB are not possible when the TAB is disconnected. The TAB is connected infrequently under procedural control by trained personnel, and only when required during surveillance testing, maintenance, and trouble-shooting while the channel is placed in the bypass mode and declared OOS.

The ALS subsystem of the DCPP PPS replacement does not use a keyswitch to enable and disable external TAB communications. The TAB communications are enabled by physically connecting the RS-485 data communication link from the ALS chassis to the MWS when necessary for surveillance testing, maintenance, or trouble-shooting. External TAB communications are disabled by physically disconnecting the data link between the ALS and the MWS when not in use. When the data link is disconnected, the bus is electrically disconnected and TAB communication between the ALS and its MWS are not possible. TAB communication between the MWS and the ALS is possible only when the TAB communication link between the ALS chassis and the MWS is physically connected. There is no software associated with physically connecting or disconnecting the TAB data link.

The TAB communication link is continuously monitored by the ALS subsystem and the ALS generates a system level trouble alarm at the ALS chassis and in the control room whenever TAB communications with an external device (i.e., the MWS) are enabled by physical connection of the TAB data link connector.

Changes to process values contained in ALS NVM and the calibration of ALS analog inputs and outputs are possible only when the TAB data link is physically connected and when the ALS detects that the TAB data link has been connected to the MWS. The ALS-102 CLB contains logic that blocks safety channel bypasses from occurring if the TAB is not enabled.

The ALS generates a system level failure alarm if any ALS I/O reports that its bypassed state has changed from a non-bypass state to a bypassed state or if an ALS-102 logic bypass register reports that a change has occurred from a non-bypassed state to a bypassed state for any partial trip logic comparator output if the TAB is not enabled.

The enabling of the TAB via connecting the TAB data link to the MWS does not interfere with the ability of the ALS safety channels to perform their respective safety function and the ALS is still operable during activation of the TAB. Placing a channel in bypass mode in an ALS core (core A or core B) for maintenance will not affect the safety function of adjacent channels in the same ALS subsystem (ALS core A or core B) that are not bypassed. ALS channels that are not bypassed for maintenance will continue to perform their safety functions. Channels are separated in the ALS-102 CLB FPGA using virtual channel data registers, as described in CSI Document No. 6002-10206, "ALS-102 FPGA Design Specification" [166], that allow the logic path and register to be placed into different operating modes (normal, bypass, calibrate, override) in which addressable constants, setpoints, and parameters can be updated. The virtual channels used in the ALS PPS subsystem are described in CSI document No. 6116-10201, "Diablo Canyon PPS ALS-102 FPGA Requirements Specification" [20].

The ALS Reliability and FMEA document for the PPS replacement is CS Innovations Document 6116-00029, Revision 1, "Diablo Canyon PPS ALS Reliability Analysis and FMEA," which was submitted in Attachment 11 to the Enclosure of PG&E Letter DCL-12-050 [157]. Table 4-10, Operational Hazards Related to Maintenance Errors, in the 6116-00029 document contains an evaluated hazard that encompasses the safety significant failure mode of the keyswitch failing such that the ASU remains connected to the ALS chassis. The evaluated hazard is "TAB enable keyswitch left in inappropriate position." This hazard also encompasses a failure where the TAB data link is inadvertently left connected.

ISG-04 Position 10 states: *Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment.*

The ALS portion of PPS design complies explicitly with this portion of the position because the ALS platform design does not permit the ALS safety application logic to be altered online. The ALS-102 CLB must be removed from the ALS chassis in order to change the FPGA safety application logic. The ALS application logic in the CLB cannot be altered from the ASU via the TAB. ALS safety application logic changes must be performed by Westinghouse/CSI. PG&E will not possess the hardware and software tools required to reprogram the FPGA. Therefore, the ALS safety division software is protected from alteration while the ALS subsystem is online.

Modification of ALS FPGA application logic will always be performed using approved DCPP procedures and will normally not be done with the plant online.

The FPGA logic programmed into the Core "A" CLB and I/O boards is the same for all four "A" chassis Protection Sets. The FPGA logic programmed into the Core "B" CLB and I/O boards is the same for all four "B" chassis Protection Sets. Core "A" logic is diverse from Core "B" logic. The Core "A" or Core "B" CLB and I/O boards are configured for the specific Protection Set through the on-board NVRAM outside the ALS chassis using specific hardware and software provided by Westinghouse/CSI. If a CLB or I/O board must be replaced, PG&E will configure the replacement board NVRAM using an approved DCPP procedure before installing the new CLB in the ALS chassis.

Should it be necessary to replace a CLB, the affected ALS chassis must be removed from service. The ALS design allows one ALS chassis (e.g., Chassis "A") to be bypassed and removed from service without affecting the safety operation of the diverse ALS chassis (e.g., Chassis "B"). To replace a single I/O board, the outputs associated with the board are bypassed to prevent partial initiation of a protective function when the board is removed. While the board is being replaced and outputs are bypassed, the diverse chassis will continue to perform the safety function without interruption.

When board replacement requires an ALS chassis to be removed from service, the replacement will be performed using an approved DCPP procedure, and will be administratively controlled to require restoration of the ALS chassis within 30 days.

ISG-04 Position 10 states: *A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable.*

Certain ALS data parameters can be modified during plant operation (with the subject instrument channel in bypass mode) or while the plant is shutdown. The non-safety MWS is used to perform these functions when the TAB is physically connected by means of the TAB access connector. TAB activation is alarmed at the ALS chassis and in the control room.

Placing an instrument channel in bypass mode for the purpose of changing addressable constants, setpoints, parameters, and other settings associated with a safety function will not affect the safety function of adjacent instrument channels in the same ALS chassis (i.e., ALS-A or ALS-B) that are not bypassed for maintenance. That is, instrument channels that are not bypassed for maintenance will continue to perform their safety functions without requiring that all instrument channels in the ALS chassis be bypassed or removed from service. The time for maintenance will be administratively controlled to require restoration of the ALS chassis within 30 days.

Each ALS chassis has its own diverse CLB (Core "A" or Core "B"). Channels are separated within the ALS-102 CLB FPGA by way of the use of the virtual channel data registers described in the CSI ISG-04 compliance document 6116-00054 [165]. Virtual channel data registers are assigned individual logic paths within the ALS-102 FPGA, which allows the logic path and register to be placed into different operating modes (normal, bypass, calibrate, override) in which addressable constants, setpoints, and parameters can be updated by qualified maintenance technicians under an approved DCPP procedure. ALS-102 instrument data registers, a term used interchangeably with virtual channel data registers, are described in CSI document 6002-10202, ALS-102 Design Specification [94]. Instrument data registers used in the ALS PPS subsystem are described in CSI document 6116-10201, "Diablo Canyon Units 1 and 2 Process Protection System, ALS-102 FPGA Requirements Specification" [20].

4.8.11 ISG-04 Interdivisional Communications Staff Position No. 11

ISG-04 Interdivisional Communications, Staff Position No. 11 States:

Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

The PPS replacement conforms to this Staff Position.

The Tricon and ALS MWS in each Protection Set cannot communicate with a Tricon or ALS processor outside the Protection Set in which it is installed. Tricon or ALS processors in different Protection Sets cannot communicate with processors in other Protection Sets.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement the primary protection is that the Tricon keyswitch must be in PROGRAM mode before reprogramming of the application program using the TriStation 1131 program on the Tricon MWS can occur. All "write" messages are ignored by the Tricon controller when not in PROGRAM or when GATEDIS is active, refer to section 4.8.3 of this LAR. Tricon controllers are qualified TMR systems and are not dependent upon interdivisional communications or external systems to perform the safety function. With the Tricon keyswitch in RUN, the Tricon application cannot be altered. With the external hardwired safety-related out of service switch in the open position, no external "writes" from the MWS are allowed. If the Tricon keyswitch is not in the RUN position, an alarm is initiated on the Control Room MAS and the Tricon is considered inoperable. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 11 can be found in section 5, Point No. 11 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

The ALS subsystem in each of the four Protection Sets cannot communicate with ALS subsystems in the other Protection Sets. In addition, for the ALS portion of the PPS replacement the ALS FPGA technology prevents the ALS Platform communication architecture from changing FPGA gate connections. The communication architecture is designed to preclude this from occurring by not providing the mechanism to alter the FPGA gate connections. Information or messages received through the RAB and TAB cannot be used to control the execution of the safety division application program. The ALS communication architecture is designed to preclude messages through the TAB from changing FPGA firmware. The RAB has no physical connections external to the ALS chassis.

The ALS MWS in each Protection Set cannot communicate with an ALS chassis outside the Protection Set in which it is installed. The ALS MWS is used for changing certain plant parameters such as setpoints and tunable constants during surveillance and maintenance while the channel is placed in the bypass mode and declared out of service. This communication is enabled through physical connection of the communication link from the TAB on the ALS chassis to the ALS MSW. Activation of the TAB access is alarmed both locally and in the control room. Changes to process values contained in ALS NVM memory and the calibration of ALS analog inputs and outputs can only be performed when the TAB data link is physically connected and when the ALS detects that the TAB data link has been connected to the MWS. The ALS-102 Core Logic Board (CLB) contains logic that blocks safety channel bypasses from occurring if the TAB is not enabled. The ALS generates a system level failure alarm if any ALS I/O reports that its bypassed state has changed from a non-bypass state to a bypassed state or if an ALS-102 logic bypass register reports that a change has occurred from a non-bypassed state to a bypassed state for any partial trip logic comparator output if the TAB is not enabled.

The failure modes for the TAB data link are either enabled when it should be disabled, or disabled when it should be enabled. In the case of it being disabled when it should be enabled, this failure mode prevents the user of the ALS MWS to have access to the ALS chassis and thus there is no direct challenge to the safety function in this failure mode. In the case of it being enabled when it should be disabled, the ALS chassis generates an ALS Comm Enable alarm status signal to alert operations that the TAB data link between the ALS MWS and the ALS chassis is enabled.

4.8.12 ISG-04 Interdivisional Communications Staff Position No. 12

ISG-04 Interdivisional Communications, Staff Position No. 12 States:

Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:

- *Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.*
- *Messages may be repeated at an incorrect point in time.*
- *Messages may be sent in the incorrect sequence.*
- *Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.*
- *Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.*
- *Messages may be inserted into the communication medium from unexpected or unknown sources.*
- *Messages may be sent to the wrong destination, which could treat the message as a valid message.*
- *Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.*
- *Messages may contain data that is outside the expected range.*
- *Messages may appear valid, but data may be placed in incorrect locations within the message.*
- *Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).*
- *Message headers or addresses may be corrupted.*

The PPS replacement conforms to this Staff Position.

The PPS replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function, thereby ensuring that interdivisional communication faults will not occur.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement the design and operation of the Tricon prevents any communication fault altering the application program or its performance. All data "writes" must be in proper format, have the proper address, and be within a given alias range. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 12 can be found in section 5, Point No. 12 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement communication faults cannot adversely affect the performance of the ALS safety functions. The ALS-102 communication functions for the two TxB lines are accomplished by logic that is independent from the FPGA logic performing the safety logic function. The same conclusions can be made for the RAB and TAB. These communication functions are also accomplished by logic that is independent from the FPGA logic performing the safety logic function. Further details regarding the ALS conformance to staff position No. 12 is provided in section 5, Table 5.4-1, Item 12 of the ALS Topical Report Submittal [15].

4.8.13 ISG-04 Interdivisional Communications Staff Position No. 13

ISG-04 Interdivisional Communications, Staff Position No. 13 States:

Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

The PPS replacement conforms to this Staff Position. The PPS replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.

4.8.14 ISG-04 Interdivisional Communications Staff Position No. 14

ISG-04 Interdivisional Communications, Staff Position No. 14 States:

Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

The PPS replacement conforms to this Staff Position.

The PPS replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function. All safety-related communications are point-to-point with no switches, hubs, or routers. There is no involvement of equipment outside the division of the sending or receiving node.

4.8.15 ISG-04 Interdivisional Communications Staff Position No. 15

ISG-04 Interdivisional Communications, Staff Position No. 15 States:

Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

The PPS replacement conforms to this Staff Position.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement the Tricon is programmed to pass all values each scan, whether the values have changed or not. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 15 can be found in section 5, Point No. 15 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25] and Section 5, NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement, the communication for the TxB, RAB and TAB communication functions use predefined packets of information. These packets of information are transmitted at constant periodic intervals which are established during the design process whether the data has changed or not. The packets typically have a continuous stream of mask/status bits to alert the CLB to anomalies in the communicated information/data. Further details regarding the ALS communications are provided in section 5, 6002-00011 ALS Platform Specification [95].

4.8.16 ISG-04 Interdivisional Communications Staff Position No. 16

ISG-04 Interdivisional Communications, Staff Position No. 16 States:

Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)

The PPS replacement conforms to this Staff Position.

The PPS replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.

a) Tricon-Based PPS Equipment

Section 4.8.1 and 4.8.2 of this LAR describe the independence of Tricon controllers from external devices and the engineered layers of protection against communication failures.

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement, all ALS communication protocol is deterministic. The scan time is maintained at a constant rate even in the case of error. RAB failures to receive/transmit are always processed a second time before the failure is alarmed. Further details regarding the ALS communications are provided in section 5, 6002-00011 ALS Platform Specification [95].

4.8.17 ISG-04 Interdivisional Communications Staff Position No. 17

ISG-04 Interdivisional Communications, Staff Position No. 17 States:

Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as *a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.*

The PPS replacement conforms to this Staff Position.

4.8.17.1 Tricon-Based PPS Equipment

Details regarding the Tricon portion of the PPS replacement conformance to this staff position No. 17 can be found in section 5, Point No. 17 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

4.8.17.2 FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement, the ALS platform includes copper media for communication. These mediums are qualified at predefined electromagnetic interference/radio frequency interference (EMI/RFI) levels to meet NRC guidance and PG&E specific levels. Details regarding the ALS communications are provided in section 5, 6002-00011 ALS Platform Specification [95]. Details regarding the ALS equipment qualification are provided in 6002-0004 ALS EQ Plan [55].

4.8.18 ISG-04 Interdivisional Communications Staff Position No. 18

ISG-04 Interdivisional Communications, Staff Position No. 18 States:

Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

The PPS replacement conforms to this Staff Position.

a) Tricon-Based PPS Equipment

For the Tricon portion of the PPS replacement, the TCM handles all protocol, start/stop bits, handshaking, tasks. The main processor is neither burdened nor interrupted. Communication errors and malfunctions do not interfere with the execution of the safety function. Further detail regarding the Tricon portion of the PPS replacement conformance to this staff position No. 18 can be found in section 5, Point No. 18 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement the CLBs are application specific. The only functions that exist in the design are those critical to the performance of the PPS safety function. Communication logic, while common to all CLBs, uses a simple master-slave protocol, with only enough functionality to ensure data integrity and reliability. Any relevant hazards and performance deficits are evaluated as part of the development process and handled accordingly. The communication architecture has been analyzed for hazards and performance deficits as reflected in the final ALS communication design. Unneeded functionality and complications are eliminated and will be rechecked and eliminated during the application design.

4.8.19 ISG-04 Interdivisional Communications Staff Position No. 19

ISG-04 Interdivisional Communications, Staff Position No. 19 States:

If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

The PPS replacement conforms to this Staff Position.

Communications are point-to-point. There are no switches, hubs, etc within the Tricon safety-related architecture. ALS communications are all point-to-point serial.

a) Tricon-Based PPS Equipment

Details regarding the Tricon portion of the PPS replacement conformance to this staff position No. 19 can be found in section 5, Point No. 19 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25].

b) FPGA-Based ALS PPS Equipment

For the ALS portion of the PPS replacement, the ALS platform architecture is designed to eliminate data congestion. The communication hardware supports the necessary capacity to support the required design functions. The number of slaves that can transmit and receive is fixed during the PPS replacement design process. Data scan rates are also set during the PPS replacement design phase and are based on a constant cycle time. More importantly, the response time of a system is set during the design phase. This time is based on the PPS replacement requirements provided in DCPP Units 1 & 2 PPS Replacement FRS [28] and is verified during FAT testing. Details regarding the ALS communications are provided in section 5, 6002-00011 ALS Platform Specification [95].

4.8.20 ISG-04 Interdivisional Communications Staff Position No. 20

ISG-04 Interdivisional Communications, Staff Position No. 20 States:

The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

The PPS replacement conforms to this Staff Position.

Details of the response time calculations are provided in Section 4.11.1.2.4 of this LAR.

4.9 System, Hardware, Software, and Methodology Modifications (Section D.8 of DI&CISG-06 [1])

a) Tricon-Based PPS Equipment

The Tricon system being installed at DCPP is an identical functional design to the Tricon system platform described in the Triconex Tricon V10 Topical Report Submittal [13], which was submitted to the NRC on May 15, 2012.

b) FPGA-Based ALS PPS Equipment

The ALS platform being installed at DCPP is an identical functional design to the ALS platform described in the ALS Topical Report Submittal [15].

4.10 Compliance with IEEE Standard 603 (Section D.9 of DI&C-ISG-06 [1])

The requirements of IEEE Standard 603-1991 [21] contain safety related system requirements in five clauses (Clauses 4, 5, 6, 7 and 8). The PPS Replacement adherence to these five clauses and their sub-clauses is described in the subsections below.

4.10.1 Clause 4 Design Basis (Section D.9.4.1 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4 states:

A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of American National Standards Institute (ANSI)/American Nuclear Society (ANS) 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:

The purpose of the PPS replacement is to replace the existing Eagle 21 based PPS with the Tricon and ALS digital platforms. The PPS is designed to monitor a set number of plant parameters that are important to reactor safety during all plant conditions and provide RT and/or ESFAS signals when required.

The plant accident analysis and TS were compared to the PPS CDD [27], hardware and software functional requirements, detailed system and hardware drawings, Tricon and ALS Topical Reports, equipment qualification reports, and interface requirement specification reports. The PPS replacement continues to meet all necessary requirements. The conclusion was reached that the PPS replacement is designed such that it can accomplish its safety functions under the full range of all anticipated conditions and continue to enable DCPP to meet the requirements set forth in the FSAR Chapter 15 Safety Analysis [26].

The Eagle 21 digital system being replaced was required to undergo a D3 evaluation similar to the position outlined in NUREG-0800 BTP 7-19 [4] albeit not as detailed and without certain time restrictions. The PPS replacement has undergone a D3 evaluation to show how the DCPP upgraded design meets the latest D3 guidance by taking advantage of an internal diversity design within the ALS platform. A number of manual actuations that were credited during the NRC Eagle 21 PPS review will be eliminated. This is described in detail in the DCPP D3 report [6] that was submitted to the NRC in 2010. The NRC issued a SER accepting this D3 report on April 19, 2011 [7].

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSAR Chapter 15 [26] event with a concurrent CCF. Therefore, where previous Eagle 21 PPS evaluations relied upon manual operator action to mitigate several such events, the PPS replacement automatic mitigation functions are generated in the independent, inherently diverse ALS portion of the PPS replacement for those events.

Therefore, the built-in diversity provided by the logic-based ALS portion of the PPS replacement ensures that all accidents and events credited with automatic PPS mitigation in the FSAR [26] Chapter 15 Safety Analyses continue to be mitigated automatically with a concurrent software CCF. The PPS replacement provides automatic mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions.

4.10.1.1 Clause 4.1 Identification of the Design Basis Events (Section D.9.4.1.1 of DI&C-ISG-06 [1])

IEEE 603-1991 [21], Clause 4.1 states:

The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.

Clause 4.1 requires the identification of the design bases events applicable to each mode of operation. This information should be consistent with the analyses of FSAR Chapter 15 [26] events. NUREG-0800, BTP 7-4 [4] provides specific guidance on the failures and malfunctions that should be considered in identification of design bases events for systems that initiate and control AFW systems. NUREG-0800, BTP 7-5 [4] provides specific guidance on the reactivity control malfunctions that should be considered in the identification of design basis events. The malfunctions postulated should be consistent with the control system failure modes described in the FSAR [26].

The PPS replacement is used as a direct replacement for the existing Eagle 21 PPS and has mostly the same design basis as the existing Eagle 21 PPS. For the D3 evaluation there is a change in the design basis due to more specific guidance being issued and the installation of an internally diverse ALS FPGA as part of the PPS replacement. A new DCPP D3 analysis was performed and the results submitted [6] to the NRC for review. The purpose of this analysis was to confirm that the PPS replacement satisfies the positions stated in BTP 7-19 [4] and the DCPP design basis [26]. The NRC issued a SER [7] accepting the DCCP D3 approach.

The design basis events applicable to each mode of operation listed in Section 4.1 of this LAR are unchanged as a result of the PPS replacement. As a result, an evaluation was not necessary for any changes to the design basis. However, a beyond design basis event, a software CCF, was re-evaluated due to the installation of the Tricon and ALS digital platforms as the PPS replacement. This event had previously been evaluated for the Eagle 21 digital platform installation with somewhat different guidance. NUREG-0800, BTP 7-19 [4] was not issued until 1997 which was after the Eagle 21 installation.

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSAR Chapter 15 [26] event with a concurrent CCF. Where previous evaluations relied upon manual operator action to mitigate several such events, automatic mitigation functions are generated in the independent, inherently diverse ALS portion of the PPS replacement for those events.

The built-in diversity provided by the logic-based ALS portion of the PPS replacement ensures that all accidents and events credited with automatic PPS mitigation in DCPP FSAR Chapter 15 Safety Analyses [26] continue to be mitigated automatically with a concurrent software CCF. Thus, the PPS replacement provides automatic mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions.

a) Tricon-Based PPS Equipment

The Tricon platform does not impact the DCPP design bases events.

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.1 by stating that conformance is application specific. The ALS platform does not impact DCPP design bases events.

4.10.1.2 Clause 4.2 Identification of Safety Functions and Protective Actions (Section D.9.4.1.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.2 states:

The safety functions and corresponding protective actions of the execute features for each design basis event.

The DCPP safety functions and related protective actions for each FSAR Chapter 15 [26] design basis event are unchanged as a result of this PPS Replacement Project. Therefore, an evaluation was not necessary for the DCPP safety functions and protective actions related to the PPS Replacement Project.

However, a beyond design basis event, a Software CCF was reevaluated due to the publication of newer guidance issued prior to this installation of the PPS replacement. This event had previously been evaluated for the Eagle 21 digital platform installation but without the guidance provided in NUREG-0800, BTP 7-19 [4].

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSAR Chapter 15 [26] accident or event with a concurrent CCF. Therefore, where the previous D3 evaluation relied upon manual operator action to mitigate several such events, automatic mitigation functions are generated in the independent, diverse ALS portion of the PPS replacement for those events.

The design diversity provided by the logic-based ALS portion of the PPS replacement ensures that all accidents and events credited with automatic PPS mitigation in DCPP FSAR Chapter 15 [26] Safety Analyses continue to be mitigated automatically with a concurrent software CCF. Additionally, the PPS replacement provides automatic mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions. This is discussed in more detail in the D3 evaluation report [6] submitted to and accepted [7] by the NRC.

a) Tricon-Based PPS Equipment

The Tricon platform does not impact the DCPP design basis for the safety functions and protective actions.

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.2 by stating that conformance is application specific. The ALS platform does not impact the DCPP design basis for safety functions and protective actions.

4.10.1.3 Clause 4.3 Permissive Conditions for Operating Bypasses (Section D.9.4.1.3 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.3 states:

The permissive conditions for each operating bypass capability that is to be provided.

The permissive conditions for the DCPP operating bypasses have not changed as a result of the PPS replacement. The PPS replacement develops the comparator outputs for P14, P13, and P11 which are sent to the SSPS where the interlocks are developed.

a) Tricon-Based PPS Equipment

The existing permissive conditions and how the Tricon supports them are discussed and defined in the project specification documents. The Tricon platform does not impact the DCPP design basis for permissive conditions regarding operating bypasses.

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.3 by stating that conformance is application specific. The existing permissive conditions and how the ALS supports them are discussed and defined in the project specification documents. The ALS platform does not impact the DCPP design basis for permissive conditions regarding operating bypasses.

4.10.1.4 Clause 4.4 Identification of Variables Monitored (Section D.9.4.1.4 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.4 states:

The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.

The PPS Replacement Project is replacing the existing Eagle 21 PPS with the Tricon and ALS digital platforms. The PPS is designed to monitor a set number of plant parameters that are important to reactor safety during all plant conditions and provide RT and/or ESFAS signals when required. The safety variables to be monitored and their analytical limits have not changed as a result of the PPS replacement. However, system response times, accuracies and setpoints require evaluation to determine if changes are needed for these areas. The setpoint calculations for the PPS replacement are contained in Westinghouse document WCAP-17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," [171] using the setpoint methodology contained in Westinghouse document WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," [173]. The setpoint calculations show an acceptable margin between all trip setpoints and the respective analytical limits. This will assure acceptable completion criteria for all of the effected protective functions.

The PPS FRS [28] provides additional details regarding setpoint calculations including response time requirements for all PPS safety input functions.

a) Tricon-Based PPS Equipment

The existing variables to be monitored and how the Tricon supports them are discussed and defined in the project specification documents. The Tricon V10 Topical Report Submittal [13] does not provide additional information for this area.

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.4 by stating that compliance is application specific. The existing variables to be monitored and how the ALS supports them are discussed and defined in the project specification documents.

4.10.1.5 Clause 4.5 Minimum Criteria for Manual Protective Actions (Section D.9.4.1.5 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.5 states:

The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. See IEEE Std 494-1974.

4.5.1 The points in time and the plant conditions during which manual control is allowed.

4.5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.

4.5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.

4.5.4 The variables in 4.4 that shall be displayed for the operator to use in taking manual action.

The PPS is designed to monitor a set number of plant parameters that are important to reactor safety during all plant conditions and provide RT and/or ESFAS signals when required. The PPS Replacement Project does not alter the system level manual actuation configuration at DCPP. The timing associated with the DCPP condition, environmental criteria, information available to the operator and justification for allowing manual control remain the same. The timing responses discussed in the safety analysis will not be impacted by the PPS replacement.

As discussed in the approved DCPP D3 Topical Report [6, 7], several manual actuations previously credited in the Eagle 21 SER to mitigate FSAR Chapter 15 [26] accident or event with a concurrent CCF have been eliminated by the PPS replacement due to the built-in diversity provided by the ALS equipment. Automatic mitigation functions will be initiated by the independent, inherently diverse ALS portion of the PPS replacement for the following events, which previously would require manual operator action for mitigation if the event were to occur with a concurrent postulated CCF to the PPS. This reduces the number of manual actions and lessens the burden on the operator.

1. Loss of forced reactor coolant flow in a single loop above P8 as indicated by 2/3 reactor coolant flow-low;
2. Pressurizer Pressure-low mitigation of RCS depressurization, including SGTR, Steam Line Break and LOCA; and
3. Containment Pressure-high mitigation of Steam Line Break and LOCA.

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSAR [26] Chapter 15 accident or event with a concurrent CCF. Therefore, where previous evaluations relied upon manual operator action to mitigate several such events, automatic mitigation functions are generated in the independent, diverse ALS portion of the PPS replacement for those events.

The built-in design diversity provided by the logic-based ALS portion of the PPS replacement ensures that all accidents and events credited with automatic PPS mitigation in FSAR [26] Chapter 15 Safety Analyses continue to be mitigated automatically with a concurrent software CCF. Additionally, the PPS replacement provides automatic mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions.

a) Tricon-Based PPS Equipment

The DCPP design bases for minimum criteria for manual protective actions have not changed as a result of the PPS replacement. Tricon support for these actions is discussed and defined in the project specification documents. The Tricon V10 Topical Report Submittal [13] does not provide additional information in this area.

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.5 by stating that conformance is application specific. The DCPP design basis for minimum criteria for manual protective actions has not changed as a result of the PPS replacement. ALS support for these actions is discussed and defined in the project specification documents.

4.10.1.6 Clause 4.6 Identification of the Minimum Number and Location of Sensors (Section D.9.4.1.6 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.6 states:

For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.

The Feedwater Flow signals and the Steam Flow/Feedwater Flow Mismatch alarms are being removed from the PPS as discussed in the PPS replacement CDD [27]. The feedwater flow signals are non-safety related and will be input to the Digital Feedwater Control System (DFWCS), which will then generate the Steam Flow/Feedwater Flow Mismatch alarms.

As described in the PPS replacement CDD [27], the spare RTDs in the thermowell of each hot leg will now be activated for use by the PPS replacement. Each thermowell contains two RTDs and currently only one in each thermowell is available for the averaging process. In the PPS replacement, a wiring change will enable the use of all 6 RTDs for this averaging process. This should improve ΔT/Tavg and increases conservatism.

The DCPP design bases for the location of sensors has not changed as a result of the PPS replacement. However, the number of sensors has been increased to include the use of the current spare hot leg RTD as described above.

a) Tricon-Based PPS Equipment

Tricon support for the supplied sensors is discussed and defined in the project specification documents. The Tricon V10 Topical Report Submittal [13] does not provide additional information in this area.

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.6 by stating that conformance is application specific. ALS support for the supplied sensors is discussed and defined in the project specification documents.

4.10.1.7 Clause 4.7 Range of Transient and Steady-State Conditions (Section D.9.4.1.7 of DI&C-ISG-06 [1])

IEEE 603-1991 [21], Clause 4.7 states:

The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.

Clause 4.7 requires, in part, that the range of transient and steady-state conditions be identified for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. If these have not changed, this should be clearly identified in the information provided. The range of conditions specified is used in evaluating the adequacy of the design and qualification of the equipment.

The range of transient and steady-state conditions during normal, abnormal, and accident conditions has not changed as a result of the PPS Replacement Project. The FSAR Chapter 15 Safety Analysis [26] does not require modifications as a result of the PPS replacement.

Both replacement digital platforms, Tricon and ALS, are located in the same cabinets that house the existing PPS. Therefore, the environmental conditions experienced by the PPS replacement remain the same. The PPS replacement is qualified to envelope the existing plant environmental qualification (including EMC and seismic) requirements.

a) Tricon-Based PPS Equipment

The PPS replacement does not impact the range of transients and accidents. Equipment qualification information is provided in the Tricon Topical Reports [8] [13].

b) FPGA-Based ALS PPS Equipment

The PPS replacement does not impact the range of transients and accidents. Section 4 of the ALS Topical Report Submittal [15] provides detailed information for the ALS equipment qualification.

4.10.1.8 Clause 4.8 Conditions Causing Functional Degradation (Section D.9.4.1.8 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.8 states:

The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).

The identification of conditions having the potential for causing functional degradation of safety system performance, and for which provisions must be incorporated to retain necessary protective action has not changed as a result of the PPS replacement.

The PPS replacement is located in the same area with a controlled environment as the existing Eagle 21 PPS. Environmental qualification requirements are provided in the PPS replacement FRS [28].

a) Tricon-Based PPS Equipment

Equipment qualification information is provided in the Tricon Topical Reports [8] [13].

b) FPGA-Based ALS PPS Equipment

Section 4 of the ALS Topical Report Submittal [15] provides detailed information for the ALS equipment qualification.

4.10.1.9 Clause 4.9 Methods Used to Determine Reliability (Section D.9.4.1.9 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.9 states:

The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.

a) Tricon-Based PPS Equipment

The platform level FMEA and reliability analyses for the Tricon digital platform has been reviewed and accepted by the NRC. In the Tricon V10 Topical Report Submittal [13], Section 2.2.12 "Reliability and Availability," both reliability and availability were calculated with the assumption that periodic testing will uncover faults that are not normally detected by the Tricon system. For test periods ranging from 6 to 30 months the calculated reliability and availability were greater than 99.9 percent which exceeds the EPRI recommended goal found in EPRI TR-107330 [81], Section 4.2.3 "Availability, Reliability and FMEA." For a periodic test interval of 18 months the reliability is 99.9987 percent and the availability is 99.9990 percent.

b) FPGA-Based ALS PPS Equipment

In the ALS topical Report Submittal [15], reliability numbers were calculated for seven different types of modules. These calculations can be found in the following documents: 6002-10212-ALS-102 FPA FMEA and Reliability Analysis [82], 6002-30212-ALS-302 FPA FMEA and Reliability Analysis [83], 6002-31112-ALS-311 FPA FMEA and Reliability Analysis [84], 6002-32112-ALS-321 FPA FMEA and Reliability Analysis [85], 6002-40212-ALS-402 FMEA and Reliability Analysis [86], and 6002-42112-ALS-421 FPA FMEA and Reliability Analysis [87].

4.10.1.10 Clause 4.10 Critical Points in Time or Plant Conditions (Section 9.4.1.10 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.10 states:

The critical points in time or the plant conditions, after the onset of a design basis event, including:

4.10.1 The point in time or plant conditions for which the protective actions of the safety system shall be initiated.

4.10.2 The point in time or plant conditions that define the proper completion of the safety function.

4.10.3 The points in time or plant conditions that require automatic control of protective actions.

4.10.4 The point in time or plant conditions that allow returning a safety system to normal.

The critical points in time with regard to the DCPP FSAR Chapter 15 [26] events have not changed as a result of the PPS replacement. The points in time for required protective actions, required automatic protective control, and the return to normal safety system operation are the same.

a) Tricon-Based PPS Equipment

There is no additional information for control after protective action in the Tricon Topical Reports [8] [13].

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.10 by stating that conformance is application specific. The critical points in time with regard to the DCPP FSAR Chapter 15 [26] events have not changed as a result of the PPS replacement.

4.10.1.11 Clause 4.11 Equipment Protective Provisions (Section D.9.4.1.11 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.11 states:

The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.

There are no equipment protective provisions associated with the PPS replacement that would prevent the safety systems from accomplishing their safety functions.

However, it should be noted that several important new features will exist upon implementation of the PPS replacement. Examples are as follows:

Signal validation is required for the Overpressure ΔT and Overtemperature ΔT channels but not for any other PPS channels.

Input range checking is required for all PPS input channels. This includes out of range high and low setpoints.

PPS replacement platforms are equipped with sufficient diagnostics to alarm and isolate system faults to the card/module level.

These features enhance the reliability of the PPS replacement and do not provide equipment protective features that would prevent the PPS from performing the required safety functions.

a) Tricon-Based PPS Equipment

There is no additional information for equipment protective provision in the Tricon Topical Reports [8] [13].

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.11 by stating that conformance is application specific. There are no equipment protective provisions associated with the PPS replacement that would prevent the safety systems from accomplishing their safety functions.

4.10.1.12 Clause 4.12 Special Design Bases (Section D.9.4.1.12 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 4.12 states:

Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).

New design provisions, which could prevent the safety systems from accomplishing their safety functions, are not imposed by the PPS Replacement Project. However, the PPS Replacement Project initiated the need for a new diversity and D3 evaluation to be performed. Even though the previous D3 evaluation was still relevant for digital systems, the decision was made to eliminate the need for certain diverse manual actuations for the events where an operator's timed response was too short.

Per NRC ISG-02 [3], automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSAR [26] Chapter 15 event with a concurrent CCF. As discussed in the approved DCPP D3 Topical Report [6, 7], several manual actuations previously credited in the Eagle 21 SER to mitigate FSAR [26] Chapter 15 accident or event with a concurrent CCF have been eliminated by the PPS replacement due to the built-in diversity provided by the ALS equipment. Automatic mitigation functions will be initiated by the independent, inherently diverse ALS portion of the PPS replacement for events that previously would require manual operator action for mitigation if the event were to occur with a concurrent postulated CCF to the PPS.

Therefore, the design diversity provided by the logic-based ALS portion of the PPS replacement ensures that all accidents and events credited with automatic PPS mitigation in DCPP FSAR [26] Chapter 15 Safety Analyses continue to be mitigated automatically with a concurrent software CCF. The PPS replacement provides automatic mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions.

PG&E submitted the report, "Diablo Canyon Power Plant Topical Report, Process Protection System Replacement Diversity & Defense-in-Depth Assessment" [6], to the NRC for review. This report provides details on the PPS replacement designs and how the strategic use of the ALS FPGAs provides the necessary diversity features. The NRC issued the results of their review in a SER [7].

a) Tricon-Based PPS Equipment

There is no additional information for special design basis in the Tricon Topical Reports [8] [13].

b) FPGA-Based ALS PPS Equipment

Section 12.1.1 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 4.12 by stating that conformance is application specific.

The D3 Assessment [6] and the ensuing NRC safety evaluation [7] provide details regarding the ALS D3 concept and conformance to this clause.

4.10.2 Clause 5 System (Section D.9.4.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5 states:

The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function.

In addressing Clauses 5.1 through 5.15 below, the evaluation confirms that the general functional criteria for the PPS Replacement Project have been appropriately allocated to the various system components. The design review in this regard concludes that the system design fulfills the system DCPP design basis criteria established. This design review is from an integrated hardware/software perspective.

4.10.2.1 Clause 5.1 Single-Failure Criterion (Section D.9.4.2.1 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.1 states:

Clause 5.6 of IEEE 603-1991 The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 provides guidance on the application of the single-failure criterion.

This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion LB2I.The performance of a probable assessment of the safety systems may be used to demonstrate that certain *postulated failures need not be considered in the application of the criterion. A probable assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion, IEEE Std 352-1987 [121] and IEEE Std 577-1976 provide guidance for reliability analysis.*

Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in 4.9 of the design basis, a probable assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.

DCPP, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, "Process Protection System Replacement Diversity & Defense-In-Depth Assessment" [7] describes the PPS replacement system level D3 details.

A System Level FMEA, which meets the requirements of IEEE 603-1991 [21], Clause 5.1 will be performed during Phase 2 of the PPS replacement project to ensure the Single Failure Criterion is met at the combined Tricon and ALS PPS replacement system level.

a) Tricon-Based PPS Equipment

PPS Replacement uses a V10 Tricon system in each of multiple process channels and trip logic trains. These redundant channels and trains are electrically isolated and physically separated. The Tricon platform hardware is designed with triple redundant safety circuitry for single failure protection. Section 4.10 of EPRI TR-1000799 "Generic Qualification of the Triconex Corporation TRICON Triple Modular Redundant PLC System for Safety-Related Applications in Nuclear Power Plants," [8] describes how the Tricon platform is designed such that no single failure will impact the ability of the equipment to perform the safety function. In addition, Section 2.2.11 of the Tricon V10 Topical Report Submittal [13], addresses the V10 FMEA submitted with the platform documentation.

b) FPGA-Based ALS PPS Equipment

Section 12.1.2 of 6002-00301 ALS Topical Report Submittal [15] describes the ALS platform compliance with the Single Failure Criterion. 6002-00031 ALS Diversity Analysis [16] describes the built-in diversity features of the ALS platform.

4.10.2.1.1 FMEA Section D.9.4.2.1.1 of DI&C-ISG-06 [1])

A System Level FMEA will be performed during Phase 2 of the PPS replacement project to ensure the requirement of IEEE 603-1991 [21], Clause 5.1 is met at the combined Tricon and ALS PPS replacement system level. IEEE Standard 379 [148] and NRC RG 1.53, R3 [149] provide guidance on application of the single-failure criterion to meet IEEE 603-1991 [21], Clause 5.1.

a) Tricon-Based PPS Equipment

Section 2.2.11 of the NRC-approved Tricon V9 Topical Report [8] describes the platform level FMEA which was performed on the Tricon V9 PLC. Further details of the Tricon V10 FMEA are located in Appendix 1, Section 5 of NTX-SER-09-10 Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24]. A Tricon application level FMEA will be performed during Phase 2 of the PPS replacement project.

b) FPGA-Based ALS PPS Equipment

Section 12.1.2 of the ALS Topical Report Submittal [15] discusses the board level FMEA performed on each of the ALS boards. An ALS application level FMEA will be performed during Phase 2 of the PPS replacement project.

4.10.2.2 Clause 5.2 Completion of Protective Action (Section D.9.4.2.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.2 states:

The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.

The design for the PPS replacement meets the requirements of IEEE 603-1991 [21] Clause 5.2, Completion of Protective Action

a) Tricon-Based PPS Equipment

The Tricon scan-based architecture is such that, once initiated, the protective action proceeds to completion. Interrupts are not used and return to normal operation requires deliberate operator action. The NRC SER [11], dated December 11, 2001, Section 5.1 documents the NRC concurrence. In addition, the FMEA submitted with the Tricon V10 Topical Report Submittal [13] provides updated analysis for the V10 platform.

b) FPGA-Based ALS PPS Equipment

Section 12.1.3 of 6101-00301 ALS Topical Report Submittal [15] discusses the capabilities of the ALS to ensure the protective action continues until complete. The

ALS platform generates a partial trip and does not require manual intervention or acknowledgment of actuation commands to complete a protective action.

4.10.2.3 Clause 5.3 Quality (Section D.9.4.2.3 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.3 states:

Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program (See ASME NQA-1-1994). Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

Section 4.2.11 of this LAR addresses the compliance with 10 CFR 50 Appendix B for PG&E, Triconex and CSI.

The design for the PPS replacement meets the requirements of IEEE 603-1991 [21] Clause 5.3, Quality.

PG&E has an NRC approved 10 CFR 50 Appendix B QA program. Procedural guidance for digital projects is provided in PG&E procedure CF2.ID9, Rev 1 Software QA for Software [51].

PPS replacement project specific QA requirements are provided in SyQAP for PPS Replacement Project [52].

a) Tricon-Based PPS Equipment

Section 5.1.1 of the Tricon V10 Topical Report Submittal [13] describes the QA program for Invensys Operation Management. The Invensys Operation Management QAP is outlined in IOM Corporate NQAM (IOM-Q2) [31].

The Tricon PPS replacement project specific QA requirements are provided in DCPP Tricon PPS SQAP [71].

b) FPGA-Based ALS PPS Equipment

Section 10 of 6101-00301 ALS Topical Report Submittal [15] describes the QA program for CSI. The QA Program used is outlined in the "Westinghouse Quality Management System" [33].

6002-00001 ALS Quality Assurance Plan [63] provides definition for the techniques, procedures, and methodologies which are used by CSI to assure quality in the design and test developments of the ALS platform.

4.10.2.4 Clause 5.4 Equipment Qualification (Section D.9.4.2.4 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.4 states:

Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.

Section 4.6 of this Enclosure addresses the conformance of the Tricon, ALS and ancillary equipment to the EQ requirements of IEEE 603 Clause 5.4. Additionally, Section 4.2.12 addresses the system time response requirements included in Section D 9.4.2.4 of DI&C-ISG-06 [1].

Refer to Section 4.11.1.2 of this Enclosure for additional details regarding the compliance with the requirements of IEEE Standard 7-4.3.2-2003 [80].

4.10.2.5 Cause 5.5 System Integrity (Section D.9.4.2.5 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.5 states:

Safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

The PPS Replacement Project is made up of both Tricon and ALS processors and associated components and has been designed and tested to confirm the equipment demonstrates system performance adequate to ensure completion of protective actions over the range of transient and steady-state plant conditions.

- In accordance with the DCPP Units 1 and 2 PPS Replacement FRS [28], Section 3, the PPS instrumentation is installed within 16 existing PPS equipment racks (per unit).
- The PPS equipment racks are located in what is considered to be a mild environment including atmospheric pressure. The design basis specifies the range of ambient temperature conditions during normal and accident conditions as 40 - 104°F. For the new system, the heat load effects are less than the current system.
- The design basis specifies the range of humidity conditions during normal and accident conditions as 0 – 95 percent relative humidity (non-condensing).
- The design basis specifies the seismic response spectra for a design basis earthquake. This specification envelopes the range of seismic based vibration conditions that could occur during normal and accident conditions.

- The design basis specifies the range of electrical power supply conditions during normal and accident conditions in the 120 volts (V) 60 hertz (Hz) AC vital power systems as ±10 percent voltage and ±3 percent frequency.

The PPS consists of four separate and isolated Protection Sets with adequate instrumentation to monitor the required reactor plant parameters and provide signals to the SSPS for use in determining when required RTS or ESFAS protective actions are required.

The PPS provides signals (isolated where appropriate) to drive indicators and/or recorders in the main control room to provide operators with operating plant information and to satisfy the requirements of RG 1.97 [36] as described in Section 7.5 of the DCPP FSAR [26].

The PPS provides isolated signals to the PDN Gateway Switch and to various plant control systems such as the DFWCS and the Rod Control System. With the exception of ΔT/Tavg, these signals are derived from the PPS channel sensor input loops and are not processed by the PPS. The signal from the PPS sensors is supplied to the AMSAC via an independent isolator. A Tricon failure cannot affect the AMSAC and an AMSAC failure cannot affect the Tricon.

The Tricon and ALS systems have been designed and tested to confirm that the equipment demonstrates system performance adequate to ensure completion of protective actions over the range of transient and steady state plant conditions. Failure modes are discussed in Paragraph 2.2.11 of the Tricon V10 Topical Report Submittal [13] and in Section 7.1 of the ALS Topical Report Submittal [15].

Computer system integrity is addressed in Section 4.11.1.3 of this Enclosure.

4.10.2.6 Clause 5.6 Independence (Section D.9.4.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.6 states:

Clause 5.6 of IEEE 603-1991 requires in part independence between 1) redundant portions of a safety system, 2) safety systems and the effects of design basis events, and 3) safety systems and other systems. SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides acceptance criteria for system integrity. This acceptance criteria states that three aspects of independence: 1) physical independence, 2) electrical independence, and 3) communications independence, should be addressed for each previously listed cases. Guidance for evaluation of physical and electrical independence is provided in Regulatory Guide 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems" (Reference 126), which endorses IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits." The safety system design should not have components that are common to redundant portions of the safety system, such as common switches for actuation, reset, *mode, or test; common sensing lines; or any other features that could compromise the independence of redundant portions of the safety system. Physical independence is attained by physical separation and physical barriers. Electrical independence should include the utilization of separate power sources. Transmission of signals between independent channels should be through isolation devices.*

SRP Chapter 7, Appendix 7.1-C, Section 5.6, "Independence" provides additional acceptance criteria for communications independence. Section 5.6 states that where data communication exists between different portions of a safety system, the analysis should confirm that a logical or software malfunction in one portion cannot affect the safety functions of the redundant portions, and that if a digital computer system used in a safety system is connected to a digital computer system used in a non-safety system, a logical or software malfunction of the non-safety system must not be able to affect the functions of the safety system.

4.10.2.6.1 Clause 5.6.1, Independence between Redundant Portions of a Safety System

IEEE Standard 603-1991 [21], Clause 5.6.1 states:

5.6.1 Between Redundant Portions of a Safety System. Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish safety function during and following any design basis event requiring that safety function.

The PPS replacement scope consists of four independent Protection Sets; each Protection Set is physically separated and electrically isolated from the other sets. The requirement for physical separation is provided in Section 1.2 of the DCPP Units 1 & 2 PPS Replacement FRS [28].

a) Tricon-Based PPS Equipment

Section 2.2 of 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25], describes the independence of the Tricon equipment.

b) FPGA-Based ALS PPS Equipment

Section 1.3 and 2.2.2 of the ALS System Requirement Specification [17] describes the independence of the ALS equipment. Section 4 of ALS Topical Report Submittal [15] describes the equipment qualification of the ALS platform.

4.10.2.6.2 Clause 5.6.2, Independence between Safety Systems and Effects of Design Basis Event

IEEE Standard 603-1991 [21], Clause 5.6.2 states:

5.6.2 Between Safety Systems and Effects of Design Basis Event. Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.

The PPS replacement scope consists of four independent Protection Sets; each Protection Set is physically separated and electrically isolated from the other sets. The requirement for physical separation is provided in Section 1.2 of the DCPP Units 1 and 2 PPS Replacement FRS [28].

a) Tricon-Based PPS Equipment

Section 2 of the Tricon V10 Topical Report [13] for the Tricon provides a summary of the equipment testing and analysis performed to meet the requirements of IEEE 603-1991 [21], IEEE Standard 323-1983 [65], EPRI TR-107330 [81], EPRI TR-102323 Revision 1 [79] and RG 1.180 Revision 1 [23]. This testing/analysis confirmed that the Tricon safety system is fully qualified and capable of performing its designated safety functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions, as required.

b) FPGA-Based ALS PPS Equipment

Section 4 of ALS Topical Report Submittal [15] describes the equipment qualification of the ALS platform.

4.10.2.6.3 Clause 5.6.3, Independence between Safety Systems and Other Systems

IEEE Standard 603-1991 [21], Clause 5.6.3 states:

5.6.3 Between Safety Systems and Other Systems. Safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

5.6.3.1 Interconnected Equipment

(1) Classification: Equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems, Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.

(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function.

A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

5.6.3.2 Equipment in Proximity

(1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981.

(2) Barriers: Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.

5.6.3.3 Effects of a Single Random Failure. Where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure.

See IEEE Std 379-1988 for the application of this requirement.

The PPS replacement scope consists of four independent Protection Sets; each Protection Set is physically separated and electrically isolated from the other sets. The requirement for physical separation is provided in Section 1.2 of the DCPP Units 1 & 2 PPS Replacement FRS [28].

a) Tricon-Based PPS Equipment

EPRI TR-1000799, "Generic Qualification of the Triconex Corporation TRICON Triple Modular Redundant PLC System for Safety-Related Applications in Nuclear Power Plants [8] describes the equipment qualification for the Tricon platform. 993754-1-912 Diablo Canyon Triconex PPS ISG-04 Conformance Report [25] describes the data and communications independence of the Tricon equipment. NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24] describes the communications independence capabilities of the Tricon platform.

b) FPGA-Based ALS PPS Equipment

Section 4 of ALS Topical Report Submittal [15] describes the equipment qualification of the ALS platform. Section 5 of ALS Topical Report Submittal [15] describes the communication independence capabilities of the ALS equipment.

Section 12.1.19 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 5.6.3.

4.10.2.7 Clause 5.7 Capability for Test and Calibration (Section D.9.4.2.7 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.7 states:

Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987 [3]. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

(1) appropriate justification shall be provided (for example, demonstration that no practical design exists),

(2) acceptable reliability of equipment operation shall be otherwise demonstrated, and

(3) the capability shall be provided while the generating station is shut down.

The PPS replacement complies with Clause 5.7 as discussed below:

The PPS replacement is a digital replacement for the existing digital Eagle 21 PPS at DCPP. The capability for testing and calibration of the PPS replacement is not significantly different from that of the existing Eagle 21 PPS. The PPS replacement provides enhanced self-testing and diagnostic functions that reduce likelihood of undetected failures in both the Tricon and ALS subsystems. However, the existing Eagle 21 technical specification surveillance requirements (SR) do not require revision as a result of this project.

The requirement for periodic testing is addressed by channel calibrations. The channel calibrations are performed online using the bypass capability of the channel or during refueling outages when the PPS is not required to be operable. Calibration and testing will be performed according to approved procedures that establish specific surveillance techniques and surveillance intervals intended to maintain the high reliability of the PPS replacement.

If on-line testing is required for troubleshooting maintenance, the PPS replacement design allows for this testing without disconnecting wires, installing jumpers, or otherwise modifying the installed equipment. Simulated signal inputs into a channel can be applied using measuring and test equipment. During performance of testing or maintenance of the PPS replacement, it may be necessary to place the individual channel into the bypass mode. Indication of bypass status is discussed in Section 4.10.2.8 of this LAR.

Administrative procedures will provide appropriate guidance in the event a portion of the PPS replacement is in bypass or is manually tripped. These procedures are augmented by automatic indication at the system level that the system is in bypass or that a portion of the protection system and/or the systems actuated or controlled by the protection system is tripped.

Both the Triconex and the ALS platforms make extensive use of watchdog timers in performing built-in self-tests. The Triconex operating system provides "hooks" to the application to enable the application to take appropriate action upon watchdog timer time-out. Refer to:

- Tricon V10 Topical Report Submittal [13] Section 2.1.2.6, 2.1.3.1, 2.2.10
- Appendix B to Tricon V10 Topical Report Submittal [13] Section 3.9.A, 3.9.B, 5.3.V
- ALS Topical Report Submittal [15] Section 2.3
- ALS System Requirements Specification [17] Section 2.7.2, 2.7.3
- ALS System Design Specification [19] Section 5.2.5

a) Tricon-Based PPS Equipment

The Triconex application program provides the means for periodic test and calibration of input sensors and output devices. Triconex PPS replacement application details are provided in the Triconex SRS [75]. Platform compliance with this clause is discussed in Tricon V10 Topical Report Submittal [13] Section 2.1 and Topical Report Appendix B Sections 3.0, 5.0, and 6.0.

b) FPGA-Based ALS PPS Equipment

Section 3.1.1.3 of the ALS Topical Report Submittal [15] separates faults into categories and describes ALS platform diagnostics and actions taken upon failure detection.

Section 3.2 of the ALS Topical Report Submittal [15] describes the ALS design to support periodic surveillance testing, channel calibration and maintenance on a particular channel, while retaining the capability to accomplish the intended safety functions on the remaining channels.

Section 3.4 of the ALS Topical Report Submittal [15] describes the ALS design to support calibration of an analog input/output channel using the ASU or the MWS - specific to the PPS replacement) and calibrated external test equipment.

Section 12.1.8 of the ALS Topical Report Submittal [15] describes the ALS platform compliance with this clause.

For both the Triconex and ALS subsystems, the platform self-tests and the application specific test and calibration functions will be performed during the FAT to verify that the safety function is not adversely affected by performance of either built-in or application specific test and calibration functions.

4.10.2.8 Clause 5.8 Information Displays (Section D.9.4.2.8 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.8 states:

5.8.1 Displays for Manually Controlled Actions. The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981 [91]. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.

5.8.2 System Status Indication. Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.

5.8.3 Indication of Bypasses. If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.

5.8.3.1 This display instrumentation need not be part of the safety systems.

5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.

5.8.3.3 The capability shall exist in the control room to manually activate this display indication.

5.8.4 Location. Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.

4.10.2.8.1 The PPS replacement complies with Clause 5.8.1 as discussed below:

The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are necessary for the safety systems to accomplish their safety functions are part of the safety systems and are unchanged from that which was approved for the Eagle 21 PPS [5]. The RTS instrumentation including manual initiations is listed in TS Table 4.3-1 of the Eagle 21 LAR [97] and the ESFAS instrumentation including manual initiations is listed in TS Table 3.3-3 of the Eagle 21 LAR [97].

a) Tricon-Based PPS Equipment

The Tricon platform has flexible hardware and software capability for communicating with a variety of analog and digital devices, including main control board analog recorders and indicators and digital visual display units such as the MWS. The Triconex platform capability is described in the Topical Report Submittal [13] Section 2.1 and the DI&C-02 and -04 Compliance Report [24] Section 3.0. Triconex PPS replacement application details are provided in the Triconex SRS [75].

b) FPGA-Based ALS PPS Equipment

ALS application details are provided in the DCPP System Design Specification [19] and the ALS-102 FPGA Requirements Specification [20]. The ALS Topical Report Submittal [15] Section 12.1.9.1 discusses compliance of the ALS platform with IEEE Standard 603 [21] Clause 5.8.1.

4.10.2.8.2 The PPS replacement complies with Clause 5.8.2 as discussed below:

The display instrumentation that indicates and identifies protective actions of the sense and command features and execute features is unchanged by the PPS replacement. This instrumentation is primarily associated with inputs and outputs of the SSPS, which is not affected by the PPS replacement. In addition, the status of all actuated components is indicated on the control boards together with the control switches that are provided for the individual components.

A bistable status light panel on the Control Board provides bistable monitoring information in the Control Room. A “postage stamp” indicator lamp on the panel illuminates to indicate that a protection channel has been activated. This panel is part of the SSPS and is not affected by the PPS replacement.

Display instrumentation that indicates and identifies the status of protective actions of sense and command features is specific to the application.

a) Tricon-Based PPS Equipment

Triconex PPS replacement application details are provided in the Triconex SRS [75]. Platform compliance with this clause is described in Tricon V10 Topical Report Submittal [13] Section 2.1 and the Triconex DI&C-02 and -04 Compliance Report [24] Section 3.0.

b) FPGA-Based ALS PPS Equipment

ALS application details are provided in the DCPP System Design Specification [19] Section 5.3.3.4 and the ALS-102 FPGA Requirements Specification [20]. The ALS Topical Report Submittal [15] Section 12.1.9.2 discusses compliance of the ALS platform with IEEE Standard 603 Clause 5.8.2.

4.10.2.8.3 The PPS replacement complies with Clause 5.8.3 as discussed below:

PPS Replacement FRS[28] paragraph 3.2.1.3.3 requires status indication signals that satisfy the requirements of RG 1.47 [105] be provided to the control room from each Protection Set for indication that a protection channel has been placed in an inoperable condition (e.g., bypassed).

Display instrumentation that indicates and identifies the status of protective actions of sense and command features is specific to the application.

a) Tricon-Based PPS Equipment

Triconex PPS replacement application details are provided in the Triconex SRS [75]. Platform compliance with this clause is described in Tricon V10 Topical Report Submittal [13] Section 2.1 and the Triconex DI&C-02 and -04 Compliance Report [24] Section 3.0.

b) FPGA-Based ALS PPS Equipment

ALS System Requirements Specification [17] requires indication of partial trip output bypasses to be provided locally at the cabinet. This requirement is implemented in ALS System Design Specification [19] Section 11.3, which requires indication that an input channel or output channel has been placed into or removed from a bypass mode or an override mode and describes means by which the information is made available for display in the control room. The ALS Topical Report Submittal [15] Section 12.1.9.2 discusses compliance of the ALS platform with IEEE Standard 603 Clause 5.8.2. ALS application details are provided in the DCPP System Design Specification [19] Section 5.3.3.4 and the ALS-102 FPGA Requirements Specification [20].

4.10.2.8.4 The PPS replacement complies with Clause 5.8.4 as discussed below:

Information displays in the control room are part of the safety systems and are unchanged from those approved for the Eagle 21 PPS [5]. The RTS instrumentation is listed in TS Table 4.3-1 of the Eagle 21 LAR [97] and the ESFAS instrumentation is listed in TS Table 3.3-3 of the Eagle 21 LAR [97].

a) Tricon-Based PPS Equipment

Triconex PPS replacement application details are provided in the Triconex SRS [75]. Platform compliance with this clause is described in Tricon V10 Topical Report Submittal [13] Section 2.1 and the Triconex DI&C-02 and -04 Compliance Report [24] Section 3.0.

b) FPGA-Based ALS PPS Equipment

ALS application details are provided in the DCPP System Design Specification [19] Section 5.3.3.4 and the ALS-102 FPGA Requirements Specification [20]. The ALS Topical Report Submittal [15] Section 12.1.9.4 discusses compliance of the ALS platform with IEEE Standard 603 Clause 5.8.4.

4.10.2.9 Clause 5.9 Control of Access (Section D.9.4.2.9 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.9 states:

The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

The location of safety related equipment is a plant specific implementation issue. In this PPS replacement, the equipment is located in a controlled area secured by the plant security system in a manner that only allows authorized personnel access. This limits the means to bypass safety system functions, via access controls, to authorized plant personnel. The PPS replacement contains design features that provide means to control physical access to safety related equipment. This includes access to PPS replacement equipment which encompasses the test points and the capabilities for changing setpoints. Keys to the cabinet doors will be maintained under the administrative control of DCPP operating staff.

The description of most of the access features is considered by PG&E to be sensitive information and, therefore, withheld from public disclosure pursuant to 10 CFR 2.390 [88].

a) Tricon-Based PPS Equipment

The Tricon has several design features to provide means to control the physical access including access to test points for verifying and changing. Control of the software and hardware during development is the responsibility of IOM. This is discussed in IOM document NTX-SER-10-14, Revision 0, "Tricon V10 conformance to RG 1.152," ML#102040062 [150] which describes the conformance of the V10 Tricon conformance to the security provisions of RG 1.152, Rev 2, "Criteria for use of Computers in Safety Systems of Nuclear Power Plants" [45]. Another document also discusses the provisions of RG 1.152, Triconex Document No. 993754-1-913, "Process Protection System Replacement DCPP RG 1.152 Conformance Report" [147].

In addition, access to equipment rooms and cabinets including the MWS will be controlled by DCPP only to personnel who are intended to have access.

b) FPGA-Based ALS PPS Equipment

Section 12.1.10 of the ALS Topical Report Submittal [15] describes the FPGA-Based ALS PPS replacement equipment conformance to Clause 5.9.

4.10.2.10 Clause 5.10 Repair (Section D.9.4.2.10 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.10 states:

The safety systems shall be designed to facilitate timely recognition, location, replacement, repair and adjustment of malfunctioning equipment.

The PPS Replacement Project is designed with monitoring features to detect both hardware and software faults and to assist in diagnostic and repair activities. Most failures are detectable within each Protection Set including the processors, I/O modules, power supplies and the communication features.

a) Tricon-Based PPS Equipment

The V10 Tricon is designed for high reliability, extensive self-diagnostics, minimal maintenance and simple on-line replacement of hardware. Maintenance and repair provisions are described in the Tricon V10 Topical Report Submittal [13].

b) FPGA-Based ALS PPS Equipment

Section 12.1.11 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 5.10

4.10.2.11 Clause 5.11 Identification (Section D.9.4.2.11of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.11 states:

In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:

Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEEE Std 384-1981 and IEEE Std 420-1982.

Components for modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.

Identification of safety system equipment shall be distinguishable from identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).

Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.

The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974.

The PPS replacement is configured in accordance with plant specific identification requirements which provide a standardized method for identifying equipment, diagrams and signals for the purpose of consistency during the replacement process. There are four Process Protection Sets each having a color coded name plate with identification for each rack identifying Protection Set I, II, III or IV. Each field wiring termination point is tagged to aid in identification. Additional details regarding DCPP can be found in the FSAR, Section 7.1.2.3 [26].

a) Tricon-Based PPS Equipment

Clause 5.11 addresses clear and distinct equipment identification. All V10 Tricon equipment is uniquely identified to assure compliance with 10CFR50 Appendix B [151] requirements as described in the IOM Corporate QAM [31].

PPS replacement components are uniquely identified by subsystem/train designations per project procedures and as defined in DCPP specification/drawings.

b) FPGA-Based ALS PPS Equipment

Section 12.1.12 of the ALS Topical Report Submittal [15] describes the FPGA-Based ALS PPS replacement equipment conformance to Clause 5.11.

4.10.2.12 Clause 5.12 Auxiliary Features (Section D.9.4.2.12 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.12 states:

Auxiliary supporting features shall meet all requirements of this standard. Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Appendix A.

The PPS replacement features (components, equipment and systems) of the PPS Replacement Project that perform safety functions satisfy the Clause 5.12 requirements of IEEE Standard 603-1991 [21] as discussed below.

The Communication architecture provides the ability to transmit information to non-safety related devices such as the MWS, PDN Gateway Switch, PDN Gateway Computer, and PPC. The communication architecture is compared with ISG-04 [2] in Section 4.8 of this LAR.

a) Tricon-Based PPS Equipment

Auxiliary features are not required for the Tricon based safety system to accomplish its safety function. At the V10 Tricon platform level, all hardware and software components are produced as safety related under the IOM 10CFR50 Appendix B [151] QA Program.

b) FPGA-Based ALS PPS Equipment

Section 12.1.13 of the ALS Topical Report Submittal [15] describes the FPGA-Based ALS PPS Replacement equipment conformance to Clause 5.12.

4.10.2.13 Clause 5.13 Multi-Unit Stations (Section D.9.4.2.13 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.13 states:

The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988.

The PPS Replacement Project does not allow sharing of any PPS structure, system, or component.

DCPP is currently committed to IEEE 308-1971 per Section 7.1.2.4 et al. of the FSAR [26]. The PPS Replacement Project will conform to IEEE-308-1980 [30] for the replacement scope only as shown in the shaded portion of Figure 4-3.

a) Tricon-Based PPS equipment

The Tricon-based PPS equipment is provided on a per unit basis with no sharing of any structure, system, or component.

b) FPGA-Based ALS PPS Equipment

Section 12.1.14 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 5.13. The ALS-based PPS equipment is provided on a per unit basis with no sharing of any structure, system, or component.

4.10.2.14 Clause 5.14 Human Factors Considerations (Section D.9.4.2.14 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.4 states:

Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.

The PPS replacement uses existing hardwired devices located on the control room vertical boards and control console. The existing operator interface using control panel mounted switches and indicators is maintained.

The PPS will share a Human System Interface (HSI) unit on CC4 that will be installed by the PCS replacement project for system health and status displays. This HSI unit will obtain PPS data through a connection to the Gateway computer.

The Main Annunciator provides non-vital 125 V DC for interrogation of alarm output contacts. Existing PPS outputs to the MAS are modified to dry contacts. The existing AC/DC converters on the PPS outputs to the MAS are deleted. Additional outputs to the MAS are provided as described in [27] and [28].

In accordance with Reference [28], The PPS HSI design should follow the guidance provided in the DCPP HSI Development Guidelines Document [37], which reference NUREG 0700 [38], and which will be implemented during development of the formal design change following receipt by PG&E of the SER approving this change.

4.10.2.15 Clause 5.15 Reliability (Section D.9.4.2.15 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 5.15 states:

For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.

a) Tricon-Based PPS Equipment

Section 2.2.12 of the Tricon V10 Topical Report Submittal [13] describes the availability and reliability analysis performed on the Tricon, per the applicable requirements of IEEE-352 [121] and EPRI TR-107330 [122]. This analysis concluded the calculated reliability and availability were greater than 99.9 percent, which exceeds the recommended goal of 99.0 percent in EPRI TR-107330 [122].

b) FPGA-Based ALS PPS Equipment

Section 5.5 of 6116-00011 Diablo Canyon PPS ALS System Design Specification [19] describes the reliability and availability analysis performed on an ALS PPS configured chassis. The analysis concluded the calculated Mean-Time-Between-Failure for a single ALS PPS configured chassis is 38,725 hours. The analysis concluded the calculated availability is 99.958 percent with an 18 month surveillance interval. The calculated availability of 99.958 percent exceeds the recommended goal of 99.0 percent in EPRI TR-107330 [122].

The analysis does not consider software because the ALS is a FPGA-based system and does not contain executable software. The analysis does consider individual component failures, including failure of components of the FPGA.

The ALS Diversity Analysis [16] provides an overview of the key design attributes for the ALS platform which are sufficient to eliminate the concern for CCF.

4.10.3 Clause 6 Sense and Command Features (Section D.9.4.3 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6 states:

In addition to the functional and design requirements in Section 5, the following requirements shall apply to the sense and command features:

Section 4.10.3.1 through 4.10.3.8 discusses the sense and command aspects of the PPS replacement. These sections provide responses to IEEE 603-1991 Clauses 6.1 through 6.8.

4.10.3.1 Clause 6.1 Automatic Control (Section D.9.4.3.1 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.1 states:

Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5.

The PPS conforms with this Clause 6.1 as discussed below:

The PPS performs sense and command functions by providing trip and actuation signals to the SSPS for use by the RTS, and ESFAS, which performs the execute functions.

The safety functions performed by the PPS and the SSPS are described in Section 4.1 of this LAR.

The PPS replacement setpoints, errors, and response times will be equal to or better than the setpoints, errors, and response times of the previously approved Eagle 21 PPS and described in Attachment B of the Eagle 21 LAR [97].

The PPS replacement adequately addresses the D3 considerations of BTP-19 as described in the approved DCPP D3 Topical Report [7]. The PPS replacement: (1) implements automatic protective functions in the Class IE software-based Triconex TRICON processor to mitigate events for which the Eagle 21 SER credited available diverse automatic mitigating functions; and (2) implements automatic protective functions in a logic-based Class IE CSI ALS that provides inherent, internal diversity to address software CCF per NRC ISG-02 [3] Position 1 and automatically mitigate events that otherwise would require manual protective action if the events were to occur with a concurrent CCF to the PPS. Refer to D3 Topical Report [6] Section 2.3.2 for details.

Requirements for the protective actions described in Section 4.1 of this LAR to be performed automatically (where currently credited with automatic initiation in the DCPP FSAR [26]) are described in the following documents:

1. DCPP Units 1 & 2 PPS Replacement FRS [28]
2. Westinghouse PPS Replacement Project ALS System Requirement Specification [17].
3. CSI document No. 6116-00011, Diablo Canyon PPS ALS System Design Specification [19]
4. CSI document No. 6116-10201 Diablo Canyon PPS ALS-102 FPGA Requirements Specification [20]

5. DCPP Tricon SRS [75]

Triconex platform compliance with this clause is discussed in Section 5.1 of the Tricon Version 9 SER [11].

ALS platform conformance is discussed in 12.1.17 of the ALS Topical Report Submittal [15].

Test Design Specifications will be provided to NRC in the PPS replacement Phase 2 documentation per DI&C-ISG-06 [1] Section D4.4.2.4. The Triconex and ALS automatic safety functions are tested during the FAT to verify that the functions perform in accordance with specified requirements.

4.10.3.2 Clause 6.2 Manual Control (Section D.9.4.3.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.2 states:

6.2.1 Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.

6.2.2 Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 that have not been selected for automatic control under 6.1.

The displays provided for these actions shall meet the requirements of 5.8.1.

6.2.3 Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.

4.10.3.2.1 The PPS replacement complies with Clause 6.2.1 as described below:

Existing means are provided in the control room for manual initiation at the division level (SSPS Train "A" and Train "B") of the automatically initiated protective actions described in Sections 4.1.23 (Manual RT), 4.1.24 (Manual SI), 4.1.25 (Manual SLI), 4.1.26, (Manual Containment Isolation Phase A), and 4.1.25, (Manual Containment Spray). These means are provided at the SSPS actuation level, downstream of the PPS, and are independent of any PPS replacement hardware or software. The PPS replacement does not affect any of the division-level manual initiation features or functions in the DCPP protection system listed in DCPP TS [42], described in the approved Eagle 21 PPS SER [5], or described in the Eagle 21 LAR [97].

4.10.3.2.2 The PPS replacement complies with Clause 6.2.3 as described below:

The PPS replacement does not affect the information provided to the operators, the actions needed of the operators, and the quantity of the associated displays and controls available to the operators compared to that of the existing Eagle 21 PPS. Safety-related controls and indicators remain Class IE; non-safety related indicators are driven by qualified isolation devices. As described in the approved PPS Replacement D3 Assessment [7], reliability and independence of non-safety indications is improved where appropriate by isolating the signals at the PPS input rather than through digital processing and isolation. The indicators are active and available as long as the instrument channel is powered, independent of digital processing.

4.10.3.2.3 The PPS replacement complies with Clause 6.2.2 as described below:

The existing means to implement manual actions at the division (SSPS Train "A" and Train "B") and the manual controls and indications required to maintain the plant in a safe condition following manual initiation are not affected adversely by the PPS replacement. Critical indications, such as those required for post-accident monitoring (PAM), are derived from raw instrument loop signals at the front end of the Replacement PPS, independent of any digital processing. Exceptions are steam flow signals and wide range RCS temperatures, where processing by the PPS is needed for compensation or signal type conversion. Isolation of non-safety related signals from safety related signals is performed by qualified isolation devices. Refer to the PPS replacement FRS [28] and IRS [29] for requirements. RCP flows are an exception, because the signals are normalized in the ALS subsystem before being output as non-safety related signals to indicators in the control room.

The existing means to implement manual actuations at the division level are not affected by the PPS replacement and need not be explicitly tested by the PPS Replacement Project. Such testing is not necessary because the controls and indications required to initiate manual actuations at the division level are periodically tested by existing DCPP surveillance test procedures.

DI&C-ISG-06 [1] advises that the manual controls required by Clause 6.2 may be different from manual actions that could be used as an acceptable diverse actuation to address BTP 7-19 Revision 6 [4], as defense against CCSF. The CCSF mitigation controls should be independent and therefore downstream of the digital portion of the safety system that is subject to the CCSF.

Means are provided in the control room for manual initiation at the division level (SSPS Train "A" and Train "B") of the automatically initiated protective actions described in

Sections 4.1.23 (Manual RT), 4.1.24 (Manual SI), 4.1.25 (Manual SLI), 4.1.26, (Manual Containment Isolation Phase A), and 4.1.27, (Manual Containment Spray). These means are provided at the SSPS actuation level, downstream of the PPS, and are independent of any PPS replacement hardware or software. The PPS replacement does not affect any of the division-level manual initiation features or functions in the DCPP protection system listed in DCPP TS [42], described in the approved Eagle 21 PPS SER [5], or described in the Eagle 21 LAR [97].

Elimination (by the PPS replacement) of manual actions credited in the Eagle 21 SER [5] for mitigation of design basis events in the event of CCSF is discussed in the approved PPS Replacement D3 Assessment [6, 7].

a) Tricon-Based PPS Equipment

Triconex platform compliance with Clause 6.2.2 is discussed in Section 5.1 of the Tricon Version 9 SER [11], and in the Tricon Version 10 ISG-02 and ISG-04 Compliance Report [24].

b) FPGA-Based ALS PPS Equipment

ALS platform conformance is discussed in 12.1.18 of the ALS Topical Report Submittal [15].

4.10.3.3 Clause 6.3 Interaction with Other Systems (Section D.9.4.3.3 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.3 states:

6.3.1 Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:

a) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:

1. *Channels that sense a set of variables different from the principal channels.*
2. *Channels that use equipment different from that of the principal channels to sense the same variable.*
3. *Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.*
4. *Both the principal and alternate channels shall be part of the sense and command features.*

b) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.

6.3.2 Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

The DCPP D3 Topical Report [6] describes the PPS replacement capability to withstand events in conjunction with a software CCF. The NRC SER [7] provides the NRC response to the analyses presented in the D3 Topical Report [6].

For events not associated with software CCF the PPS replacement design minimizes the possibility of occurrence of events described in IEEE 603, Section 6.3.1 [21]. Transmitter (sensor) inputs required by both the PPS and the control system are provided to the control system via qualified isolation devices (independent of the PPS) located on the transmitter input circuit. The analog signal for use by the control system is not processed by the PPS equipment and thus is not subject to software CCF.

RTD inputs to PPS channels are an exception. RTD inputs are conditioned (resistance to temperature) by the ALS and output to the Tricon as 4-20 mA analog signals for processing by wide range temperature channels, pressurizer vapor temperature channel, and ΔT/Tavg (DTTA) channels. The DTTA channels provide analog outputs to the rod speed and direction control system.

Similarly, analog signals to control board indicators are provided from the transmitter input circuit (isolated where required) and are not processed by the PPS and thus not subject to software CCF. Reactor coolant flow, steamline flow and PPS temperature (Wide Range Temperature, Pressurizer Vapor Temperature, and DTTA) channels are an exception. These channels process the inputs and provide analog signals to control board indicators/recorders (no control system interface).

a) Tricon-Based PPS Equipment

The Tricon Version 10 Topical Report [13] provides no additional information regarding conformance to Clause 6.3.

b) FPGA-Based ALS PPS Equipment

Section 12.1.19 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 6.3 by stating that conformance is application specific. Conformance to Clause 6.3 is discussed above.

4.10.3.4 Clause 6.4 Derivation of System Inputs (Section D.9.4.3.4 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.4 states:

To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.

The process variables and derived parameters used for the PPS replacement actuation functions are the same as those currently being used for the Eagle 21 PPS and do not change from those used by the current safety analysis.

The following reactor plant parameters are monitored by the PPS replacement as identified in Section 1.5 of the PPS FRS [28]:

- Reactor Coolant Flow (all loops)
- Wide Range Reactor Coolant Temperature (hot and cold legs, all loops)
- Wide Range Reactor Coolant Pressure (loops 3, 4)
- Narrow Range Reactor Coolant Temperature (hot and cold legs, all loops)
- Power Range Neutron Flux (from the Nuclear Instrument System)
- Pressurizer Level
- Pressurizer Pressure
- Pressurizer Vapor Temperature
- Steamline Flow (all steam generators)
- Steamline Pressure (all steam generators)
- Steam Generator Narrow Range Level (all steam generators)
- Turbine Impulse Chamber Pressure
- Containment Pressure

The Feedwater Flow signals and the Steam Flow/Feedwater Flow Mismatch alarms have been removed from the PPS replacement. The Feedwater Flow signals are non-safety related and will be input to the DFWCS, which will then generate the Steam Flow/Feedwater Flow Mismatch alarms.

a) Tricon-Based PPS Equipment

The Tricon V10 Topical Report Submittal [13] does not provide additional information regarding conformance to Clause 6.4.

b) FPGA-Based ALS PPS Equipment

The FPGA-based ALS platform will not adversely affect the performance characteristics (range, accuracy, resolution, response time, and sample rate) of the existing safety system transmitters and sensors, as discussed in Section 12.1.20 of the ALS Topical Report Submittal [15].

4.10.3.5 Clause 6.5 Capability for Testing and Calibration (Section D.9.4.3.5 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.5 states:

6.5.1 Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

(1) by perturbing the monitored variable,

(2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or

(3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.

6.5.2 One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:

(1) Checking the operational availability of sensors by use of the methods described in 6.5.1.

(2) Specifying equipment that is stable and retains its calibration during the post-accident time period.

DI&C-ISG-06 [1], Section D.9.4.3.5 states:

Clause 6.5 requires that it must be possible to check, with a high degree of confidence, the operational availability of each sense and command feature input sensors needed for a safety function during reactor operation, including the availability of each sense and command feature needed during the post-accident period. SRP Chapter 7, Appendix 7.1-C, Section 6.5, "Capability for Testing and Calibration," provides acceptance criteria for Clause 6.5.

The PPS replacement is a digital replacement for the digital Eagle 21 PPS at DCPP. The existing Technical Specification SRs for Eagle 21 are applicable to the PPS replacement. The capability for testing/calibration of the PPS replacement is not significantly different than for the Eagle 21 PPS.

The PPS replacement incorporates self-testing diagnostic features as well as range checking on all sensor inputs. A trouble alarm is generated upon detection of an input failure or an out-of-range low or out-of-range high input condition at -5 percent (low) and 105 percent (high) of span.

The capability for testing or calibration in bypass or partial-trip mode at all power levels is provided with indication of bypass provided in the control room in accordance with the requirements of RG 1.47 [105].

The PPS replacement provides the capability for Channel Checks using indications provided in the control room.

Post-accident monitoring capabilities are enhanced with the PPS replacement. With the exception of Steamflow, reactor coolant flow, and temperature (loop wide range, loop Tavg, loop ΔT, and Pressurizer vapor temperature), all provided PPS process indications are from the transmitter input (via qualified isolation devices where required) and are not processed by the digital PPS replacement equipment. The temperature, Steamflow, and reactor coolant flow analog inputs require processing (RTD conversion or square root conversion) which is performed in the PPS as is currently done with the Eagle 21 PPS.

a) Tricon-Based PPS Equipment

The Tricon V10 Topical Report Submittal [13] does not provide additional information regarding conformance to Clause 6.4.

b) FPGA-Based ALS PPS Equipment

Section 12.1.21 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 6.5 by stating that conformance is application specific. Conformance to Clause 6.5 is discussed above.

4.10.3.6 Clause 6.6 Operating Bypasses (Section D.9.4.3.6 of DI&C-ISG-06 [1])

IEEE 603-1991 [21], Clause 6.6 states:

Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall accomplish one of the following actions:

1) *Remove the appropriate active operating bypass(es).*
2) *Restore plant conditions so that permissive conditions once again exist.*
3) *Initiate the appropriate safety function(s).*

The operating bypass design and conditions for the DCPP operating bypasses have not changed as a result of replacing the Eagle 21 digital PPS with the Tricon and ALS PPS. Tricon and ALS develop the comparator outputs for the P14, P13, and P11 operating permissives which are sent to the SSPS where the interlocks are developed.

FSAR Table 7.3-3 [26] lists the operating bypasses for the ESF actuation system. This table shows the inputs and the functions performed for each of the interlocks. Likewise, FSAR Table 7.2-2 [26] lists the operating bypasses for the RTS. Interlock permissives P6, P7, P8, P9 and P10 are provided through the NIS and are independent of the PPS replacement. .

Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions for the bypass are not satisfied. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed accordingly. Indication is provided in the control room if some part of the protection system has been administratively bypassed or taken out of service.

If a protection channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room. The design for the RTS and ESFAS operating bypasses satisfy IEEE 603 Clause 6.6 [21] requirements in that the operating bypasses shown in the two tables noted above are automatically removed when plant conditions require their removal and automatically restored when plant conditions require their restoration. The ability to initiate appropriate safety functions is available at all times.

a) Tricon-Based PPS Equipment

Tricon documentation does not add any additional information pertaining to Clause 6.6.

b) FPGA-Based ALS PPS Equipment

Section 12.1.22 of the ALS Topical Report Submittal [15] describes the FPGA-based replacement equipment conformance to Clause 6.6 by stating that conformance is application specific. Conformance with Clause 6.6 is discussed above.

4.10.3.7 Clause 6.7 Maintenance Bypass (Section D.9.4.3.7 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.7 states:

Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.

EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated) that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).

Clause 6.7 of IEEE 603-1991 [21] states that the capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. Clause 6.7 further states that during such operation, the sense and command features shall continue to meet the requirements of Clauses 5.1 and 6.3, with the exception that one-out-of-two portions of the sense and command features are not required to meet Clauses 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (i.e., that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significant detrimental effect on the overall sense and command features availability). SRP Chapter 7 [4], Appendix 7.1 C, Section 6.7, "Maintenance Bypass," provides acceptance criteria for IEEE 603-1991 Clause 6.7 [21]. This acceptance criterion states that provisions for this bypass need to be consistent with the required actions of the plant TS.

FSAR Section 7.2.2.2.1.7 [26] discusses testing in bypass and presents the normal method for removing channels for maintenance. Alternatively, administrative control allows, during channel testing, that the channel output be put in a trip condition that de-energizes (operates) the input relays in SSPS Train A and Train B cabinets. Of necessity this is done on only one channel at a time. Status lights and single channel trip alarms in the control room verify that the logic input relays have been de-energized and the channel outputs are in the trip mode. An exception to this is containment spray, which is energized to actuate two-out-of-four logic and reverts to two-out-of-three logic when one channel is in the maintenance bypass mode. Only one channel can be bypassed at any one time, i.e., bypass of two or more channels at the same time shall not be allowed as per DCPP TS [42].

For the PPS replacement, the configuration control for maintenance bypass is now through the Tricon and the ALS digital platforms. The Bypassed and Inoperable status indications in the control room have not been modified as a result of the PPS replacement and continue to meet the guidance provisions of RG 1.47 [105]. As before, a PPS channel can be placed in Bypass mode to facilitate maintenance activities. Indication is provided in the control room whenever a PPS channel has been administratively bypassed for maintenance or taken out of service.

The PPS replacement is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. Use of the bypass mode disables the individual channel comparator trip circuitry that forces the associated logic input relays to remain in the non-tripped state until the "bypass" is removed. If the PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room.

The DCPP FMEA, a Phase 2 deliverable, for the PPS Replacement Project assumes that one of the initial conditions is a PPS channel that is placed in the Bypass Mode. This initial condition imposed on the FMEA determines the overall effect of an evaluated failure on the safety system's capability to perform the required safety functions in this non-conservative mode. The FMEA must show sufficient redundancy, independence and other required design fundamentals ensuring that the safety function can be performed even with a channel in the Bypass Mode.

a) Tricon-Based PPS Equipment

The MWS supports maintenance activities, such as periodic maintenance, instrument loop testing, troubleshooting, etc. The MWS normally simply displays plant parameters, perhaps including division diagnostic information. Access to features beyond displaying data, such as the maintenance bypass, will be controlled using administrative and physical controls. During maintenance, the MWS would be used for modifying trip setpoints. These activities will be performed in accordance with site-specific administrative (procedural) and physical-access controls to set and/or change Tricon safety system parameters while the channel and protection loops are OOS (i.e, in bypass or partial trip mode). Such procedures would require manipulation of the Tricon hardware out of service switch specific to a given instrument loop under test. These procedures are discussed in more detail in Section 4.2.4.5 of the LAR.

b) FPGA-Based ALS PPS Equipment

Section 12.1.23 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 6.7.

Manual bypass switches are provided for each comparator output in the ALS as described in ALS System Design Specification [19], Section 3.3.4.2.

4.10.3.8 Clause 6.8 Setpoints (Section D.9.4.3.8 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 6.8 states:

The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1987.

Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required.

The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.

The current calculations of record for the Eagle 21 PPS, a digital-based protection system, are provided in Westinghouse WCAP-11082 [39]. These setpoint calculations have been revised for the PPS replacement and are contained in Westinghouse document WCAP-17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," [171] using the setpoint methodology contained in Westinghouse document WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant" [173]. The approach used for the methodology is consistent with ISA-67.04.01- 2006 [78] and included input from RIS 2006-17 [40] and TSTF-493 R4 [41].

The revised calculations contained in Westinghouse document WCAP-17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," [171] confirm that there is adequate margin between the current TS trip setpoints and the safety limits (and analytical limits) such that the system initiates protective actions before safety limits are exceeded and that there is adequate margin between operating limits (or alarm limits) and trip setpoints such that there is a low probability for inadvertent actuation of the system. Table 4-10 provides the summary of the analytical limits and current TS setpoints for the PPS.

4.10.4 Clause 7 Execute Features (Section D.9.4.4 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 7 states (in part):

In addition to the functional and design requirements in Section 5, the following requirements shall apply to the execute features.

Section 4.10.4.1 through 4.10.4.5 of this LAR discuss the execute features of the PPS replacement. These sections comply with and provide responses to IEEE 603-1991 [21] Clauses 7.1 through 7.5.

4.10.4.1 Clause 7.1 Automatic Control (Section D.9.4.4.1 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 7.1 states:

Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis.

Table 4-10 Total Loop Uncertainty

Trip Function	Analytical Limit	Current DCPP TS Setpoint
Overtemperature ΔT	Function (Note 1)	Function (Note 2)
Overpower ΔT	Function (Note 1)	Function (Note 2)
Pressurizer Pressure – Low, RT	1845 PSIG	1950 PSIG
Pressurizer Pressure – High	2445 PSIG	2385 PSIG
Pressurizer Water Level – High	Not used in Safety Analysis	90% Span
Loss of Flow	85% Flow	90% Flow
Steam Generator Water Level – Low-Low	0% Span	15% Span
Containment Pressure – High	5 PSIG	3 PSIG
Containment Pressure – High-High	24.7 PSIG	22.0 PSIG
Pressurizer Pressure – Low, SI	1680 PSIG	1850 PSIG
Steamline Pressure – Low (Rosemount)	444.0 PSIG	600 PSIG
Steamline Pressure – Low (Barton)	444.0 PSIG	600 PSIG
Steam Generator Water Level – High-High	98.78% Span	90.0% Span
RCS Loop ΔT Equivalent To Power - ΔT	59% RTP	50% RTP

Note 1: As noted in Figure 15.1-1 of Updates FSAR

Note 2: As noted in Table 2.2-1 of DCPP TS

IEEE Standard 603-1991 [21], Clause 4.4 states:

The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.

The PPS conforms with Clause 7.1 as discussed below:

The PPS performs sense and command functions by providing trip and actuation signals to the SSPS for use by the RTS, and ESFAS. PPS protection outputs provide ON/OFF (partial trip) signals to the two trains of the SSPS whenever measured parameters indicate that safety limits are being approached (a pre-established setpoint is exceeded). The SSPS initiates a RT or actuates ESFAS when the requisite number of PPS channels have tripped (designed coincidence logic is satisfied).

Thus, execute features of the overall DCPP RPS are performed by the existing SSPS illustrated in Figure 4-1 of this LAR and the before and after PPS replacement depictions in Figure 4-2 and Figure 4-3, respectively. The SSPS and the functions it performs are described in Section 4.1 of this LAR.

RT, once initiated either automatically or manually, proceeds to completion because the mechanical action of the RT circuit breakers (also shown in Figures 4-2 and 4-3) require an external electrical reset command to reclose the breakers. The ESFAS functions described in Section 4.1 proceed to completion because the output signals from the SSPS are electrically latched and seal-in on command. These signals also require a manual operator action to unlatch them. In addition, the SI signal has a timer that prevents manual reset by the operator for 30 seconds following SI actuation to ensure the SI proceeds to completion.

The above execute features and functions are not affected by the PPS replacement, as illustrated in Figure 4-2 of this LAR.

4.10.4.2 Clause 7.2 Manual Control (Section D.9.4.4.2 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 7.2 states:

If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.

The PPS replacement conforms to Clause 7.2 as discussed in the IEEE Standard 603 Clause 6.2 response in Section 4.10.3.2 of this LAR.

4.10.4.3 Clause 7.3 Completion of Protective Action (Section D.9.4.4.3 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 7.3 states:

The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function.

Clause 7.3 requires that the design of the execute features be such that once initiated, the protective actions of the execute features shall go to completion. However, this requirement does not preclude the use of equipment protective devices identified in Clause 4.11 of the design basis or the provision for deliberate operator interventions. Additionally, when the sense and command features reset, the execute features shall not automatically return to normal, but shall need separate, deliberate operator action to be returned to normal.

All execute features are performed by the SSPS. The execute features of the plant protection system are not changed. The SSPS is not being revised as part of the PPS Replacement Project and it functionality remains the same. RT and ESFAS actuation protection functions are not changed or modified by the PPS Replacement Project.

The PPS monitors plant parameters and sends partial trip/actuation signals to the SSPS when predetermined setpoints are exceeded. The SSPS provides sealed-in RT or ESFAS actuation signals when the coincidence logic for a particular trip/actuation function is satisfied. The SSPS does not require manual intervention or acknowledgement of actuation commands to complete a protective function. The SSPS RT or ESFAS actuation signal requires manual action to reset following completion of the protective action and only after the PPS initiating signals have reset.

4.10.4.4 Clause 7.4 Operating Bypasses (Section D.9.4.4.4 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 7.4 states:

Whenever the applicable conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety *function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*

Remove the appropriate active operating bypass(es).

Restore plant conditions so that permissive conditions once again exist.

Initiate the appropriate safety function(s).

The requirements of IEEE Standard 603-1991 Clause 7.4 [21] require that if applicable conditions are not met, a safety system must automatically prevent the activation of an operating bypass or initiate the appropriate safety function, and if plant conditions change so that an activated operating bypass is no longer permissible, the safety system must either remove the appropriate active operating bypass, restore plant conditions so that the permissive conditions once again exist, or initiate the appropriate safety function(s). This is the same as the requirements for Clause 6.6 [21] except the requirements are for the executive feature and not the sense and command features.

The operating bypasses are performed by the SSPS and are not performed by the PPS. The existing SSPS operating bypass functions are maintained with the Tricon and ALS PPS replacement. They are automatically removed when plant conditions change to an operating mode in which protective actions are required to be operable so that a design basis event can be mitigated.

4.10.4.5 Clause 7.5 Maintenance Bypass (Section D.9.4.4.5 of DI&C-ISG-06 [1])

IEEE Standard 603-1991 [21], Clause 7.5 states:

The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.

Clause 7.5 of IEEE 603-1991 [21] states that the capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Furthermore it provides for acceptability of reducing redundancy to zero if the reliability of the execute features equipment is acceptable and reliability of equipment operation is otherwise demonstrated (i.e., that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significant detrimental effect on the overall execute features availability). SRP Chapter 7, Appendix 7.1 C, Section 7.5 [4], "Maintenance Bypass," provides acceptance criteria for IEEE 603-1991 Clause 7.5 [21]. This acceptance criterion states that provisions for this bypass need to be consistent with the required actions of the plant TS.

The execute features and maintenance bypass functions are performed by the SSPS and are not being revised as part of the PPS Replacement Project. The Tricon and ALS PPS replacement only impacts the command features. The DCPP safety systems are still capable of accomplishing their safety functions when the execute features equipment is in bypass. The maintenance bypass features remain consistent with the required actions of the existing DCPP TS.

a) Tricon-Based PPS Equipment

There is no impact by the Tricon on the separate SSPS bypass functions.

There are no communications switches in the architecture and there is no direct access to safety-related Protection Set communications from outside the Protection Set.

b) FPGA-Based ALS PPS Equipment

There is no impact by the ALS on the separate SSPS bypass functions.

4.10.5 Clause 8 Power Source (Section D.9.4.5 of DI&C-ISG-06 [1])

DI&C-ISG-06 [1], Section D.9.4.5 states:

Clause 8 provides the requirements for the power sources supporting the digital I&C system. Clause 8 requires that those portions of the Class 1E power system that are needed to provide the power to the many facets of the safety system are governed by the criteria of IEEE Std 603-1991 and are considered a portion of the safety systems. Clauses 8.1 and 8.2 apply the requirements of IEEE Std 603-1991 to electrical and non-electrical power sources, respectively.

Clause 8.3 requires that the capability of the safety system to accomplish its safety function be retained when the power source is in maintenance bypass. Additionally, portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability.

4.10.5.1 Clause 8.1, Electrical Power Sources

IEEE Standard 603-1991 [21], Clause 8.1 states:

Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1980.

DCPP is currently committed to IEEE 308-1971 per Section 7.1.2.4 et al. of the FSAR [26]. The PPS Replacement Project will conform to IEEE-308-1980 for the replacement scope only as shown in the shaded portion of Figure 4-3.

The PPS replacement utilizes the existing Class 1E power sources provided for use by the Eagle 21 PPS without change. Each PPS replacement Protection Set is powered from a separate 120 V AC vital bus via a Class 1E uninterruptible power supply as stated in Section 3.1.1.4 of the PPS FRS [28]. DCPP Class 1E power sources are implemented as stated in Section 8.1.1.4 of the DCPP FSAR [26].

Class 1E power sources used by safety systems actuated by signals generated from the PPS replacement are not affected by the PPS Replacement Project.

4.10.5.2 Clause 8.2, Non-Electrical Power Sources

IEEE Standard 603-1991 [21], Clause 8.2 states:

Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.

The PPS replacement does not rely on non-electrical power sources for performance of its safety related functions. The PPS replacement does not affect any non-electrical power source used by any safety system that is actuated based on signals generated by the PPS replacement in a manner different from the existing Eagle 21 PPS (e.g., PORV and Main Steam Isolation Valve actuator bottled gas backup systems).

4.10.5.3 Clause 8.3, Maintenance Bypass

IEEE Standard 603-1991 [21], Clause 8.3 states:

The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.

The PPS replacement is required to be operational in all modes as specified in the DCPP TS [42]. In order to satisfy TS requirements, safety related power must be maintained to the PPS replacement when it is required to be operational.

The redundant power sources to the replacement PPS have not changed. If an external power source for a safety-related Protection Set (or division) fails, the remaining safety-related Protection Sets (divisions) will ensure that the safety system remains capable of performing the assigned safety function.

Additional redundancy to assure reliability is provided within the Protection Sets as described below.

a) Tricon-Based PPS Equipment

Version 10 Tricon chassis power supplies are qualified Class 1E power modules. Each chassis has two redundant chassis power supplies that can be supplied from separate redundant external power sources. Each chassis power supply is capable of supplying full chassis load in the event of failure (or bypass) of the other power supply. See Section 2.1.2.5 of the Tricon Version 10 Topical Report Submittal [13].

b) FPGA-Based ALS PPS Equipment

Section 12.1.30 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 8.0.

4.11 Conformance with IEEE Standard 7-4.3.2 (Section D.10 of DI&C-ISG-06 [1])

The PPS replacement is a digital system replacement for the digital Eagle 21 PPS. As such, it requires conformance with RG 1.152 [45] which endorses IEEE Standard 7-4.3.2 [80]. Compliance with IEEE Standard 7-4.3.2 [80] is discussed in the following Sections.

4.11.1 Clause 5 System (Section D.10.4.2 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5 states:

The following subclauses list the safety system criteria in the order they are listed in IEEE Std 603-1998. For some criteria, there are no additional requirements beyond what is stated in IEEE Std 603-1998. For other criteria, additional requirements are described in 5.1 through 5.15.

LAR Section 4.11.1 provides the PPS replacement conformance with IEEE Standard 7-4.3.2-2003 [80] Clauses 5.1 through 5.15.

IEEE Standard 7-4.3.2-2003 [80], Clause 5.1, Single-Failure Criterion, states:

No requirements beyond IEEE Std 603-1998 are necessary (see also Annex B).

LAR Section 4.10.2.1 addresses the issues associated with Clause 5.1.

IEEE Standard 7-4.3.2-2003 [80], Clause 5.2, Completion of Protection Action, states:

No requirements beyond IEEE Std 603-1998 are necessary.

LAR Section 4.10.2.2 addresses the issues associated with Clause 5.2.

4.11.1.1 Clause 5.3 Quality (Section D.10.4.2.3 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.3 states:

Hardware quality is addressed in IEEE Std 603-1998. Software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards. Computer development activities shall include the development of computer hardware and software. The integration of the computer hardware and software and the integration of the computer with the safety system shall be addressed in the development process.

A typical computer system development process consists of the following life cycle processes:

- *Creating the conceptual design of the system, translation of the concepts into specific system requirements*
- *Using the requirements to develop a detailed system design*
- *Implementing the design into hardware and software functions*
- *Testing the functions to assure the requirements have been correctly implemented*
- *Installing the system and performing site acceptance testing*
- *Operating and maintaining the system*
- *Retiring the system*

In addition to the requirements of IEEE Std 603-1998, the following activities necessitate additional requirements that are necessary to meet the quality criterion:

- *Software development*
- *Qualification of existing commercial computers (see 5.4.2)*
- *Use of software tools*
- *Verification and validation*
- *Configuration management*
- *Risk Management*

LAR Sections 4.11.1.1.1 through 4.11.1.1.6 address the issues associated with Criterion 5.3.

a) Tricon-Based PPS Equipment

Triconex software development and system integrity was evaluated and accepted by the NRC in the Tricon V9 SER [11]. Tricon V10 software quality conformance with Clause 5.3 is described in the V10 Topical Report Submittal [13].

b) FPGA-Based ALS PPS Equipment

Section 12.2.4 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 5.3.

4.11.1.1.1 Clause 5.3.1 Software Development (Section D.10.4.2.3.1 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [76] Clause 5.3.1 states:

Computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996. The software QA plan shall address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can be found in IEC 60880 (1986-09) [B4] and IEEE Std 730™-1998 [B8].

IEEE Standard 7-4.3.2-2003 [76] Clause 5.3.1.1 states:

The use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following life cycle phase characteristics should be considered:

- *Correctness/Completeness (Requirements phase)*
- *Compliance with requirements (Design phase)*
- *Compliance with design (Implementation phase)*
- *Functional compliance with requirements (Test and Integration phase)*
- *On-site functional compliance with requirements (Installation and Checkout phase)*
- *Performance history (Operation and Maintenance phase)*

The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Std 1061™-1998 [B11] provides a methodology for the application of software quality metrics.

Section 4.5 of this Enclosure provides a complete description of the Software Development Process for the PPS Replacement Project.

The DCPP SyQAP for the PPS Replacement Project [52] establishes the goals, processes, and responsibilities required to implement effective software quality management for the PPS system software at DCPP.

a) Tricon-Based PPS Equipment

The Software QAP 993754-1-801 [71] establishes the activities to be followed in the design, development, review, and testing of the PPS replacement. Additional details on the Triconex software development process are included in Section 4.5 of this Enclosure.

b) FPGA-Based ALS PPS Equipment

The 6002-00001 ALS QA Plan [63] established the techniques, procedures, and methodologies to be followed in the design, development, review, and testing of the PPS replacement. Additional details on the ALS software development process are included in Section 4.5 of this Enclosure.

4.11.1.1.2 Clause 5.3.2 Software Tools Section D.10.4.2.3.2

IEEE Standard 7-4.3.2-2003 [76] Clause 5.3.2 states:

Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management. One or both of the following methods shall be used to confirm the software tools are suitable for use:

a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.

b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects.

a) Tricon-Based PPS Equipment

Section 2.3.3 of the Tricon V10 Topical Report Submittal [13] discusses the TUV-Rheinland hardware and software evaluation of V10.2.1. This evaluation included the application development tools software, TriStation 1131. In addition to the TriStation 1131, Triconex utilizes a validation tool which was developed under the Triconex 10CFR50 Appendix B QA program, called the Emulator Test Driver, which is addressed in the Triconex SQAP [71].

b) FPGA-Based ALS PPS Equipment

Section 12.2.7 of CSI document No. 6002-00301 ALS Topical Report Submittal [15] discusses the software tools used to support the development processes and V&V processes for the ALS platform.

The CSI tool assessment and qualification is performed using the CSI document No. 6002-00030 ALS Design Tools [126].

4.11.1.1.3 Clause 5.3.3 Verification and Validation (Section D.10.4.2.3.3 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.3 states:

NOTE-See IEEE Std 1012-1998 and IEEE Std 1012a^{TM}-1998 [B10] for more information about software V&V.

V&V is an extension of the program management and systems engineering team activities. V&V is used to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements regarding the expected operating conditions across the full spectrum of the system and its interfaces.

V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, e valuation, review, inspection; and testing of products and processes.

This standard adopts the IEEE Std 1012-1998 terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.

V&V processes shall address the computer hardware and software integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.

The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces.

The software V&V effort shall be performed in accordance with IEEE Std 1012-1998. The IEEE Std 1012-1998 V&V requirements for the highest integrity level (level 4) apply *to systems developed using this Std (i.e., IEEE Std 7-4.3.2). See IEEE Std 1012-1998 Annex B for a definition of integrity level 4 software.*

In following the LAR format recommended in DI&C-ISG-06 [1], this subject is addressed in Section 4.5.6 of this Enclosure.

4.11.1.1.4 Clause 5.3.4 Independent V&V (IV&V) (Section D.10.4.2.3.4 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.4 states:

The previous section addresses the V&V activities to be performed. This section defines the levels of independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence. These parameters are described in Annex C of IEEE Std 1012-1998.

The development activities and tests shall be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.

Oversight of the IV&V effort shall be vested in an organization separate from the development and program management organizations. The V&V effort shall independently select:

a) The segments of the software and system to be analyzed and tested,

b) The V&V techniques, and

c) The technical issues and problems upon which to act.

The V&V effort shall be allocated resources that are independent of the development resources.

See Annex C of IEEE Std 1012-1998 for additional guidance.

In following the LAR format recommended of DI&C-ISG-06 [1], this subject is addressed in Section 4.5.6 of this Enclosure. Additional information is provided here to address organizational alignment for each vendor for complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.4 and BTP-7-14 [4].

a) Tricon-Based PPS Equipment

Section 2.3.3 of the Tricon V10 Topical Report Submittal [13] provides an overview of the Software V&V Process for the Tricon. For the PPS replacement, a project specific IOM SVVP Section 4 [73], describes the independence of software V&V activities for the software development cycle including the organizational chart showing the different reporting chain of command for V&V functions from that of the design functions for the project. This supports technical, managerial and financial independence which are critical criteria in establishing the basis for independence. The V&V team is made up of personnel who are not involved in the development of the software and are sufficiently proficient in software engineering to ensure that software V&V is adequately implemented. The independent verifiers are also knowledgeable regarding nuclear safety applications. The V&V team reports to the IOM Nuclear IV&V Director who reports directly to the IOM Senior Vice President of Delivery and indirectly to the IOM Quality Management.

b) FPGA-Based ALS PPS Equipment

Section 6.3 of the ALS Topical Report Submittal [15] provides an overview of the Software Verification and Validation process for the ALS. V&V activities are performed in a bottom-up fashion that progresses from the FPGA digital logic programming level, to the board level, and then up to the system level. The IV&V team is independent in management, schedule and finance. The specific guidance for V&V of the DCPP PPS Replacement Project is included in Reference [54], including roles and responsibilities for assigned personnel.

4.11.1.1.5 Clause 5.3.5 Software Configuration Management (Section D.10.4.2.3.5 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.5 states:

Software configuration management shall be performed in accordance with IEEE Std 1042-1987. IEEE Std 828^{TM}-1998 provides guidance for the development of software configuration management plans.

The minimum set of activities shall address the following:

a) Identification and control of all software designs and code

b) Identification and control of all software design functional data (e.g., data templates and data bases)

c) Identification and control of all software design interfaces

d) Control of all software design changes

e) Control of software documentation (user, operating, and maintenance documentation)

f) Control of software vendor development activities for the supplied safety system software

g) Control and retrieval of qualification information associated with software designs and code *h) Software configuration audits*

i.) Status accounting

Some of these functions or documents may be performed or controlled by other QA activities. In this case, the software configuration management plan shall describe the division of responsibility.

A software baseline shall be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline shall be added to the baseline.

The labeling of the software for configuration control shall include unique identification of each configuration item, and revision and/or date time stamps for each configuration item.

Changes to the software/firmware shall be formally documented and approved consistent with the software configuration management plan. The documentation shall include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version).

In following the LAR format recommended in DI&C-ISG-06 [1], this subject is addressed in Section 4.5.7 of this Enclosure.

4.11.1.1.6 Clause 5.3.6 Software Project Risk Management (Section D.10.4.2.3.6 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.6 states:

Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer -system to perform safety related functions. Software project risk management differs from hazard analysis, as defined in 3.1.3 1, in that hazard analysis is focused solely on the technical aspects of system failure mechanisms.

Risk management shall include the following steps:

a) Determine the scope of risk management to be performed for the digital system.

b) Define and implement appropriate risk management strategies.

c) Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project.

d) Analyze risks to determine the priority for their mitigation.

e) Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions.)

f) Take corrective actions when expected quality is not achieved.

g) Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Additional guidance on the topic of risk management is provided in IEEE/EIA 12207.0-1996, and IEEE Std 1540TM-2001.

In following the LAR format recommended by DI&C-ISG-06 [1], this subject is addressed in Section 4.5.1 of this Enclosure. Additional information is provided here to address organizational alignment for each vendor in complying with IEEE Standard 7-4.3.2-2003 [80], Clause 5.3.6 and BTP-7-14 [4].

a) Triconex-Based PPS Equipment

Triconex uses a standardized project management process to assess risks, as described in Section 3.4 and 3.5 of the Triconex DCPP Software PMP [69]. This methodology is used to identify, assess, monitor, and control areas of risk that arise during the software development project. In the course of project execution, the project risks are monitored, and the current assessment is reviewed to determine if it needs to be modified.

b) FPGA-Based ALS Equipment

As described in Reference [15], Section 12, risk management for the ALS platform is a part of the SDP. This is included as part of the Life Cycle and is documented in the ALS Management Plan [59]. The ALS Life Cycle Management Process is described in Section 6 of the ALS Management Plan [59].

4.11.1.2 Clause 5.4 Equipment Qualification (Section D.10.4.2.4 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.4 states:

In addition to the equipment qualification criteria provided in IEEE Std 603-1998, the requirements listed in 5.4.1 and 5.4.2 are necessary to qualify digital computers for use in safety systems."

IEEE Standard 7-4.3.2 [80] Clauses 5.4.1 and 5.4.2 address computer system testing and qualification of existing commercial computers, respectively. Computer system qualification testing is discussed in Section 4.5 of this enclosure.

A multi-level test program is used to ensure quality in the hardware and software products. The testing addresses the hardware and software used, from input to output terminals. The testing also includes the MWS and the ASU. The overall qualification testing includes the following, as described in Section 4.11.1.2.1:

- Component Testing
- Qualification Testing
- Development Testing

PPS replacement equipment qualification testing for both the Tricon and ALS, was performed with the computers functioning, with software and diagnostics as representative of operational service. Future testing, including factory acceptance, installation and post-installation, will be performed with the computers fully functional as well. All portions of the computer used for safety functions, or whose operation or failure could impair safety functions, will be tested. The testing will demonstrate compliance with performance requirements related to safety functions.

a) Tricon-Based PPS Equipment

The equipment qualification for the Tricon platform being installed at DCPP is described in the Triconex Tricon V10 Topical Report Submittal [13], which was submitted to the NRC on May 15, 2012.

b) FPGA-Based ALS PPS Equipment

The equipment qualification for the ALS platform being installed at DCPP is described in the ALS Topical Report Submittal [15]. Equipment qualification information is provided in Section 4 of the ALS Topical Report Submittal [15]. There are no differences between the ALS platform submitted for generic approval and the ALS system being installed at DCPP.

4.11.1.2.1 Clause 5.4.1 Computer System Testing (Section D.10.4.2.4.1 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [76] Clause 5.4.1 states:

Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the *memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.*

a) Tricon-Based PPS Equipment

The Tricon PLC has been qualified in accordance with EPRI TR- 107330, which included extensive testing and encompasses IEEE- 7-4.3.2. The Tricon V9 system was endorsed in a NRC SER [11]. Changes for V10 of the Tricon platform were further qualified to the same standard (TR-107330) per Tricon V10 Topical Report Submittal [13]. IEEE 7-4.3.2 aspects were reviewed in the Software Qualification Report 9600164-535 [124] and Critical Digital Review 9600164-539 [125].

The Triconex Software V&V Plan [73] provides the scope and content of the V&V program for the IOM scope of the PPS replacement as described in Section 4.5.6 of this Enclosure. The Triconex Software Validation Test Plan [74] provides and scope and content of the test program for the IOM scope of the PPS Replacement Project as described in Section 4.5.8 of this Enclosure.

b) FPGA-Based ALS PPS Equipment

Section 12.2.12.1 of 6002-00301 ALS Topical Report Submittal [15] describes the qualification testing and how the testing meets the requirement of Clause 5.4.1.

The ALS V&V Plan [54] provides the scope and content of the V&V program for the CSI scope of the PPS replacement as described in Section 4.5.6 of this Enclosure. The ALS Diablo Canyon System Test Plan [67] describes scope and content of the test program for the CSI scope of the PPS Replacement Project as described in Section 4.5.8 of this Enclosure.

4.11.1.2.2 Clause 5.4.2 Qualification of Existing Commercial Computers (Section D.10.4.2.4.2 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.4.2, Qualification of commercial computers states:

NOTE—See Annex C for more information about commercial grade item dedication.

The qualification process shall be accomplished by evaluating the hardware and software design using the criteria of this standard. Acceptance shall be based upon evidence that the digital system or component, including hardware, software, firmware, and interfaces, can perform its required functions. The acceptance and its basis shall be documented and maintained with the qualification documentation.

In those cases in which traditional qualification processes cannot be applied, an alternative approach to verify a component is acceptable for use in a safety-related *application is commercial grade dedication. The objective of commercial grade dedication is to verify that the item being dedicated is equivalent in quality to equipment developed under a 10 CFR 50 Appendix B program [B16].*

The dedication process for the computer shall entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can achieve the safety function. The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware shall, whenever possible, include an evaluation of the design process. There may be some instances in which a design process cannot be evaluated as part of the dedication process. For example, the organization performing the evaluation may not have access to the design process information for a microprocessor chip to be used in the safety system. In this case, it would not be possible to perform an evaluation to support the dedication. Because the dedication process involves all aspects of life cycle processes and manufacturing quality, commercial grade item dedication should be limited to items that are relatively simple in function relative to their intended use.

Commercial grade item dedication involves preliminary phase and detailed phase activities. These phase activities are described in 5.4.2.1 through 5.4.2.2.

5.4.2.1 Preliminary phase of the COTS dedication process

In the preliminary phase, the risks and hazards are evaluated, the safety functions are identified, configuration management is established, and the safety category of the system is determined.

5.4.2.1.1 Evaluate the system safety function risks and hazards

An analysis shall be performed to identify the functional and performance requirements of the safety system. This analysis shall identify the risks and hazards that could interfere with accomplishing the safety function.

5.4.2.1.2 Identify the safety function(s) the COTS item shall perform

Once the system-level functions have been identified and the risks and hazards have been evaluated, the dedicating organization shall identify the safety functions to be performed by the COTS item. This process shall address all safety functions to be performed by the COTS, and the potential affect of the COTS function(s) on other safety-related functions or interfaces.

5.4.2.1.3 Establish configuration management controls

COTS items to be used in safety systems shall be controlled in a configuration management process that provides traceability of the COTS item development life cycle processes.

5.4.2.2 Detailed phase of the COTS dedication process

Following this preliminary phase of commercial dedication, the commercial grade item is evaluated for acceptability using detailed acceptance criteria. The critical characteristics by which a COTS item will be evaluated for use in a safety system shall be identified by a technical evaluation. Each critical characteristic shall be verifiable (e.g., by inspection, analysis, demonstration, or testing). This standard uses the following three categories of commercial grade item critical characteristics:

- *Physical characteristics include attributes such as physical dimensions, power requirements, part numbers, hardware and software model and version numbers, and data communication physical requirements.*
- *Performance characteristics include attributes such as response time, human-machine functional requirements, memory allocation, safety function performance during abnormal conditions, reliability, error handling, required imbedded functions, and environmental qualification requirements (e.g., seismic, temperature, humidity, and electromagnetic compatibility).*
- *Development process characteristics include attributes such as supporting life cycle processes (e.g., verification and validation activities, configuration management processes, and hazard analyses), traceability, and maintainability.*

As part of defining these critical characteristics, analyses shall identify potential hazards that could interfere with the safety functions (see Annex D).

Annex C describes the processes that should be used individually or in combination to evaluate the physical, performance, and development process critical characteristics.

5.4.2.3 Maintenance of commercial dedication

If computer hardware, software, or firmware has been procured as a commercial grade item and accepted through a commercial dedication process, then changes to the commercially dedicated computer hardware, software, or firmware shall be traceable through formal documentation.

Changes to the commercially dedicated computer hardware, software, or firmware shall be evaluated in accordance with the process that formed the basis for the original acceptance. Included in this evaluation shall be consideration of the potential impact that computer hardware revisions may have on software or firmware. If any elements of *the approved process have been omitted during the computer hardware, software, or rewire revision process, further evaluation shall be required.*

Commercial grade dedication of computer hardware, software, or rewire is performed for a septic safety system application. Use of a commercially dedicated item in safety system applications beyond that included in the baseline dedication shall require additional evaluation for the new application.

Documentation supporting the commercial grade item dedication shall be maintained as a configuration item.

IEEE Standard 7-4.3.2 [80] Clauses 5.4.1 and 5.4.2 address computer system testing and qualification of existing commercial computers, respectively. Computer system qualification testing is discussed in Section 4.5 of this enclosure.

The PPS replacement equipment does not contain any commercial digital computers. All components are qualified in accordance with References [13] and [15]. Therefore, Clause 5.4.2 does not apply.

4.11.1.2.3 CLAUSE 5.4.3 Deterministic System Behavior (Section 3.10.1.2.3 of DI&C-ISG-06 [1])

Deterministic behavior for the PPS replacement is addressed in Section 4.4 of this Enclosure and in the approved Tricon V9 Topical Report [8] (Section 3.3.3 and Appendix A Section 4.4.1.3) and ALS Topical Report Submittal [15] Sections 2.2.1, 2.3.4, 3.1, and 12.1.7.

4.11.1.2.4 Performance – System Response Time (Section 3.10.1.2.4 of DI&C-ISG-06 [1])

Response time analysis is addressed in Section 4.2.12, System Response Time, of this Enclosure.

4.11.1.3 Clause 5.5, System Integrity (Section D.10.4.2.5 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.5 states:

In addition to the system integrity criteria provided in IEEE STD 603-1998, the following are necessary to achieve system integrity in digital equipment for use in safety systems:

- *Design for computer integrity*
- *Design for test and calibration*
- *Fault detection and self-diagnostics*

In addition to the system integrity discussed in IEEE Standard 603 [21] and the guidance in NUREG 0800 Appendix 7.1-C, IEEE Standard 7-4.3.2-2003 [80] includes criteria in sub-clauses 5.5.1 thru 5.5.3 on designs for computer integrity, test and calibration, fault detection and self-diagnostics activities.

a) Tricon-Based PPS Equipment

The Tricon has been designed and tested to confirm that the equipment demonstrates system performance adequate to ensure completion of protective actions over the range of transient and steady state plant conditions. Failure modes are discussed in Paragraph 2.2.11 of the Tricon V10 Topical Report Submittal [13].

b) FPGA-Based ALS Equipment

The ALS equipment has been designed and tested to confirm that the equipment demonstrates system performance adequate to ensure completion of protective actions over the range of transient and steady state plant conditions. Failure modes are discussed in Section 7.1 of the ALS Topical Report Submittal [15].

4.11.1.3.1 Clause 5.5.1, Design for Computer Integrity (Section D.10.4.2.5.1of DI&C-ISG-06 [1])

IEEE 7-4.3.2-2003 [80], Clause 5.5.1 states:

The computer shall be designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. For example, input and output processing failures, precision or roundoff problems, improper recovery actions, electrical input voltage and frequency fluctuations, and maximum credible number of coincident signal changes.

If the system requirements identify a safety system preferred failure mode, failures of the computer shall not preclude the safety system form being placed in that mode. Performance of computer system restart operations shall not result in the safety system being inhibited from performing its function.

a) Tricon-Based PPS Equipment

From Reference [13], Sections 2.1.1 and 2.1.2.6, the Tricon is triple redundant from input terminal to output terminal. The TMR architecture is intended to allow system operation in the presence of any single point of failure within the system. The TMR architecture is also intended to allow the Tricon to detect and correct individual faults on-line, without interruption of monitoring, control and protection capabilities. In the presence of a fault, the Tricon alarms the condition, removes the affected portion of the faulted module from operation, and continues to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

The Tricon main chassis is powered by two redundant power supply modules in the chassis which are rated to each provide the power requirements of a fully populated chassis. On the main Tricon chassis, the alarm contacts on both power supply modules actuate on the states listed in Section 4.11.1.3.3 below. In addition, at least one of the chassis power supply alarm contacts actuates when the following power condition exists:

- A power supply module fails
- Primary power to a power supply module is lost
- A power module has a low battery or over temperature condition

b) FPGA-Based ALS PPS Equipment

As described in Reference [15], Sections 2 and 3, the ALS platform is designed with redundancy and embedded self-test capability to ensure system integrity by detecting and announcing faults. Diagnostics and testing capabilities are designed into the ALS platform to ensure there is a systematic approach to maintaining and testing the system.

From Reference [15] Section 2.6.2, each ALS safety system cabinet contains two qualified, independent AC/DC power supplies. Each power supply is capable of providing 150 percent of the cabinet load, and operates in a redundant configuration. The cabinet load consists of all ALS platform components and peripheral devices. Power supply failures (loss of output voltage) and opening of distribution breakers are alarmed.

4.11.1.3.2 Clause 5.5.2 Design for Test and Calibration (Section D.10.4.2.5.2 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2 [80], Clause 5.5.2 states:

Test and calibration functions shall not adversely affect the ability of the computer to perform its safety function. Appropriate bypass of one redundant channel is not considered an adverse effect in this context. It shall be verified that the test and calibration functions do not affect computer functions that are not included in a calibration change (e.g., setpoint change).

V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data.

V&V, configuration management, and QA shall be required when the test and calibration function is inherent to the computer that is part of the safety system.

V&V, configuration management, and QA are not required when the test and calibration function is resident on a separate computer and does not provide the sole verification of test and calibration data for the computer that is part of the safety system.

The PPS replacement complies with Clause 5.5.2 as described below:

The PPS replacement permits any individual instrument channel to be maintained and calibrated in a bypassed condition, and, when required, tested during power operation without initiating a protective action at the system level. This is accomplished without lifting electrical leads or installing temporary jumpers. The PPS permits periodic testing during reactor power operation without initiating a protective action from the channel under test.

External hardwired switches are provided on PPS trip and actuation outputs. The switches may be used for SSPS input relay testing or to trip or actuate the channel manually if needed. Activation of the external trip switches is indicated in the control room through the SSPS partial trip indicators. Actuation of bypass switches is indicated through the MAS.

For both the Triconex and ALS subsystems, the platform self-tests and the application specific test and calibration functions will be verified during the FAT to ensure that the Protection Set safety function is not adversely affected by performance of either built-in or application specific test and calibration functions.

a) Tricon-Based PPS Equipment

Figure 4-10 in this LAR illustrates the Tricon DO loopback feature, which enables the PPS to determine if the external trip switch is open, or if the DO channel is producing an erroneous output. A PPS trouble alarm is generated if the instrument loop is not out of service and if the comparator output is true (commanding an energized output) and the de-energize to trip DO loopback is sensed as de-energized. A PPS failure alarm is generated if the de-energize to trip DO loopback is sensed as energized and the comparator output is false (commanding a de-energized output), whether or not the instrument loop is out of service.

On-line testing in the Tricon is controlled by the non-safety related MWS and by safety related logic enabled via an external safety related hardwired out of service switch. When the out of service switch is activated, the safety related logic in the associated Protection Set allows the associated instrument channel to be taken out of service while maintaining the rest of the instrument channels in the Protection Set operable; that is, an individual out of service switch only removes an individual instrument channel from service and no other instrument channel. If the out of service switch is returned to the normal position during test, the safety related logic automatically restores the instrument channel to safety related operation.

The test and calibration functions are initiated by the non-safety related MWS, but are controlled by the safety related Triconex processor application program. There is one Tricon MWS per Protection Set to ensure that a test or calibration function on one Protection Set will take place only on the Protection Set for which the action is intended, and that only one Protection Set can be affected by actions taken at any single MWS. The MWS from one Protection Set cannot communicate with any other Protection Set.

Data is allowed to be received by the safety related Protection Set from the non-safety MWS only when the channel is out of service. The channel is taken out of service by taking multiple deliberate actions: (1) activating a hardware out of service switch locked in a cabinet; and (2) activating a software switch on the Workstation requiring password access. In addition, feedback is provided to the user on the MWS that the out of service switch for the loop to be tested has been activated. If the safety related hardware out of service switch is not activated, non-safety related actions or failures cannot adversely affect the safety related function.

The non-safety Triconex MWS software is designed, developed and tested under the Triconex software development programs described in the Tricon V10 Topical Report Submittal [13] to address the Clause 5.5.2 requirement for V&V, configuration management, and QA shall be required for test and calibration functions on separate computers (e.g., test and calibration computer) that provide the sole verification of test and calibration data. Triconex platform compliance with this clause is discussed in the Software Qualification Report [124] Sections 4.0 and 8.0, the Critical Digital Review [125] Sections 1.0, 2.0, 3.0, 4.0, and Appendix B and the Topical Report Submittal [13] Section 2.1 and Appendix B Section 3.0.

b) FPGA-Based ALS PPS Equipment

The ALS provides test and calibration capability as described in Section 2.3.2 and Section 3 of the ALS Topical Report Submittal [15] and Sections 10.2 and 10.3 of the ALS System Design Specification [19]. Each Protection Set has one ALS MWS (with ASU software) associated with the ALS subsystems in that set. The TAB allows the non-safety related ALS MWS to interact with the ALS components for test and calibration only when the TAB communication link is physically connected to the ALS MWS. ALS platform compliance with this clause is discussed in Section 12.2.13.2 of the ALS Topical Report Submittal [15].

In the PPS replacement, the MWS described in Section 4.2.4.5 of this LAR is the hardware platform on which the ASU function is implemented. The non-safety related ASU software is designed, developed, and tested under the CSI software development program to address the Clause 5.5.2 requirement that V&V, configuration management, and QA shall be required for test and calibration functions on separate computers.

4.11.1.3.3 Clause 5.5.3 Fault Detection and Self-Diagnostics (Section D.10.4.2.5.3 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.5.3 states:

Computer systems can experience partial failures that can degrade the capabilities of the computer system, but may not be immediately detectable by the system. Self-diagnostics are one means that can be used to assist in detecting these failures. Fault detection and self-diagnostics requirements are addressed in this subclause.

The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostics are incorporated into the system requirements, these functions shall be subject to the same V&V processes as the safety system functions.

If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner. Conversely, self-diagnostic functions shall not adversely affect the ability of the computer system to perform its safety function, or cause spurious actuations of the safety function. A typical set of self-diagnostic functions includes the following:

- *Memory functionality and integrity tests (e.g., programmable read-only memory checksum and random access memory (RAM) tests)*
- *Computer system instruction set (e.g., calculation tests)*
- *Computer peripheral hardware tests (e.g., watchdog timers and keyboards)*
- *Computer architecture support hardware (e.g., address lines and shared memory interfaces)*
- *Communication link diagnostics (e.g., CRC checks)*

Infrequent communication link failures that do not result in a system failure or a lack of system functionality do not require reporting.

When self-diagnostics are applied, the following self-diagnostic features shall be incorporated into the system design:

- *Self-diagnostics during computer system startup*
- *Periodic self-diagnostics while the computer system is operating*
- *Self-diagnostic test failure reporting*

The PPS replacement complies with Clause 5.5.3 as discussed below:

a) Tricon-Based PPS Equipment

The Tricon is a fault tolerant controller as described in Section 5.7 of the Triconex System Description [34]. As such, it is designed to run continuous diagnostics to detect and mask or override faults. Diagnostic results are available to host devices via communication modules and alarm contacts on the Main Chassis. The alarm contacts on Main Chassis Power Modules are asserted when:

1. The system configuration does not match the control-program configuration
2. A Digital Output Module experiences a LOAD/FUSE error
3. A module is missing somewhere in the system
4. A Main Processor, I/O or Communication module in the Main Chassis fails
5. An I/O or Communication module in an Expansion Chassis fails
6. A Main Processor detects a system fault
7. The inter-chassis I/O bus cables are incorrectly installed-for example, the cable for Leg-A is accidentally connected to Leg-B
8. A Power Module fails
9. Primary power to a Power Module is lost
10. A Power Module has a Low Battery or Over Temperature warning

Extensive diagnostics validate the health of each Main Processor as well as each I/O module and communication channel. Transient faults are recorded and masked by the hardware majority voting circuit. Persistent faults are diagnosed, and the errant module is hot-replaced or operated in a fault-tolerant manner until hot replacement is completed.

Main Processor diagnostics do the following:

1. Verify fixed-program memory
2. Verify the static portion of RAM
3. Test all basic processor instructions and operating modes
4. Test all basic floating-point processor instructions
5. Verify the shared memory interface with each I/O communication processor and communication leg
6. Verify handshake signals and interrupt signals between the Central Processing Unit (CPU), each I/O communication processor and communication leg
7. Check each I/O communication processor and communication leg microprocessor, ROM, shared memory access and loopback of RS-485 transceivers
8. Verify the TriClock interface
9. Verify the TriBUS interface

All I/O modules sustain complete, ongoing diagnostics for each leg. Failure of any diagnostic on any leg, activates the module's FAULT indicator, which in turn activates the chassis alarm signal. The FAULT indicator points to a leg fault, not a module failure. The module is designed to operate properly in the presence of a single fault and may continue to operate properly with some multiple faults.

TMR Digital Input Modules with Self-Test continuously verify the ability of the Tricon to detect the transition of a normally energized circuit to the OFF state. TMR High-Density Digital Input Modules continuously verify the ability of the Tricon to detect transitions to the opposite state.

Each type of digital output module executes a particular type of Output Voter Diagnostic (OVD) for every point. In general, during OVD execution the commanded state of each point is momentarily reversed on one of the output drivers, one after another. Loop-back sensing on the module allows each microprocessor to read the output value for the point to determine whether a latent fault exists within the output circuit.

A DC voltage digital output module is specifically designed to control devices, which hold points in one state for long periods. The OVD strategy for a DC voltage digital output module ensures full fault coverage even if the commanded state of the points never changes. On this type of module, an output signal transition occurs during OVD execution, but is designed to be less than 2.0 milliseconds (500 microseconds is typical) and is transparent to most field devices.

The results of all diagnostic tests are available to a host device via each installed communication module. Individual diagnostic flags are asserted upon any module fault within any chassis, DO load fuse or output voter fault, printer fault, math error, scan time overrun, Tricon keyswitch out of position, host communication error, program change, and I/O point disabled.

The Tricon Planning and Installation Guide [35] provide descriptions of the main processor and I/O modules diagnostics.

b) FPGA-Based ALS PPS Equipment

As described in Reference [15], Section 3, the ALS platform incorporates advanced failure detection and isolation techniques. The operation of the system is deterministic in nature and allows the system to monitor itself in order to validate its functional performance. The ALS platform implements advanced failure detection and mitigation in the active path to avoid unintended plant events, and in the passive path to ensure inoperable systems do not remain undetected. The system utilizes logic to perform distributed control where no single failure results in an erroneous plant event while maintaining the ability to perform its intended safety function.

The ALS platform incorporated self-diagnostics, application specific diagnostics and self-test features into the input boards, bus communications, CLBs, and output boards. In addition, system level diagnostics are incorporated as divided into four categories: fatal, vital, non-vital, and undetectable, as described in Reference [15] Section 3.1.1.

IEEE Standard 7-4.3.2 [80] Clauses 5.4.1 and 5.4.2 address computer system testing and qualification of existing commercial computers, respectively. Computer system qualification testing is discussed in Section 4.6 of this enclosure.

4.11.1.4 Clause 5.6 Independence (Section D.10.4.2.6 of D&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [76] Clause 5.6 states:

In addition to the requirements of IEEE Std 603-1998, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function.

IEEE Std 603-1998 requires that safety functions be separated from non-safety functions such that the non-safety functions cannot prevent the safety system from performing its intended functions. In digital systems, safety and non-safety software may reside on the same computer and use the same computer resources.

Either of the following approaches is acceptable to address the previous issues:

a) Barrier requirements shall be identified to provide adequate confidence that the non-safety functions cannot interfere with performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The non-safety software is not required to meet these requirements.

b) If barriers between the safety software and non-safety software are not implemented, the non-safety software functions shall be developed in accordance with the requirements of this standard.

Guidance for establishing communication independence is provided in Annex E.

PPS replacement conformance with this clause is discussed in the following paragraphs.

a) Tricon-Based PPS Equipment

993754-1-912 DCPP Triconex PPS ISG-04 Conformance Report [25], describes the data and communications independence of the Tricon equipment and compliance with DI&C-ISG-04 [2]. NTX-SER-09-10, Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4 [24] describes the communications independence capabilities of the Tricon platform and generic Tricon platform and compliance with DI&C-ISG-04 [2].

b) FPGA-Based ALS PPS Equipment

Section 5 of ALS Topical Report Submittal [15] describes the communication capabilities of the ALS equipment and compliance with DI&C-ISG-04 [2].

4.11.1.5 Clause 5.7 Capability for Test and Calibration (Section D.10.4.2.7 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2 [76] Clause 5.7 states:

No requirements beyond IEEE Std 603-1998 are necessary.

The PPS replacement conforms with Clause 5.7 as discussed in Section 4.10.2.7 of this LAR.

4.11.1.6 Clause 5.8 Information Displays (Section D.10.4.2.8 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.8 states:

No requirements beyond IEEE Std 603-1998 are necessary.

The PPS replacement does not utilize any safety or non-safety related information display or control station to perform any control or protective action. The PPS replacement does utilize a non-safety related Tricon MWS and ALS MWS in each of the four Protection Sets for the purpose of performing maintenance activities on the Tricon and FPGA-based ALS PPS equipment. These MWS function with and communicate with the PPS replacement equipment as described in LAR Section 4.2.4.5.

a) Tricon-Based PPS Equipment

The Tricon system architecture has flexible hardware and software capability for communicating with a variety of non-safety workstations. See Section 2.1 of the Tricon Version 10 Topical Report Submittal [13].

b) FPGA-Based ALS PPS Equipment

Section 12.2.16 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 5.8.

4.11.1.7 Clause 5.11 Identification (Section D.10.4.2.11 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80], Clause 5.11 states:

To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification requirements specific to software systems shall be met:

a) Firmware and software identification shall be used to assure the correct software is installed in the correct hardware component.

b) Means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools.

c) Physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std 603-1998 [21].

The PPS replacement equipment conformance to Clause 5.11 is discussed in Section 4.11.1.7.1 (Tricon-Based equipment) and Section 4.11.1.7.2 (FPGA-Based ALS equipment).

a) Tricon-Based PPS Equipment

The following documents describe the Tricon-based PPS replacement equipment conformance to Clause 5.11.

Software identification control for embedded software is described in Sections 1.2.1 and 1.2.2 of the Triconex Software QAP [52].

Software identification control for application software is described in Section 3.1 of the Triconex DCPP SCMP [77].

Hardware identification control is described in Section 2.0 of the Tricon V10 Topical Report Submittal [13]. The Topical Report provides a reference to the Triconex Master Configuration List [93].

b) FPGA-Based ALS PPS Equipment

Section 12.2.19 of the ALS Topical Report Submittal [15] describes the FPGA-based ALS PPS replacement equipment conformance to Clause 5.11.

Section 2.1.5.2 of the ALS Topical Report Submittal [15] provides the method for conformance with the identification requirement of Clause 5.11.

Section 1.2 of the ALS CMP [66] identifies the configuration requirements applicable to satisfying Clause 5.11.

4.11.1.8 Clause 5.15 Reliability (Section D.10.4.2.15 of DI&C-ISG-06 [1])

IEEE Standard 7-4.3.2-2003 [80] Clause 5.15 states:

In addition to the requirements of IEEE Std 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing.

Software error recording and trending may be used in combination with analysis, field experience, or testing.

The PPS Replacement Project meets IEEE 7-4.3.2 [80] Clause 5.15 as described in the following sections. Additional information is provided in Section 4.10.2.15 of this Enclosure.

a) Tricon-Based PPS Equipment

Reliability of the computer system is addressed in the Reliability/Availability Report 9600164-532 [123]. In addition, software reliability pursuant to IEEE 7-4.3.2 criteria has been addressed in the Software Qualification Report 9600164-535 [124] and the Critical Digital Review 9600164-539 [125].

b) FPGA-Based ALS PPS Equipment

The ALS does not utilize executable software therefore there is no software to include when determining reliability. The ALS being an FPGA-based system is configured which results in a hard wired system consisting solely of hardware items. Once V&V has determined the quality of the FPGA configuration and testing has determined that the configuration functions correctly to perform the safety function, there is no executable software used during the operation of the system. Therefore, there is no further contribution of software failure to the overall failure rate. Additional details regarding the V&V and testing for the PPS replacement are provided in 6002-00003 ALS V&V Plan [54], 6002-00005 ALS Test Plan [56], and ALS 6116-00005 Diablo Canyon PPS System Test Plan [67].

4.12 Technical Specifications (Section D.11 of DI&C-ISG-06 [1])

The four criteria of 10 CFR 50.36 (d) (2) (ii) require establishment of a TS Limiting Condition for Operation (LCO) for a system or function to define the lowest functional capability or performance level of a system.

The PPS replacement has been specified and designed such that it meets the current TS and FSAR Chapter 6 and 15 [26] accident analysis requirements. No new TS LCOs or SRs are required to be added because the current TS LCOs and SRs adequately specify the lowest functional capability and testing requirements for the PPS replacement. Howerver, the TS 1.1 definition of COT is revised to allow incorporation of the diagnostic and self-test capabilities of the PPS replacement components.

The TS were revised in License Amendments 84 and 83, dated October 7, 1993 [98] to support the use of the existing Eagle 21 digital PPS. The TS changes made in Amendments 84 and 83 allow a channel operational test for a digital channel, allow a channel functional test for a digital channel including injection of a simulated signal into the channel, and allow bypassing an inoperable channel when performing surveillance tests on an operable channel. The PPS replacement has been specified and designed such that it meets these existing TS features.

To support installation of Eagle 21, the TS definitions were revised to allow a channel operational test for a digital channel and to allow a channel functional test for a digital channel, that includes the injection of a simulated signal into the channel as close to the sensor input to the process racks as practical, to verify operability of all devices in the channel required for channel operability. The PPS replacement has been specified and designed such that it has the capability to meet these current TS definitions.

The Eagle 21 PPS has the capability to allow bypassing an inoperable channel when performing surveillance tests on an operable channel. Placing the inoperable channel in bypass results in an indication to the operator and allows testing of an operable channel including placing the operable channel in trip. The PPS replacement has been specified and designed such that it meets the current TS capability for the inoperable channel to be placed in bypass.

4.12.1 TS 1.1 COT Definition Revision

The current TS 1.1 Definition for "CHANNEL OPERABILITY TEST (COT)" states:

A COT shall be the injection of a simulated or actual signal into the channel as close to the sensor as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY. The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. The COT may be performed by means of any series of sequential, overlapping or total channel steps.

The available diagnostic and self-test capabilities of the PPS replacement components eliminate the need to inject a signal into the channel in order to verify OPERABILITY during performance of the COT. In addition, for the PPS replacement components the setpoints are contained in digital memory and will not experience drift in the same manner that is possible for setpoints stored in analog systems. Therefore, the COT definition is revised to provide separate and more appropriate definitions for the current analog, bistable, and current Eagle 21 process protection system digital channels, and the Tricon/ALS PPS digital channels.

The proposed TS 1.1 Definition for COT states:

A COT shall be:

a. *Analog, bistable, and Eagle 21 process protection system digital channels - the injection of a simulated or actual signal into the channel as close to the sensor input* *to the process racks as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.*

b. Tricon/Advanced Logic System process protection system digital channels - the use of diagnostic programs to test digital hardware, manual verification that the setpoints and tunable parameters are correct, and the injection of simulated process data into the channel as close to the sensor input to the process racks as practical to verify channel OPERABILITY of all devices in the channel required for OPERABILITY.

The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. The COT may be performed by means of any series of sequential, overlapping or total channel steps.

The proposed COT definition includes a definition that applies to the current TS 3.3.1. TS 3.3.2, TS 3.4.11 (Pressurizer Power Operated Relief Valves), and TS 3.4.12 (Low Temperature Overpressure Protection System) analog instrumentation channels, the current bistable channels with outputs from relay contacts (RCP breaker, 12kV UV/UF, seismic, etc.) sensed by the SSPS equipment, and the current Eagle 21 bistable outputs sensed by the SSPS equipment. The proposed COT definition also includes a definition for the Triconex/Advanced Logic System process protection system digital channels. The proposed COT definition does not revise the current COT requirement that the COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy, or the current allowance that the COT may be performed by means of any series of sequential, overlapping or total channel steps. The current six month COT frequency for the TS 3.3.1 and 3.3.2 surveillances is not being revised as part of the PPS Replacement Project.

a) Tricon-Based PPS Equipment

The self-test capabilities of the Tricon-based PPS equipment are discussed in Sections 2.1.3 and 3.9 of the Triconex approved Topical Report 7286-545-1-A, Revision 4 [13] and in Section 3.4.3 of the NRC safety evaluation report contained in the Triconex approved Topical Report 7286-545-1-A, Revision 4 [13].

The V10 Tricon incorporates integral online diagnostics. Probable failure modes are anticipated and made detectable by specialized circuitry with all faults being annunciated. Fault annunciation is done with the failed modules fault light emitting diode and the system alarm. Fault-monitoring circuitry in each module helps fulfill this requirement. The circuitry includes, but is not limited to, I/O loopback, dead-man timers, and loss-of-power sensors. This aspect of the system design enables the V10 Tricon to reconfigure itself and perform limited self-repair according to the health of each module and channel.

Tricon modules house the circuitry for three identical channels (A, B, and C). Although the channels reside on the same module, they are isolated from each other and operate independently, and therefore a fault on one channel cannot pass to another. Each V10 Tricon module can activate the system integrity alarm. The alarm consists of a normally closed or normally opened relay contact on each power module. Any failure condition, including loss or brownout of system power, activates the alarm to inform plant personnel in the control room.

3703EN, 3721N Analog Input Modules

For the 3703EN and 3721N analog input modules, each of the three channels asynchronously measure the input signals and places the results into a table of values. Each of the three channel input tables are passed to its associated 3008N MP using the I/O bus. One value is selected from the tables using a mid-value selection algorithm.

Each 3703EN and 3721N analog input detects internal stuck-high and stuck-low faults. stuck-at legs, which are most likely to occur when, input values remain within miscompare limits for extended periods of time, are detected by automatic leg calibration within the analog input modules. Each analog input module leg is automatically calibrated using multiple reference voltages. Out-of-tolerance data is reported to the respective 3008N MP. The 3008N MP fault analyzer routines diagnose faulty input module legs at the end of each scan. One-time and short-term differences that result from sample timing variations are distinguished from a pattern of differing data.

3805HN Analog Output Module

The 3805HN analog output module receives three tables of output values, one for each channel from the corresponding 3008N MP. Each channel has its own digital-to-analog converter. One of the three channels is selected to drive the analog outputs. The output is continuously checked for correctness by loopback inputs on each point which are read by all three microprocessors. If a fault occurs in the driving channel, that channel is declared faulty, and a new channel is selected to drive the field device. The designation of driving channel is rotated among the channels so that all three channels are periodically tested. The channels not actively driving the output still internally drive the selected current. This is monitored by the diagnostics to insure the channel can properly drive the output when it becomes the selected channel.

3501TN2, 3503EN2 Digital Input Modules

There are two basic types of digital input modules, TMR and single. The PPS replacement only uses the TMR digital input module. Each of the three input channels asynchronously measures the input signals from each point on the input module, determines the respective states of the input signals, and places the values into input tables A, B, and C respectively. Each of the three input tables is passed to its associated 3008N MP using the I/O bus. One value is selected from the tables using a mid-value selection algorithm.

The 3503EN2 includes additional circuitry from the 3501TN2 to detect stuck-on faults. This feature verifies the ability to detect a transition from a normally energized circuit to the off state. To test for stuck-on inputs, a switch within the input circuitry is closed to allow a zero input (off) to be read by the optical isolation circuitry. The last data reading is frozen in the I/O processor while the test is running.

3601TN Digital Output Module

The 3601TN digital output module uses a quadruplicated output circuitry, referred to as quad voter, which votes on the individual output signals just before they are applied to the load. This voter circuitry is based on parallel-series paths which pass power if the drivers for Channels A and B, or Channels B and C, or Channels A and C command them to close, i.e, 2-out-of-3 drivers voted on. The quadruplicated output circuitry provides multiple redundancies for all critical signal paths.

The 3601TN executes a specific type of output voter diagnostics for every point. This safety feature facilitates unrestricted operation under a variety of multiple-fault scenarios. During output voter diagnostics execution, the commanded state of each point is momentarily reversed on one of the output drivers, one after another. Loopback on the module allows each channel's microprocessor to read the output value for the point to determine whether a latent fault exists within the output circuit.

A faulty switch identified by the output voter diagnostics process causes the output signal to transition to the opposite state for a maximum of half an AC cycle. After a fault is detected, the module discontinues further iterations of output voter diagnostics. Each point on the 3601TN requires periodic cycling to both the on and off states to ensure 100 percent fault coverage.

If the analog to digital converter (ADC) module has been significantly adjusted or is outside the limited automatic calibration limits, the module will be marked faulted and an alarm will be generated in the control room.

The hardware and software used to perform automatic self-testing are classified as safety-related, having the same quality and reliability as the Tricon PLC. The Invensy

Operations Management document number 9700077-016, "Planning and Installation Guide for Tricon V9-V10 Systems," dated February 2012, provides detailed descriptions of each diagnostic test and flag for the Tricon modules.

The available Tricon diagnostic programs and self-test capabilities, through periodic injection of precision reference voltages into the ADC modules, verify the circuitry and calibration and eliminate the need to inject test signals manually into the channel during performance of the COT.

The Tricon allows manual verification that the setpoints and tunable parameters are correct by displaying the current values on the Tricon MWS during performance of the COT.

If a Tricon I/O board is replaced, the MPs detect the presence of a replacement module. The MPs initiate local health state diagnostics and, if the module is healthy, automatically switch over to the new module.

If the Tricon MP power is turned off, the Tricon includes self-test features to confirm computer system operation upon system initialization. Upon power up (when the MP is inserted in the MP slot of the main chassis), the electronic main processor goes through the power up initialization and diagnostics. The power up sequence includes a series of power up diagnostics – microprocessor tests, random access memory tests, flash memory tests, watchdog test, and clock calendar test. These self-test and diagnostic features eliminate the need for injection of a simulated or actual signal into the channel to verify proper operation of the Tricon.

b) FPGA-Based ALS PPS Equipment

The FPGA-based ALS PPS equipment has diagnostics and testing capabilities designed into the ALS platform to ensure there is a systematic approach to maintaining and testing the system. Sections 3.1.1.1 and 3.1.1.3 of the ALS Topical Report Submittal [15] describe the system self-diagnostics and Section 3.1.1.2 describes the the self-testing features. The ALS platform incorporates advanced failure detection and isolation techniques. The operation of the system is deterministic in nature and allows the system to monitor itself in order to validate its functional performance. The ALS platform implements advanced failure detection and mitigation in the active path to avoid unintended plant events, and in the passive path to ensure inoperable systems do not remain undetected.

The ALS platform incorporates self-diagnostic features that provide a means to detect and alarm any significant failure within the platform. Details of the ALS board self-diagnostic features are described in the hardware specification associated with each board and the ALS platform fault detection and self-diagnostics are described in the document 6002-00011, "ALS Platform Specification" [95]. The self-diagnostic features are integral to the platform, and are, therefore, subject to the same high quality design development and IV&V processes as the rest of the platform. The self-diagnostic features are functional during all modes of ALS platform operation, including power-up, operation, and test. Although not being requested by this LAR, the ALS platform is designed to eliminate the need for periodic surveillance testing with a combination of redundancy and self-testing which automatically and transparently verifies critical system functions.

As described in Section 3.1.1.1 of the ALS Topical Report Submittal [15], the ALS platform self-test strategy is based on four simple and effective steps:

> Detect: The ALS platform detects faults in its circuits or connected field devices by running background tests on a regular interval, and by redundancy.
>
> Mitigate: The circuits causing the failure are isolated before the failure is allowed to propagate from an ALS board to another and from the ALS to other systems.
>
> Announce: The detected failure is announced using the ALS chassis alarm and an alarm on the Control Room MAS "window" indicator. The online ALS non-safety communications capability provide real-time, online data and status information on the PDN Gateway Computer and to the MWS. The use of the online ALS non-safety communications capability provides redundant, real-time results of the diagnostic and self test features that provide timely diagnostic information on instrument channel OPERABILITY and status details that assist in timely performance of required trouble-shooting and maintenance. In addition, the MWS can provide detailed status indication, such as indicating in which function the failure occurred and providing indication as to whether the system remains operable.
>
> React: The failure is announced using the system alarm and by other application specific means. The online ALS non-safety communications capability provide real-time, online data and status information on the PDN Gateway Computer and to the MWS. The use of the online ALS non-safety communications capability provide timely diagnostic information and status details that assist in timely performance of required trouble-shooting and maintenance. In addition, the MWS can provide detailed status indication to support trouble-shooting and maintenance.

Section 2.8 of the document 6002-00011, "ALS Platform Specification," [95] describes the BIST used for exercising all critical functions within a board to ensure latent failures cannot buildup in the sytem and make it inoperable without knowledge of plant personnel. This section also describes the inherent self-test method used to quickly detect stuck or open failures.

Section 3.1.1.2 of the ALS Topical Report Submittal [15], discusses self-testing performed from the field input, through the ALS input board, ALS CLB, ALS output board, and the field output. Table 3.1-1 of the ALS Topical Report Submittal [15] identifies the self-testing test intervals for each ALS board.

The ALS-311 input board BIST operation begins with providing a single dedicated multi-channel ADC for each input for the purpose of measuring the field input signal and for sampling the onboard diagnostic signal references. Document 6002-31102, "ALS-311 Design Specification," Section 3.5, provides an example configuration and ADC channel assignment for an ALS-311 input board configured with an RTD input. In normal operation, the ADC will perform the sample loop. Disabled channels will not sample data, nor perform self-test functions. If an input fails the integrity BIST, this is reported via the integrity status bit located in the CSI20 message packet for analog boards, or in the integrity monitor register for digital I/O boards. In the ALS used for the DCPP PPS replacement subsystem, any integrity BIST failure is alarmed at the system level and provided to the MAS. The ALS-321 input board BIST is the same as for the ALS-311 input board.

The ALS-402 output board BIST integrity checking is accomplished by continually monitoring a feedback signal tied to an output to verify the commanded state matches the feedback state. The technique used is described in the document 6002-40202, "ALS-402 Design Specification," [109]. To verify operability of the circuit beyond the circuit isolation barrier and verify operability of downstream wiring and devices (SSPS, etc.) in the DCPP PPS replacement, the ASU can be used to place the ALS-402 output in question into an override mode and can then be used to command the output to the desired state (i.e. open/close). If an ALS-402 board output fails its integrity BIST, a failure is alarmed at the system level and provided to the MAS. A failed ALS-402 board output is driven automatically to its predefined failsafe state. Therefore, verification of ALS-402 operability does not require an injected signal source.

In addition to the encoding diversity that occurs on ALS boards, the ALS-102 CLB uses several levels of checking internal memory to verify that no change in safety logic has occurred. In the configuration section of NVM on every board, a 32-bit checksum is run against the following address locations:

- Board ID
- Project ID
- Channel Configuration
- Linearization Coefficients

In addition, a 16-bit cycle redundancy check is run on every NVM memory address location. An ALS board that does not pass the NVM check will revert to the FAIL mode and the board will not operate.

The FPGA design uses the on-chip static random access memory (SRAM) blocks, and provisions are made that ensure that single event upsets of the SRAM content does not result in the board being incapable of performing its safety function.

The Actel ProASIC®3L device family used in the ALS contains SRAM blocks which are used by the ALS logic. When these SRAM blocks are used, redundancy checking, parity checking and cycle redundancy checks are employed to ensure that corruption of a memory cell does not cause the ALS board to enter a halt state. Persistent memory corruptions are announced.

The BIST integrity checking on the ALS-421 output board is accomplished in a similar manner as is performed on the ALS-402 board. As described in document 6002-42102, "ALS-421 Design Specification," [110], the ALS-421 output board uses the combination of a digital-to-analog and an ADC for command and feedback for an output. The ALS-421 output board performs a difference detection between the commanded output and the output feedback, and if the feedback value exceeds a defined plus/minus error percentage, the ALS-421 output board will report the channel as an error. If an ALS-421 board output fails its integrity BIST, a failure is alarmed at the system level and provided the MAS. A failed ALS-421 board output is driven automatically to its predefined failsafe state. As with the ALS-402 board, an ALS-421 board output of interest can be placed into an override mode and commanded to a known analog output level for the purposes of determining the operation of downstream devices (e.g., Tricon). Therefore, verification ALS-421 operability does not require an injected signal source.

The available ALS diagnostic programs and self-test capabilities, through periodic injection of simulated process data into the channel, allow the performance of the COT, without injection of an external simulated or actual signal into the channel.

The ALS platform allows manual verification that the setpoints and tunable parameters are correct by displaying the current values on the ALS MWS during performance of the COT. The ALS is capable of reporting the contents of all FPGA registers and NVM memory locations within an ALS chassis for the purpose of allowing an I&C technician to perform a comparison of memory contents between surveillance intervals.

4.12.2 PPS RTS and ESFAS TS Setpoints

Setpoints for Eagle 21 PPS

To support the installation of the existing Eagle 21 PPS, the setpoints analysis for the protection system functions processed through Eagle 21 were revised to reflect revised setpoint input values for rack calibration accuracy, rack drift, and temperature effect values as discussed in Section D of PG&E Letter DCL-92-203 [97] and the RTS and

ESFAS TS allowable values were revised to incorporate the results of the revised setpoint analysis in Amendments 84 and 83. The functional requirements in the PPS Replacement FRS [28] have been specified such that they are the same as or better than the current Eagle 21 PPS for instrument rack calibration accuracy, rack drift, temperature effect values, and response time. These functional requirements are the PPS parameters that impact the setpoint analysis and specifying the functional requirements in this manner allows the existing TS 3.3.1 RTS and TS 3.3.2 Nominal Trip Setpoints and Allowable Values to be applicable to the PPS replacement.

Setpoints for PPS Replacement

The setpoint calculations are contained in Westinghouse document WCAP-17696 P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," [171]. The setpoint calculations satisfy all of the informational requirements set forth in Section D.9.4.3.8 of DI&C-ISG-06 [1]. The setpoint calculations determine the margin that exists between operating limits and setpoints, to ensure there is a low probability for inadvertent actuation of the system and to ensure margin exists between setpoints and safety limits.

The algorithms used to determine the PPS replacement TS setpoints are believed to provide total instrument loop uncertainties, termed channel statistical allowance, at a two-sided 95 percent probability and 95 percent confidence level; as stated in NRC RG 1.105, Revision 3, Regulatory Position C.1 [172]. In addition, the setpoint calculations determine the as-found and as-left tolerances.

The setpoint methodology is contained in Westinghouse document WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," [173]. The approach used for the methodology is consistent with ISA-67.04.01- 2006 [78]. The basic uncertainty algorithm is the square root sum of the squares (SRSS) of the applicable uncertainty terms, which is endorsed by the standard. All appropriate and applicable uncertainties, as defined by a review of the plant baseline design input documentation, have been included in each PPS related RTS or ESFAS function uncertainty calculation. The algorithms in WCAP-17706-P used to determine the TS setpoints assume that actions specified in Section 5 of WCAP-17706-P are included in the plant surveillance procedures. The actions specified in Section 5 of WCAP-17706-P will be included in the plant surveillance procedures during implementation of the amendment.

ISA standard ISA-RP67.04.02, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation" [174] was considered, as a general guideline, but each uncertainty and its treatment is based on Westinghouse methods which are consistent or conservative with respect to this document. The current version of NRC RG 1.105, Revision 3 [172], endorses the 1994 version of ISA standard ISA-S67.04, Part I [175]. Westinghouse has evaluated this NRC document and has determined that the uncertainty algorithms contained in the setpoint calculations are consistent with the guidance contained in RG 1.105, Revision 3 [172] and NRC Branch Technical Position 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints," Revision 5 [4].

Control of As-found and As-left Tolerances at DCPP

At DCPP, setpoints are controlled using a graded approach by following PG&E Inter-Departmental Administrative Procedure (IDAP) CF6.ID1, "Setpoint Control Program," [176] a procedure subject to 10 CFR 50.59. CF6.ID1 [176] requires that electrical setpoints shall be fully documented by a calculation performed using a specified methodology.

For DCPP, the Corrective Action Program (CAP) procedure is PG&E Program Directive OM7, "Corrective Action Program," [177] and problems are documented per the DCPP supporting CAP procedure IDAP OM7.ID1, "Problem Identification and Resolution" [177]. The CAP includes a process to perform a TS operability review, and document as necessary per DCPP IDAP OM7.ID12, "Operability Determination," and to determine the necessary corrective actions to be taken, including corrective actions. An issue is entered as a notification into a computer based tracking program.

The surveillance requirements (SRs) 3.3.1.7, 3.3.1.10, 3.3.2.5, and 3.3.2.9 for the channel operability tests and channel calibrations for the RTS and ESFAS PPS functions are performed using surveillance test procedures that are subject to 10 CFR 50.59. The current surveillance test procedures for SRs 3.3.1.7, 3.3.1.10, 3.3.2.5, and 3.3.2.9 for the RTS and ESFAS PPS functions contain acceptance criteria that require that if the as-found data for the setpoints are not within desired range, to notify management and to initiate a notification. These surveillance test procedures also require that the as-left data shall be within the desired range. The instrument channel cannot be returned to service and declared operable unless the setpoint can be reset to within the as-left setpoint and the evaluation of the channel shows it is functioning as required. The TS Bases changes for SRs 3.3.1.7, SR 3.3.1.10, 3.3.2.5, and 3.3.2.9, provided in Attachment 4 to this Enclosure, include a sentence that plant procedures verify that the instrument channel functions as required by verifying the "as left" and "as found" settings are consistent with those established by the setpoint methodology.

Although the nominal trip setpoints for the RTS and ESFAS PPS functions are not required to be be replaced due to the PPS replacement, in order to ensure appropriate control of the as-found and as-left tolerances associated with the TS setpoints for the RTS and ESFAS PPS functions, the 10 CFR 50.59 controlled surveillance test procedures applicable to SRs 3.3.1.7, 3.3.1.10, 3.3.2.5, and 3.3.2.9 will be updated as required as part of implementation of the amendment for each unit. The actions for the various potential surveillance outcomes will be required as follows:

(1) The instrument channel setpoint exceeds the as-left tolerance but is within the as-found tolerance:

- Reset the instrument channel setpoint to within the as-left tolerance;
- If the instrument channel setpoint cannot be reset to a value that is within the as-left tolerance around the instrument channel setpoint at the completion of the surveillance, if not already inoperable, the instrument channel shall be declared inoperable.

(2) The instrument channel setpoint exceeds the as-found tolerance but is conservative with respect to the TS allowable value (AV):

- Reset the instrument channel setpoint to within the as-left tolerance;
- If the instrument channel setpoint cannot be reset to a value that is within the as-left tolerance around the instrument channel setpoint at the completion of the surveillance, if not already inoperable, the instrument channel shall be declared inoperable;
- Enter the channel's as-found condition in the CAP for prompt verification that the instrument is functioning as required, and for further evaluation. Evaluate the channel performance utilizing available information to verify that it is functioning as required before returning the channel to service. The evaluation may include an evaluation of magnitude of change per unit time, response of instrument for reset, previous history, etc., to provide confidence that the channel will perform its specified safety function;
- Document the condition for continued OPERABILITY.

(3) The instrument channel setpoint is non-conservative with respect to the TS AV:

- If not already inoperable, declare the channel inoperable;
- Reset the instrument channel setpoint to within the as-left tolerance;
- Enter the channel's as-found condition in the CAP for evaluation. Evaluate the channel performance utilizing available information to verify that it is functioning as required before returning the channel to service. The evaluation may include an evaluation of magnitude of change per unit time, response of instrument for reset, previous history, etc., to provide confidence that the channel will perform its specified safety function.

These procedure actions are the minimum actions which the procedures will require and additional actions may be taken. These procedure actions will apply until procedure actions consistent with a license amendment for TSTF-493, Revision 4, are implemented for all automatic protective devices related to variables having significant safety functions as delineated by 10 CFR 50.36(c)(1)(ii)(A).

In addition, the "Equipment Control Guidelines" (ECGs) will be updated as part of implementation of the amendment for each unit to identify the methodologies used to determine the as-found and as-left tolerances. The ECGs are documents controlled under 10 CFR 50.59 and are incorporated into the FSAR by reference.

4.12.3 PPS RTS and ESFAS TS Completion Times, Bypass Test Times, and COT Surveillance Test Intervals

For Eagle 21 processed RTS or ESFAS functions for the condition of one inoperable channel, the DCPP TS 3.3.1 and 3.3.2 Actions allow a channel to be placed in trip in a completion time of 72 hours and allow a bypass test time of 12 hours. WCAP-14333-P-A, Revision 1 [167], provided the justification for increasing completion times from 6 hours to 72 hours and for increasing the bypass test times from 4 hours to 12 hours for the Eagle 21 PPS. For Eagle 21 processed RTS or ESFAS functions, the DCPP TS 3.3.1 and 3.3.2 surveillances for the channel operability test allow a surveillance test interval of 6 months. WCAP-15376-P-A, Revision 1 [168], provided the justification for increasing the channel operability test surveillance test intervals from 3 months to 6 months. PG&E obtained NRC approval to use the TS 3.3.1 and 3.3.2 completion times, bypass test times, and channel operability test surveillance test intervals based on WCAP-14333-P-A, Revision 1 [167], and WCAP-15376-P-A, Revision 1 [168], in Amendments 179 and 181 [169].

Section 5 of the NRC Safety Evaluation contained in WCAP-15376-P-A, Revision 1, stated, "For future digital upgrades with increased scope, integration and architectural differences beyond that of Eagle 21, the staff finds the generic applicability of WCAP-15376-P, Rev. 0 to future digital systems not clear and should be considered on a plant-specific basis." Therefore, an assessment has been performed that provides a qualitative comparison of the Tricon and ALS subsystems to the Eagle 21 system. The assessment is contained in the Westinghouse Document, "Justification for the Application of Technical Specification Changes in WCAP-14333 and WCAP-15376 to the Tricon/ALS Process Protection System at the Diablo Canyon Power Plant [170]." The assessment [170] provides a qualitative comparison of features important to the reliability of the Tricon and ALS subystems and the Eagle 21 system, evaluates the applicability of the WCAP-14333-P-A, Revision 1 [167], and WCAP-15376-P-A, Revision 1 [168], analyses to the PPS replacement configuration, and evaluates the compliance with the staff conditions and limitations contained in the NRC safety evaluations for WCAP-14333 and WCAP-15376.

Section 4.3 of Amendments 179 and 181 [169] contained the staff's findings on the applicability of WCAP-14333-P-A, Revision 1 [167], and WCAP 15376-P-A, Revision 1 [168] to DCPP. The staff findings were based on tables submitted by PG&E that address the applicable assumptions, conditions, and limitations of WCAP-14333-P-A, Revision 1 [167], and WCAP 15376-P-A, Revision 1 [168]. The staff findings were also based on the DCPP procedures and commitments for avoidance of risk-significant plant-specific configurations and risk-informed plant configuration control and management, and the plant-specific configuration risk management program. The assessment [170] addresses the tables submitted by PG&E for the applicable assumptions, conditions, and limitations of WCAP-14333-P-A, Revision 1 [167]; and WCAP 15376-P-A, Revision 1 [168]; and the DCPP procedures for avoidance of risk-significant plant-specific configurations and risk-informed plant configuration control and management. PG&E will continue to implement the commitments for the RTS and ESFAS reflected in Amendments 179 and 181 [169] to avoid risk-significant plant-specific configurations and will continue to use the DCPP plant-specific configuration risk management program procedure AD7.DC6, "On-Line Maintenance Risk Management," to provide plant configuration control and management with the PPS replacement.

The assessment [170] has concluded the current TS 3.3.1 and 3.3.2 completion times, bypass test times, and surveillance test intervals for the PPS replacement components based on WCAP-14333-P-A, Revision 1 [167], and WCAP 15376-P-A, Revision 1 [168], continue to be applicable for the PPS replacement. The conclusion is based on the following:

- Following the current industry standards, NRC RGs, and industry guidance documents ensures that the Tricon/ALS based PPS replacement will meet the industry's and NRC's design and operational requirements, and result in a highly reliable system. Since these requirements are more stringent than those in place when the Eagle 21 system was developed, the Tricon/ALS based PPS replacement is expected to meet and exceed the performance of the Eagle 21 system.

- Both the Eagle 21 and the Tricon/ALS based PPS replacement subsystems process the same signals. A number of other signals are processed outside the Eagle 21 system and will remain so with the Tricon/ALS based PPS replacement subsystems.

- The Eagle 21 and the Tricon subsystems are digitally based and the ALS subsystem relies on a simple hardware architecture and does not utilize a microprocessor or software for operation albeit the firmware originated as software. The Eagle 21 system is subject to common cause failures in hardware and software that can fail signal processing. The potential for common cause failure of the Tricon/ALS based PPS replacement design is reduced due to the significant differences in the design of the Tricon subsystem and the ALS subsystem.

- Both the Eagle 21 and the Tricon/ALS based PPS replacement subsystems have the ability to detect failures via their self-test features. These features ensure system failures are identified and corrected in a timely fashion. Neither system can detect all postulated failures with their self-diagnosis features; therefore, there is some dependency on the periodic channel operability test to identify failures in both systems.

- The TMR design of the Tricon subsystem provides a system that can tolerate failures within a channel and maintain the safety function provided by that channel. The combination of design and test strategies in the ALS subsystem, including FPGA redundancy and built-in self-test and inherent self-test features, maintains a high reliability. Therefore, the Tricon/ALS based PPS replacement is expected to be as or more reliable than the Eagle 21 system with respect to its protection function.

- Diversity exists in the Tricon/ALS based PPS replacement design that does not exist in the Eagle-21 system.

The DCPP TS have been revised to incorporate the TS 5.5.18 Surveillance Frequency Control Program and the TS 3.3.1 and 3.3.2 surveillance frequencies, except the TS 3.3.1 surveillances that are condition based, have been relocated to PG&E control in accordance with the Surveillance Frequency Control Program. However, there are no changes to the TS 3.3.1 and 3.3.2 surveillance frequencies, such as the current six month COT frequncy, being considered as part of the PPS Replacement Project.

Each of the four Protection Sets contains a Tricon subsystem comprised of three separate legs and an ALS subsystem comprised of an A core and B core. Any of the three Tricon legs and both the ALS A or B cores in each Protection Set can perform the protection function.

a) Tricon-Based PPS Equipment

For the condition that one Tricon leg in a channel is out of service, the protection function can still be performed and the channel is operable, however the redundancy of the Tricon has been reduced and therefore the situation will be administratively controlled to require restoration of the Tricon leg within 30 days. For the condition that two Tricon legs in a channel are out of service, the protection function can still be performed and the channel is operable, however the redundancy of the Tricon has been significantly reduced and therefore the situation will be administratively controlled to require restoration of one of the two Tricon legs within 7 days. For the condition that all three Tricon legs in a channel are out of service, the protection function cannot be performed and the channel is inoperable and the appropriate TS Condition for the function will be entered.

b) FPGA-Based ALS PPS Equipment

For the condition that the ALS A or B core is out of service, the protection function can still be performed and the channel is operable, however the redundancy and diversity of the ALS has been reduced and therefore the situation will be administratively controlled to require restoration of the ALS core within 30 days. For the condition that an ALS A or B core is out of service in Protections Sets I and II, TS 3.3.3 Condition A will also need to be entered because the RCS wide range temperature parameter provided by ALS to the Post Accident Monitoring Instrumentation RCS hot leg temperature, RCS cold leg temperature, and reactor vessel water level indication system parameters will be inoperable. If both the ALS A and B core are out of service, then the protection function cannot be performed and the channel is inoperable and the appropriate TS Condition for the function will be entered.

4.13 Secure Development and Operational Environment (Section D.12 of DI&C-ISG-06 [1])

Following the LAR format recommended in DI&C-ISG-06 [1], the Secure Development and Operational Environment (SDOE) for IOM, CSI and PG&E in support of the PPS Replacement Project, are described in the following sections.

The NRC approved the DCPP Cyber Security Plan (CSP) in Amendment No. 210 to Facility Operating License DPR-80 and Amendment No. 212 to Facility Operating License DPR-82 for DCPP Unit No. 1 and 2, respectively on July 15, 2011 [48]. In Section 3.0 of the safety evaluation for Amendments 210 and 212, the staff found that the DCPP CSP [48], with the exception of deviations described in Section 4.0 of the safety evaluation, generally conformed to the guidance in NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” Revision 6 [47], which was found to be acceptable by the NRC staff as comparable to RG (RG) 5.71 [46], “Cyber Security Programs for Nuclear Facilities,” to satisfy the requirements contained in 10 CFR 73.54 [44].

The cyber security program that is being implemented per the NRC approved CSP [48] includes provisions applicable to all phases of a systems’ life cycle, including the PPS replacement and modification of critical digital assets. In 2011, the Cyber Security Program Manager and other members of the (Cyber Security Assessment team) CSAT met with the PPS Replacement Project design engineer to discuss the PPS replacement design. The CSAT was formed in accordance with Section 3.1.2 of the CSP [48], and Milestone a on October 3, 2011. A list of critical digital systems and assets was created in accordance with Section 3.1.3 of the CSP [48] and Milestone b on October 31, 2011. The CSAT reviewed scheduled digital upgrades, and added the future equipment to the list of critical digital systems. The CSAT determined the PPS replacement equipment will be a critical system, with several critical digital assets. In addition, the Cyber Security Program Manager and PPS Replacement Project Manager have met with procurement personnel to discuss cyber security principles to be written into the procurement procedures, and the steps that facilitate a secure supply chain.

In December, 2012, the DCPP internal network was isolated from internet connected networks by a deterministic network device, per Milestone c of the CSP [48]. With this deterministic network device, many network attacks, including many that depend on a back door created by a vendor, are not possible. In addition, DCPP personnel implemented actions to lessen the likelihood of an attack initiated by a portable electronic device, or portable media such as a thumb drive, per Milestone d, and section D 1.19 of NEI 08-09 [47]. These actions will mitigate portable media based attacks that depend on a back door created by a vendor.

The Cyber Security Implementation Project Manager has developed a detailed project plan. Several existing plant procedures will be revised. The PPS replacement will inherit the controls implemented by these procedures. Many of the existing procedures will have been changed or new procedures created before the PPS replacement is installed.

The CSAT is collecting and reviewing PPS replacement design information as it becomes available and will make recommendations to enhance the cyber security posture of the PPS upgrade throughout the project. The collected documentation will be reviewed in a formal desktop evaluation per the CSP [48], Section 3.1.5, prior to the PPS replacement installation. The offsite testing facility will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to be turned over to operations, per Section 3.1.5 of the security plan. The CSAT will make their final recommendations after the system walkdown, per Section 3.1.6 of the CSP [48]. Disposition of all controls will be documented in the cyber security assessment tool, CyberWiz. Recommended mitigation will be documented in CyberWiz and the Corrective Action Program.

The DCPP Cyber Security Team will interface with NUPIC (Nuclear Procurement Issues Committee) and the NEI/NITSL counterfeit parts task force to address digital equipment supply chain security.

With regard to software development, NRC RG (RG) 1.152, Rev 3 [45], "Criteria for use of Computers in Safety Systems of Nuclear Power Plants," [45] describes a method that the NRC deems acceptable for complying with regulations for promoting high functional reliability, design quality, and security for the use of digital computers in safety systems for nuclear power plants. In the context of RG 1.152, "security" refers to protective actions taken against a predictable set of non-malicious acts that could challenge the integrity, reliability, or functionality of a digital safety system.

Both IOM and ALS have addressed establishment of a secure development and operational environment in their respective Topical Reports [13], Section 5.3 and [15], Section 8) submitted to NRC for review. Procedures and programs have been put in place to address requirements in this area throughout the life cycle elements that are the primary responsibility of the vendor as described in the following sections.

The PPS replacement is being reviewed to comply with 10 CFR 50.73, the DCPP CSP [48] and NEI 08-09 R6 [47]. A description of the security controls to be included in the PPS replacement is security-related information per 10 CFR 2.390 and was submitted to the NRC staff in PG&E Letter DCL-11-123, dated December 20, 2011 [164].

a) PG&E SDOE

References [49], [50] and [51] provide the DCPP station control procedures for software development throughout the remaining life cycle phases under the control of PG&E after development and delivery of the software from the vendor to PG&E.

b) Invensys SDOE

Triconex Document No. 993754-1-913, PPS Replacement DCPP RG 1.152 Conformance Report [147], meets the guidance in NRC RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," [45] and establishes the Secure Development and Operational Environment for the Triconex portion of the PPS Replacement Project, running on the safety-related V10 Tricon platform hardware.

On July 9 through July 12, 2012, the Cyber Security Project Manager accompanied members of the PG&E Quality Verification group to examine the design and production facilities of Invensys in Lake Forest, California, and examined the code production practices and the development environment, and determined that Invensys has a secure development envirionment, and ensures their employees are reliable and trustworthy.

c) CSI SDOE

CSI Document No. 6002-00006 ALS Security Plan [64], meets the guidance of in NRC RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," [45] and establishes the Secure Development and Operational Environment for the CSI portion of the PPS Replacement Project, running on the safety-related ALS platform hardware.

On September 24 through 26, 2012, the Cyber Security Supervisor accompanied members of the PG&E Quality Verification group to examine the design and production facilities of CS Innovations in Scottsdale, Arizona, and examined the code production practices and the development environment, and determined that CS Innovations had a secure development envirionment in accordance with NRC RG 1.152, Rev 3 [45].

4.14 Tricon V10 Safety Evaluation Application Specific Action Items

The Tricon V10 Safety Evaluation (SE) [158] Section 4.2 lists 19 application-specific actions items (ASAIs) that an applicant needs to address when requesting approval for a safety-related system based on the Tricon V10 platform. This section addresses each of the Tricon V10 Safety Evaluation [158], Section 4.2, ASAIs for the PPS replacement.

ASAI 1

As noted in Section 2.1, IOM also submitted the Nuclear Safety Integration Program Manual (NSIPM). The NSIPM governs application specific development activities that occur at IOM's facility. The NRC staff reviewed this document, but made no safety determinations and it is not approved by this SE. It is an ASAI for the NRC staff to perform a review of any application specific development activities governed by the NSIPM when requesting NRC approval for the installation of a SR system based on the Tricon V10 platform.

As an approved 10 CFR Part 50 Appendix B supplier, Invensys Operations Management adheres to the Invensys Operations Management NSIPM to ensure compliance with NRC requirements regarding safety-related software development. The Invensys Operations Management Quality Procedures Manual (QPM), Project Procedures Manual (PPM), and Manufacturing Department Manual (MDM) are the implementing procedures under the NSIPM.

For the DCPP PPS Replacement Project, Invensys Operations Management is providing the documents listed in Enclosure B to ISG-06. Documents generated by Invensys Operations Management Nuclear Delivery for the PPS Replacement Project are preceded by the number 993547. Invensys Operations Management document 993754-1-905, "Project Management Plan, Appendix A," contains the set of documents Invensys Operations Management is delivering to support the PPS Replacement Project. The details on the project-specific document numbering scheme are contained in 993754-1-905, "Project Management Plan, Appendix B". Section 1.2 of the Project Management Plan provides more detail on the ISG-06 Enclosure B documents that are produced during PPS Replacement Project Phases. Invensys document 993754-1-906, "Software Development Plan," provides details on the application program development process for the PPS Replacement Project.

ASAI 2

Section 3.2 of this SE discusses the software development processes for the Tricon V10 platform. Although the NRC staff has approved the IOM software development and lifecycle planning program (Plans), the NRC staff determined that some of these Plans are also the responsibility of the licensee, and must be developed before the Tricon V10 platform software can be used for SR applications in nuclear power plants. Therefore, *the following Plans must be developed and submitted with any license specific application referencing the Tricon V10 platform:*

- *Software Installation Plan*
- *Software Maintenance Plan*
- *Software Operations Plan*
- *Software Safety Plan*

The NRC staff will evaluate these plans in accordance with BTP 7-14 when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

As described in ISG-06 Sections D.4.4.1.5, D.4.4.1.6, D.4.4.1.8, and Enclosure B, the Software Installation Plan, Software Maintenance Plan, and Software Operations Plan are Phase 3 documents that do need to be submitted to the staff prior to approval and are to be available for inspection in support of any regional inspections of the installation prior to the system being installed.

For the Software Safety Plan, PG&E is not developing software, and therefore no PG&E specific Software Safety Plan is being developed. The Software Safety Plan document for IOM is Triconex Document No. 993754-1-911, "PPS Replacement DCPP SSP," [72] and is discussed in Section 4.5.5.2. The Software Safety Plan document for CSI is CSI Document No. 6116-00000, "Diablo Canyon PPS Management Plan" [60] and is discussed in Section 4.5.5.3."

The System Quality Assurance Program (SyQAP) and System Verification and Validation Plan (SyVVP) discuss that the vendor software is controlled by the vendor at the vendor facilities as discussed in Section 4.5.5.1. The PG&E SCMP [159] has been developed to establish and document a process of change control and for software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility and for the remainder of its life cycle following installation at DCPP. Document SCM 36-01 addresses in part ISG-06, Enclosure B, Item 1.10, "Software Configuration Management Plan."

ASAI 3

Section 2.2 of this SE discusses the regulatory criteria used as the basis for this review. Determination of full compliance with the applicable regulations remains subject to plant specific licensing review of a full system design based on the Tricon V10 platform. Licensees must make a determination of full compliance with the design criteria and regulations identified in SRP Chapter 7, Table 7-1, which are relevant to specific applications of DI&C systems. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The PPS replacement is being licensed in accordance with ISG-06, Revision 1. Guidance to ensure that applicable regulatory requirements, including SRP Chapter 7, Table 7-1, is met for the proposed PPS replacement based in part on the Tricon V10 platform.

ASAI 4

Section 3.1.3.2 of this SE discusses the use of the TriStation 1131. That section noted that the Tricon V10 platform is designed such that the Tricon V10 platform would not normally be connected to a TriStation PC during SR operation. The plant-specific procedures which disconnect or control the connection of the TriStation PC such that theTriStation tool cannot affect the safety related functions of the Tricon PLC system during operation will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform. In addition, the testing of the operational software produced by the TriStation 1131, and these test plans, procedures, and results will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

Invensys Operations Management places no restrictions on duration of the connection of the computer with TriStation 1131 installed to the V10 Tricon. This is because TriStation 1131 has no effect on the TriStation Application Program (TSAP) executing on the V10 Tricon when the Tricon keyswitch is in the RUN position. The V10 Tricon rejects all programming messages from TriStation 1131 while in the RUN mode. The operating mode of the V10 Tricon is changed by placing the Tricon keyswitch to the PROGRAM position to allow accepting the programming messages from the TriStation 1131. The operating mode of the V10 Tricon is not changed by TriStation 1131. For the PPS Replacement Project, the TriStation 1131 TSAP will initiate an alarm output for the operator when the V10 Tricon keyswitch is not in the RUN postion. A combination of physical access controls and administrative controls will be utilized by PG&E during TSAP changes and the affected PPS instrument channel will procedurally be placed out of service any time the Tricon operational mode change Tricon keyswitch is not in the RUN position. Details of the operation of the Tricon keyswitch is contained in Section 4.8.10.

The analysis of the failure modes, i.e., list of failures, their severity, and potential impact, of the Tricon keyswitch is contained in Invensys Operations Management document 9600164-531, "Tricon V10 Failure Modes and Effects Analysis," Revision 1, submitted for the Tricon Approved Topical Report [13]. The effects of failures in the V10 Tricon portion of the PPS Replacement are contained in Invensys Operation Management document 993754-1-811, "Failure Modes and Effects Analysis."

The Invensys Operations Management NSIPM describes the Invensys Operations Management nuclear system integration process, while the Invensys Operations Management Project Procedures Manual (PPM) contains the set of implementing procedures. For the PPS Replacement project, Invensys Operations Management is generating the necessary test documentation to satisfy the guidance contained in ISG-06, including, but not limited to, test plans, test procedures, and test reports for TSAP software verification and V10 Tricon PPS Replacement validation activities.

ASAI 5

Section 3.2 of this SE discusses verification and validation. Although IOM did not strictly follow guidelines of IEEE Std 1012, the NRC staff determined that the combination of the internal IOM review, the TÜV certification, and the review by independent consultants provided acceptable verification and validation for software that is intended for SR use in nuclear power plants. However, the NRC staff noted that a significant portion of its acceptance is predicated upon the independent review by TÜV-Rheinland, and licensees using any Tricon PLC system beyond Tricon V10.5.1 must ensure that similar or equivalent independent V&V is performed; without this, the Tricon PLC system will not be considered acceptable for SR use at nuclear power plants. Should licensees use future Tricon PLC systems beyond Tricon V10.5.1 which have not received TÜV-Rheinland certification, the NRC staff will review the acceptability of the independent V&V during the plant-specific safety evaluation.

For the Tricon V10 being used for the PPS replacement, an independent review by TÜV-Rheinland was performed in accordance with the Invensys Operations Management Engineering Department Manual and Nuclear Qualified Equipment List. The Nuclear Qualified Equipment List contains those products that have been qualified by Invensys Operations Management under its approved 10 CFR Part 50 Appendix B program for nuclear safety-related applications. For the V10 Tricon, before a given release (e.g., 10.5.3) can be put on the Nuclear Qualified Equipment List it must first be certified by TÜV-Rheiland in accordance with the Invensys Operations Management Engineering Department Manual. The Invensys Operations Management Engineering Department Manual was reviewed by the staff during the V10 Tricon SE. The PPS Replacement Project will utilize version 10.5.3 of the V10 Tricon that is on the Invensys Operations Management Nuclear Qualified Equipment List. A Reference Design Change Analysis report for differences between V10.5.1 and 10.5.3 was submitted to the staff in accordance with ISG 06, Section D.8.2 in the Invensys Operations Management Document 993754-1-916, in Attachment 4 to the Enclosure of PG&E Letter DCL-12-069 [160].

ASAI 6

Sections 3.3 and 3.10.2.4 of this SE discuss environmental qualification. EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially

Available PLC for Safety-Related Applications in Nuclear Power Plants," which was accepted by NRC SE dated July 30, 1998, presents a set of requirements to be applied to the generic qualification of PLCs for application to SR I&C systems in nuclear power plants. It is intended to provide a qualification envelope for a plant-specific application. As noted in Section 3.3 of this SE, several EQ tests did not fully meet the acceptance criteria of TR-107330 (e.g., EMC and Seismic Withstand). The licensee must make a determination that the as-tested envelope bounds the requirements of the specific application. Also, licensees must verify that the maximum test voltages cited in Section 3.3 envelop the maximum credible voltages applied to Non-Class 1E interfaces at their facility. Furthermore, licensees must provide further testing or mitigations for equipment that does not meet plant specific requirements such as the multi-mode fiber optic cable noted in Section 3.3.1. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The physical requirements for the DCPP PPS replacement equipment were specified to the vendors in Section 3.1 of the DCPP FRS [28]. Physical requirements specified include temperature, relative humidity, pressure, radiation, seismic, electromagnetic capability, and emissions. The CSI and Invensys Operations Management vendors are required to confirm the equipment meets the physical requirements in the DCPP FRS [28]. The vendors documented how the equipment meets the physical requirements in the DCPP FRS [28] in the vendor requirements traceability matrix (RTM) documents for the PPS replacement in accordance with ISG-06. The RTM for the DCPP PPS replacement for the FPGA-based ALS equipment is CSI document 6116-00059, Revision A, "Diablo Canyon PPS Traceability Matrix," and was submitted to the staff in Attachment 9 to the Enclosure of PG&E Letter DCL-12-050 [157]. The RTM for the DCPP PPS replacement for the Tricon equipment is Invensys Operations Management document 993754-1-804, Revision 1, "Process Protection System Replacement Project, Project Traceability Matrix," and was submitted to the staff in Attachment 12 to the Enclosure of PG&E Letter DCL-12-120 [161].

PG&E will verify that the maximum test voltages applied to the Tricon during Tricon qualification testing envelop the maximum credible voltages for the Non-Class 1E interfaces with the DCPP PPS.

Invensys Operations Management does not manufacture fiber optic cables and thus they are procured from third parties. Therefore safety-related applications of the V10 Tricon utilizing fiber optic communications requires procurement of qualified fiber optic cables. For the PPS Replacement Project, Invensys Operations Management document 993754-1-914, "System Architecture Description," shows the hardware configuration of the V10 Tricon portion of the PPS Replacement, that was submitted in Invensys Operations Management Project Letter to the NRC 993754-26T [162]. There are two points at which the safety-related equipment is interfacing to non-safety equipment: 1) the connection between the safety-related Primary RXM Chassis and the non-safety Remote RXM Chassis; and 2) the connection between the safety-related TCM and the NetOptics Port Aggregator Tap (to allow communications with the non-safety MWS). At both points, the electrical and communications isolation is at the safety-related component (i.e., the Primary RXM Chassis and the TCM, respectively). In both points, the fiber optic cable is performing a non-safety function because it is the medium for non-vital (i.e., non-safety) communications. Therefore, for the PPS Replacement application, the fiber optic cable is not required to be qualified as safety-related.

ASAI 7

Sections 3.4.1 and 3.10.2.5 of this SE discuss response time. On the basis of the measured response times for the baseline testing, the Tricon V10 platform is not in compliance with Section 4.2.1, Item A, of EPRI TR-107330. However, the NRC staff determined that the response time characteristics are suitable to support SR applications in nuclear power plants. The licensee must make a determination regarding the response time performance of a SR system based on the Tricon V10 platform to ensure that it satisfies its plant- and application-specific requirements for system response time presented in the accident analysis in Chapter 15 of the safety analysis report for the plant. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The DCPP PPS time response allotment is 0.409 seconds as described in Section 4.2.12 and is required by Section 3.2.1.10 of the FRS [28]. For the (temperature) channels shared with the ALS FPGA-based system, the 0.409 seconds is allocated between the ALS and the Tricon as stated in Section 1.5.8 of the IRS [29]. Invensys Operations Management performed a worst case time response calculation for the DCPP PPS replacement in Invensys Operations Management document 993754-1-817, "Maximum TSAP Scan Time," that was submitted to the staff in Attachment 1 to the Enclosure of PG&E Letter DCL-12-039 [163].

The Tricon response time will be verified as part of the FAT to verify that Tricon throughput time is bounded by the calculation and in no case exceeds the DCPP PPS replacement allotment (plus contingency) in accordance with the IRS [29]. The results will be documented in the Invensys Operations Management System Response Time Confirmation Report, 993754-1-818, that will be submitted to the staff as part of the ISG-06 Phase 2 submittals at the completion of FAT for the V10 Tricon PPS Replacement architecture.

ASAI 8

Section 3.4.3 of this SE discusses diagnostics and self-test capabilities. The NRC staff reviewed these self-test capabilities, and finds them to be suitable for a digital system *used in SR applications in nuclear power plants. It may also be possible to use some of these diagnostic capabilities to modify or eliminate certain TS-required periodic surveillance tests; however this is a plant specific, application-dependent issue and, therefore, is not addressed in this SE. The licensee must provide any such surveillance test modifications or eliminations as part of plant-specific licensing amendment requests. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.*

PG&E is not requesting to eliminate current TS required periodic surveillance tests or revise current TS surveillance frequencies based on the diagnostic capabilities of the PPS replacement. However, a change to the TS 1.1 definition for COT is proposed based on the diagnostic and self-test capabilities of the Tricon subsystem in the PPS replacement. The change to the TS 1.1 definition for COT is described and justified in Section 4.12.1.

ASAI 9

Section 3.7.2.1 of this SE discusses communications interconnections. All external communications connections will require justification of the deterministic quality of TCM routed data in the application specific review. The licensee must provide a justification that should include the minimum guaranteed throughput on the COMBUS based on application specific scan time and number of I/O and the selected protocol. The justification should also include an assessment of TCM vulnerabilities based on the application specific design (reference CDR Report (Reference 32) and ISG 2&4 NTX-SER-09-10 (Reference 29)). This justification will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

This item is not applicable to the DCPP PPS replacement project because the TCM is not utilized in the DCPP PPS replacement architecture for any safety related communications within a Protection Set or between the four Protection Sets. Interdivisional communications is not incorporated in the PPS replacement design and is prevented through separation of the Protection Sets. The TCM is used to broadcast information to the PDN Gateway Switch (that is connected to the PDN Gateway Computer) via a Port Aggregator tap which allows only one-way communication to the PDN Gateway Switch. The TCM communicates with the non-safety related MWS which is dedicated to the Tricon in its Protection Set (one MWS per Protection Set) via a separate tap on the Port Aggregator which allows two-way communication. Tricon communications is discussed in Section 3.2.2.1 and the PPS replacement communications structure is shown graphically on Figure 3-3. The replacement PPS Non-Safety-Related communications architecture is described in Section 1.5.7 of Figure 1-22 of the IRS [29].

ASAI 10

Section 3.7.2.2 of this SE discusses non-safety I/O connected to a remote RXM chassis. The NRC staff concluded that adequate protection is provided to the safety side I/O bus and the overall safety function. All data received from a non-safety remote RXM must be treated as non-safety data. The licensee must make a determination that adequate isolation is maintained in the design and that no data received from the non-safety I/O is used to make a safety determination. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

For the V10 Tricon portion of the PPS replacement, the TSAP is being developed such that non-safety data from the non-safety I/O will not prevent the safety function when demanded by plant conditions, nor will failures of non-safety I/O points (whether field inputs or non-safety V10 Tricon components) prevent the safety function. As with the safety-related portions, the V10 Tricon utilizes built-in system diagnostics for the non-safety portions of the V10 Tricon system. However, the diagnostics associated with the non-safety portions of the system will not prevent the safety function nor cause spurious trips. The system diagnostics related to the non-safety portions is being provided as alarm outputs (e.g., for use at the non-safety MAS), but will not be used in any TSAP logic for safety-related trip functions.

ASAI 11

Section 3.7.3.1 of this SE discusses the 20 individual points of DI&C-ISG-04, Section 1, Interdivisional Communications. The LTR does not provide a specific safety system design. The licensee must make a determination regarding interdivisional communication including justifications as noted in the individual subsections of Section 3.7.3.1 of this SE report. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The 20 individual positions of DI&C-ISG-04, Section 1, "Interdivisional Communications," are addressed for the PPS replacement in Section 4.8.

ASAI 12

Section 3.7.3.2 of this SE discusses DI&C-ISG-04, Section 2 - Command Prioritization. The design of field device interfaces and the determination of means for command prioritization are application-specific activities. Since the LTR does not address a specific application, no evaluation against this NRC staff position could be performed. The licensee must provide the design of field device interfaces and the determination of means for command prioritization. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on *the Tricon V10 platform.*

The PPS replacement does not utilize command prioritization.

ASAI 13

Section 3.7.3.3 of this SE discusses DI&C-ISG-04, Section 3, Multidivisional Control and Display Stations. The design of information displays and operator workstations and the determination of information sources and interconnections are application-specific activities. Since the LTR does not address a specific application nor include display devices within the scope of the platform, the licensee must provide the design of information displays and operator workstations and the determination of information sources and interconnections. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The PPS replacement does not utilize multidivisional control and display stations. Each Protection Set in the PPS replacement is provided with a dedicated non-safety-related Tricon MWS for the purpose of maintenance and calibration. The MWS within a redundant Protection Set is connected to and communicates with the safety-related equipment in the associated Protection Set. A MWS is not connected to and cannot communicate with safety-related equipment outside its associated Protection Set. Section 4.2.9 discusses the Tricon MWS.

ASAI 14

Section 3.8.1 of this SE discusses the secure development environment. The NRC staff observed elements of the secure development environment during the December 2010 audit at IOM's Irvine, California facility. The NRC staff also reviewed Sections 4.2 and 5.1 of the Tricon V9 SE and find that the previous conclusions still apply. Based on a review of "Tricon V10 Conformance to R.G. 1.152," IOM document NTX-SER-10-14 (Reference 35), Section 3.1, regarding secure development environment and a comparison to the previously reviewed development environment from the Tricon V9 SE combined with direct observations of the current development environment at IOM's facility in Irvine, California, the NRC staff determined that IOM meets the requirements for secure development environment in RG 1.152, Revision 3. The licensee must make a determination that the secure development environment has not changed and confirm that the application secure development environment is the equivalent or otherwise meets the requirements of RG 1.152, Revision 3. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

Invensys Operations Management document 993754-1-913, "Regulatory Guide 1.152 Conformance Report," for the PPS Replacement Project describes the secure development environment at the Invensys facility at Lake Forest, California. Document 993754-1-913 was enclosed in Invensys Operations Management Project Letter 993754-26T to the NRC [162]. The document describes the secure development environment, including a conformance matrix to Regulatory Guide 1.152, Revision 3 [45]. The Lake Forest facility provides enhanced physical access controls to nuclear system integration areas while maintaining the network, personnel, and manufacturing controls that were previously reviewed and approved by the staff for the facility in Irvine, California.

PG&E personnel performed a walkdown of the Lake Forest facility on January 26, 2012, and reviewed Invensys Operations Management compliance with Invensys document 993754-1-913, including security controls, computer access controls, and the application development environment. In addition, from July 10 through 12, 2012, personnel from the PG&E Quality and Cyber Security organizations performed an audit at the Invensys factility in Lake Forest, California to determine if the work for the PPS Replacement Project was being performed in accordance with Regulatory Guide 1.152, Revision 3 [45], and that the secure development environment and secure operational environment was identical to that evaluated by the NRC in the NRC Final Safety Evaluation for the Invensys Operations Management Triconex Topical Report [158]. Compliance to Regulatory Guide 1.152, Revison 3 [45], was checked using a checklist based on this Regulatory Guide, The audit determined Invensys Operations Management work was being performed in a SDOE in accordance with the guidance provided in Regulatory Guide 1.152, Revision 3 [45], and that the secure development environment and secure operational environment was identical to that evaluated by the NRC in the NRC Final Safety Evaluation for the Invensys Operations Management Triconex Topical Report [158].

ASAI 15

Section 3.8.1 of this SE discusses the secure operational environment. Without a specific operational environment to assess, the NRC staff could not reach a final conclusion on the Tricon V10 platform's ability to withstand undesirable behavior of connected systems and preclude inadvertent access. However, the Tricon V10 platform does have features that could be credited by a licensee when demonstrating these protections. Licensees must provide a description of the secure design and operational environment for the application software and hardware at their facility, which will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The Tricon software for the PPS replacement is being developed by Invensys Operations Management at their facilities. For the time period during development of the Tricon at the Invensys Operations Management facilities, Triconex Document Number 993754-1-913, "Nuclear Safety Related Process Protection System Replacement DCPP Regulatory Guide 1.152 Conformance Report," applies and meets the guidance in NRC RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Revision 3 [45], for the safety-related Tricon platform hardware.

PG&E has developed a SCMP [159] for the PPS replacement to document a process for change control and software configuration management for the PPS replacement for the period after shipment of the Tricon equipment from the vendor and for the remainder of its life cycle. PG&E submitted the SCMP to the NRC in Enclosure 4 to PG&E Letter DCL-12-050 [157]. In addition, for the time period following installation of the Tricon in the plant, Section 4.13 on SDOE discusses the DCPP procedures for control and software development throughout the remaining life cycle phases. PG&E, DCPP Procedures CF2, “Computer Hardware, Software, and Database Control,” CF2.ID2, “Software Configuration Management for Plant Operations and Operations Support,” and CF2.ID9, “Software Quality Assurance for Software Development,” provide the DCPP station control procedures for software. A project specific SyQAP and SyVVP have been developed by PG&E to control and administer the Tricon software during all life cycles.

A description of the security controls to be included in the PPS replacement is security-related information per 10 CFR 2.390 and was previously submitted to the NRC in PG&E Letter DCL-11-123 [164].

ASAI 16

Section 3.9 of this SE discusses diversity and defense-in-depth (D3). Since both diversity and defense-in-depth are plant specific topics, the LTR did not address these topics, and therefore are not within the scope of this SE. Sections 3.6.2 and 3.6.3 of Appendix B, "Application Guide," to IOM Document No. 7286-545-1, provide guidance in the preparation of a plant specific D3 evaluation. A review of the differences between the Tricon V10 system and the non-safety control system implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in-depth continue to be maintained must be addressed in a plant-specific D3 evaluation. These determinations will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The D3 evaluation for the DCPP PPS replacement was prepared in accordance with the guidance in NUREG-0800, Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth (D3) in Digital Computer Based Instrumentation and Control Systems," Revision 5, March 2007; submitted to the NRC for approval in PG&E Letter DCL-10-114 [6]; and approved by the NRC in the NRC Letter “Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, ’Process Protection System Replacement Diversity & Defense-In-Depth Assessment’" (TAC Nos. ME4094 and ME4095)” [7].

ASAI 17

Section 3.10.3 of this SE discusses conformance with IEEE Std 603-1991, including setpoint determination. IOM has performed an analysis of accuracy, repeatability, thermal effects and other necessary data for use in a plant-specific setpoint analysis. Licensees must ensure that, when the Tricon V10 is installed, setpoint calculations are reviewed and, if required, setpoints are modified to ensure that the Tricon V10 platform will perform within system specifications. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

Setpoint evaluations and calculations have been performed by Westinghouse for the PPS replacement as described in Section 4.12.2. The setpoint calculations consider the accuracy, repeatability, and thermal effects for the Tricon subsystem.

ASAI 18

Section 3.7.1 of this SE discusses communications with SR equipment. The documentation confirms testing of the TriStation 1131 library with the SAP protocol. However, the protocol will also be implemented at the application layer of the connected SR equipment, presumably an SVDU. The documentation does not confirm that the protocol has been tested with any specific external SR devices. Therefore, it is an ASAI for the applicant to verify that the SAP library is tested in any proposed application specific SR devices. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

This item is not applicable to the DCPP PPS replacement project because an SVDU is not utilized in the DCPP PPS replacement architecture.

ASAI 19

Section 3.7.3.1.10 of this SE discusses protection of safety division software. In order for the NRC staff to accept this keyswitch function as compliant with this Staff Position, the NRC staff will have to evaluate an application specific system communications control configuration including the operation of the keyswitch, the software affected by the keyswitch, and any testing performed on failures of the hardware and software associated with the keyswitch when an applicant requests NRC approval for the installation of a SR system based on the Tricon V10 platform.

The Tricon keyswitch is a four-position, three-ganged switch so that the three MP modules can monitor the position of the switch independently. The Operating System Executive (ETSX) executing on the MP application processor monitors the position of the Tricon keyswitch. The three MPs vote the position of the Tricon keyswitch. The voted position of the Tricon keyswitch is available as a read-only system variable that can be monitored by the TSAP. This allows alarming the Tricon keyswitch position when it is taken out of the RUN position. TriStation 1131 messages to and from the Tricon (i.e., ETSX executing on the MPs) are of a defined format. TriStation 1131 messages for control program (i.e., TSAP) changes, whether download of new control programs or modification of the executing control program, are uniquely identifiable. Such messages are received by ETSX and appropriate response provided depending upon, among other things, the position of the Tricon keyswitch. When a request from TriStation 1131 is received by ETSX to download a new control program or modify the executing control program, ETSX accepts or rejects the request based on the voted Tricon keyswitch position. If the Tricon keyswitch is in RUN, all such messages are rejected. If the Tricon keyswitch is in PROGRAM, the Tricon is considered out of service and ETSX runs through the sequence of steps to download the new or modified control program, as appropriate. Additional information on operation of the Tricon keyswitch is contained in Section 4.8.10.

The analysis of the failure modes, i.e., list of failures, their severity, and potential impact, of the Tricon keyswitch is contained in Invensys Operations Management document 9600164-531, "Tricon V10 Failure Modes and Effects Analysis," Revision 1, submitted for the Tricon Approved Topical Report [13]. The effects of failures in the V10 Tricon portion of the PPS Replacement are contained in Invensys Operation Management document 993754-1-811, "Failure Modes and Effects Analysis."

4.15 Testing

Since the ALS and Tricon FAT is being performed at vendor facilities in different locations, an integrated FAT with the ALS subsystem connected to the Tricon subsystem will not be performed. An overlapping test methodology as described below will ensure that all specified PPS safety function requirements for each platform are verified at the FAT performed for each subsystem. Following completion of the FAT at each vendor facility, PG&E will stage the integrated system and perform an integrated, end-to-end test. A detailed description of the FAT and SAT for the PPS replacement design and the FAT and SAT plan outline is contained below. Invensys Operations Management Document, 993754-1-813, "Validation Test Plan," [74] addresses testing of the Tricon subsystem and CS Innovations Document No. 6116-00005, "DCPP PPS System Test Plan" [67] addresses testing of the ALS subsystem.

4.15.1 Detailed Description of FAT and SAT for PPS Replacement Design

The ALS and the Tricon are directly connected via the analog RCS temperature channels. The ALS provides Class IE signal conditioning for the pressurizer vapor space temperature, RCS wide range temperature, and narrow range RTD inputs to the OPDT and OTDT thermal trip functions due to its improved ability to process 200 Ohm RTD inputs versus Triconex. The ALS processes the resistance (ohms) RTD input signals and transmits the temperature values to the Tricon as analog 4-20 mA signals for the respective protection set.

The resistance to mA conversion will be tested at the ALS FAT to verify that all requirements specified for converting the resistance to current are met. The Tricon FAT will test these channels by injecting the corresponding 4 to 20 mA signals into the Tricon and verifying that all requirements specified for the temperature channels are met. After the FAT, the equipment will be shipped to DCPP and then both systems will be integrated to perform the SAT which will test the analog interface directly along with other interfaces that cannot be tested at the FAT, such as the connection to the PDN Gateway Switch to which the Gateway Computer connects. The PDN Gateway Switch and PDN Gateway Computer(s) were installed in the plant by a previous project and therefore are existing installed plant equipment that does not need to be tested explicitly at the FAT or SAT.

Within each protection set, the ALS and the Tricon are connected to separate and independent MWS units via dedicated digital communication links. The two MWS units share a common KVM interface through a KVM switch. The KVM switch allows the two MWSs to share common peripherals, but does not allow communications between or among any of the computers that are connected to it. A USB printer will be connected to the KVM switch for each protection set to facilitate testing and maintenance activities.

Tricon communications with its dedicated MWS are bidirectional (read/write) using Triconex NET2 port via the fiberoptic media 4352AN TCM. As discussed in Section 3.1.2.9 of the Triconex V10 SE report [13], the TCM provides functional isolation from external devices. The ALS communications with its dedicated MWS are via the unidirectional TXB2 communication links from the ALS-102 board. The TXB2 communication links are electrically isolated at the ALS-102. Unidirectional communications provides functional isolation from the MWS. The unidirectional nature of the links will be verified at the FAT.

For each protection set, the ALS and the Tricon are connected via dedicated digital communication links to the PDN Gateway Computer. A port aggregator network tap is connected between the Tricon and the MWS via bidirectional Port A and Port B. All network traffic between Port A and Port B is reflected to unidirectional Port 1. There is no communication path from Port 1 to either Port A or Port B. In addition to the functional isolation provided by the TCM, the port aggregator provides further functional isolation between the PDN Gateway Computer and the Tricon. The connection between aggregator ports A and B is passive. The port aggregator does not perform any signal processing with respect to communications between Ports A and B, and loss of power to the port aggregator will not prevent communications between Ports A and B.

An ethernet switch is provided between the port aggregator network tap Port B and the Tricon MWS to ensure continued Multicast operation (and availability of Tricon data to the PDN Gateway Computer) in the event of MWS network communication failure. Without the ethernet switch, Multicast transmission would cease on loss of the link up to the MWS. Continued Multicast operation in the event of MWS failure will be verified at FAT.

The ALS communications with the Gateway computer are via the unidirectional TXB1 communication links from the ALS-102 boards. The TXB1 communication links are electrically isolated at the ALS-102 board. Unidirectional communications provides functional isolation from the Gateway computer. The unidirectional nature of the links will be verified at the ALS FAT.

The ALS also communicates with ASU application software in the ALS MWS via the bidirectional TAB communication link. Per the ALS Topical Report [15], Table 5-2, Item 8, the TAB bus is used for communication of information from and to the ASU with the ALS Platform. This communication process is independent from the safety function logic. To enable the TAB bus to the ASU requires physical connection of a communications cable. When the TAB is enabled, an alarm is activated locally and in the main control room. The TAB will be physically disconnected from the ALS MWS when the TAB is not in use. Communications between the ALS MWS and the ALS via the TAB are not possible when the TAB is disconnected. The TAB bus and its interfaces are designed such the buses are non-intrusive in that the bus cannot interfere with processing of any information or data on the RAB. The ALS FAT will verify that the TAB, when enabled, does not interfere with ALS logic processing.

Per the ALS System Design Specification, CS Innovations Document No. 6116 00011 [19], the ALS allows for online maintenance of an operational system such as the bypassing and control of individual ALS outputs and the calibration of individual ALS I/O without affecting adjacent non-bypassed safety channels. The ALS Topical Report [15], Section 3.4, describes calibration of an analog I/O channel using the ASU. The ALS MWS (running the ASU software) is used to select the channel to be calibrated and place that particular channel in BYPASS mode before the external test equipment is connected to the channel wiring on test points located on the field terminal blocks. The channel is placed in CALIBRATE mode to perform the calibration. ALS Topical Report [15], Section 3.5 explains how specific digital output channels may also be placed in BYPASS or OVERRIDE mode from the ALS MWS. The ALS FAT will verify that individual ALS outputs may be bypassed and controlled, and individual ALS I/O may be calibrated without affecting adjacent non-bypassed safety channels.

For the Tricon FAT, PG&E will provide the MWS, port aggregator network tap, network switches, KVM switch, printer, KVM and media converters as needed to test the complete interface between the MWS and the Tricon. Each protection set has its own separate and independent Tricon and ALS MWSs. The MWSs are not shared between or among protection sets. The MWSs share KVM hardware through the KVM switch.

The Tricon FAT will be performed on all four protection sets. Each protection set will be integrated with all equipment necessary to support the FAT. The functionality of the Tricon MWS will be tested during the FAT to verify requirements specified in the PPS replacement Functional Requirements Specifications [28], Interface Requirements Specifications [29] and the Tricon System Requirements Specification [75]. The FAT will verify correct two-way data communications between the Tricon and the MWS through ports A and B of the port aggregator. The FAT will verify that there is no inbound communication path from the network port aggregator tap Port 1 to either Port A or Port B. The Tricon FAT will verify operation of the KVM switch.

PG&E will provide an MWS for the ALS FAT. The port aggregator is not required for the ALS. The communications from both TxB1 and TxB2 one-way RS-422 ports will be tested to verify all specified data is being transmitted correctly. The MWS data display application will be running to display the read only parameters. The ASU software running on the MWS will be tested during the FAT to verify its functionality and to identify any interactions between the ALS ASU software, the ALS MWS data display application, and/or the ALS MWS operating system. The two-way EIA-485 TAB port will be tested by physically connecting and disconnecting the TAB interface cable to verify the ability to isolate the MWS from the ALS, to update specified ALS parameters, and to perform trouble-shooting and diagnostic tasks.

All boards of the same type in the ALS platform have the same capabilities. The boards can be configured by the user to meet the requirements of any protection set. The FAT will be performed on each protection set configuration, the ALS MWS, and all associated equipment that supports the safety function for the specific protection set. That is, Protection Set 1 will be configured and tested with all the associated sensor inputs and appropriate loads on the digital and analog outputs. Upon completion of testing, the equipment will be reconfigured as Protection Set 2 and tested. The same process will be used for Protection Sets 3 and 4.

The PG&E SAT will be performed on an integrated system, including the MWSs, port aggregator network tap, network switches, KVM switch, printer, KVM and media converters. The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT. The SAT will verify functions and connections that cannot be tested at the Tricon or ALS FAT, prior to installation in the plant. The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

4.15.2 FAT Plan Outline

The Tricon FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 mA DC analog temperature input signals from ALS; these signals will be generated by a loop simulator or equivalent test equipment.
2. The FAT will verify bidirectional non-safety NET2-port communications from Tricon TCM1 and TCM2 to the Tricon MWS through the two ethernet media converters, and Ports A and B of the two port aggregator network taps.
3. The FAT will verify continued Multicast transmission from TCM1 and TCM2 in the event of MWS network communication failure.
4. The Tricon FAT configuration will include the MWSs, port aggregator network tap, network switches, KVM switch, printer, and KVM and media converters.
5. The FAT will verify no inbound communication path from Port 1 of the port aggregator network tap to either Port A or Port B exists.
6. The FAT will verify outbound communications from Port 1 of the port aggregator network tap.

The ALS FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 mA DC analog temperature output signals to Tricon: This interface will be monitored by external equipment to verify conversion and scaling. The ALS analog temperature output channels will be terminated with 250 ohm resistors to simulate the Triconex external termination assembly (ETA) panel. Voltage across the resistors will be measured to verify analog output function.
2. Unidirectional only, non-safety EIA-422 communications from the ALS-102 “A” and ALS-102 “B” TXB1 channels: The TXB1 channels will be monitored during the ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB1 channel to either ALS-102 “A” or “B”.
3. Unidirectional only, non-safety EIA-422 communications to the ALS MWS from the ALS-102 “A” and ALS-102 “B” TXB2 channels: The TXB2 channels will be monitored during ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB2 channel to either ALS 102 “A” or “B”.
4. The ALS FAT configuration will include the MWS, KVM switch, printer, KVM and media converters.
5. Bidirectional EIA-485 TAB communication between ALS Chassis “A” and Chassis “B” and ASU software running on the ALS MWS can take place only if

the communication links are physically connected and enabled. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected and enabled.

4.15.3 SAT Plan Outline

1. The PG&E SAT will be performed on an integrated system, including the Tricon and ALS subsystems, MWSs, port aggregator network tap, network switches, KVM switch, printer, KVM and media converters.
2. The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT.
3. The SAT will verify interfaces that cannot be tested at the Tricon or ALS FAT, including, in part, verification of information that is transmitted to the Gateway computer and the control board display.
4. Additional testing of communications between the Tricon and its MWS (including network failure) will be performed at the SAT.
5. The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

5. ABBREVIATIONS, ACRONYMS, AND REFERENCES

5.1 Abbreviations and Acronyms

Table 5-1 Abbreviations & Acronyms

Acronym	Definition
AC	Alternating Current
ADAMS	Agencywide Documents Access and Management System
AFW	Auxiliary Feedwater
ALS	Advanced Logic System
ANS	American Nuclear Society
AMSAC	ATWS Mitigation System Actuation Circuitry
ANSI	American National Standards Institute

Acronym	Definition
ASAI	ApplicationSpecific Action Item
ASME	American Society of Mechanical Engineers
ASU	ALS Service Unit
ATWS	Anticipated Transient Without Scram
BIST	Built-In-Self-Test
BTP	Branch Technical Position
CCF	Common Cause Failure
CCSF	Common Cause Software Failure
CDD	Conceptual Design Document
CLB	Core Logic Board
CMP	Configuration Management Plan
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSI	CS Innovations, Inc.
CSP	Cyber Security Plan
CVI	Containment Ventilation Isolation
D3	Diversity & Defense-in-Depth
DC	Direct Current
DCPP	Diablo Canyon Power Plant
DFWCS	Digital Feedwater Control System
DI&C	Digital Instrumentation & Controls
DIP	Dual In-line Package

Acronym	Definition
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DO	Discrete Output
DPRAM	Dual Port Random Access Memory
DTTA	Delta-T/Tavg
EQ	Environmental Quality
ERO	Enhanced Relay Output
ESD	Electrostatic Discharge
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
ETA	External Termination Assembly
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FRS	Functional Requirements Specification
FSAR	Final Safety Analysis Report
FSM	Finite State Machine
HICR	Highly Integrated Control Room
HSI	Human System Interface
Hz	Hertz
I&C	Instrumentation & Controls
IEC	International Electrotechnical Commission

Acronym	Definition
IEEE	Institute of Electrical and Electronic Engineers
INPO	Institute of Nuclear Power Operations
I/O	Input/Output
IOCCOM	I/O and Communication
IOM	Invensys Operations Management
IRS	Interface Requirements Specification
ISA	International Society of Automation
ISG	Interim Staff Guidance
IV&V	Independent Verification & Validation
KVM	Keyboard Video Mouse
LAR	License Amendment Request
LCO	Limiting Condition for Operation
LED	Light-Emitting Diode
LOCA	Loss of Coolant Accident
LTOP	Low Temperature Overpressure Protection
mA	Milliampere
MAS	Main Annunciator System
MFW	Main Feedwater
MSFIS	Main Steam and Feedwater Isolation System
MSI	Maintenance and Service Interface
MTP	Modification Test Plan
MWS	Maintenance Workstation

Acronym	Definition
NIS	Nuclear Instrumentation System
NQAM	Nuclear Quality Assurance Manual
NRC	Nuclear Regulatory Commission
NSIPM	Nuclear System Integration Program Manual
NVRAM	Non-volatile Random Access Memory
OPΔT, OPDT	Overpower Trip
OTΔT, OTDT	Overtemperature Trip
OVD	Output Voter Diagnostic
P2P	Peer-to-Peer
PG&E	Pacific Gas & Electric Company
PLC	Programmable Logic Controller
PLD	Programmable Logic Device
PMP	Project Management Plan
PORV	Power Operated Relief Valves
PPC	Plant Process Computer
PPM	Project Procedures Manual
PPS	Process Protection System
QA	Quality Assurance
QAM	Quality Assurance Manual
QAP	Quality Assurance Program
RAB	Reliable ALS Bus

Acronym	Definition
RAM	Random Access Memory
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RG	Regulatory Guide
RIS	Regulatory Information Summary
RPS	Reactor Protection System
RT	Reactor Trip
RTA	Reactor Trip Circuit Breaker A
RTB	Reactor Trip Circuit Breaker B
RTD	Resistance Temperature Detector
RTS	Reactor Trip System
RXM	Remote Expander Module
SAT	Site Acceptance Test
SCMP	Software Configuration Management Plan
SDD	Software Design Description
SDOE	Secure Development and Operational Environment
SDP	Software Development Plan
SDS	Software Design Specification
SER	Safety Evaluation Report
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SLI	Steam Line Isolation

Acronym	Definition
SMP	Software Management Plan
SQAP	Software Quality Assurance Plan
SR	Surveillance Requirements
SRS	Software Requirements Specification
SSP	Software Safety Plan
SSPS	Solid State Protection System
STP	Software Test Plan
SyQAP	System Software Quality Assurance Plan
SyVVP	System Verification and Validation
TAB	Test ALS Bus
TC	Thermocouple
TCM	Tricon Communications Module
TMR	Triple Modular Redundant
TS	Technical Specifications
TSAP	Triconex Software Application Program
TTD	Trip Time Delay
TVS	Transient Voltage Suppressor
UV	Undervoltage
V	Volt
V&V	Validation & Verification
WCGS	Wolf Creek Generating Station

5.2 References

1. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Revision 1, “DI&C-ISG-06 Task Working Group #6: Licensing Process Interim Staff Guidance,” January 19, 2011 (ADAMS Accession No. ML110140103)
2. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Revision 1, “DI&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms - Communications Issues (HICRc),” March 6, 2009 (ADAMS Accession No.ML083310185)
3. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Revision 2, “DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues Interim Staff Guidance,” June 5, 2009 (ADAMS Accession No. ML091590268)
4. U.S. Nuclear Regulatory Commission, NUREG-0800, Revision 5, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR [Light-Water Reactor] Edition," (SRP), (ADAMS Accession No. ML070880680)
5. U.S. Nuclear Regulatory Commission, Letter S. Peterson (NRC), to G. Rueger, (PG&E), "Issuance of Amendments for Diablo Canyon Nuclear Power Plant, Unit No.1 (TAC No. M84580) and Unit No.2 (TAC No. M84581),” October 7, 1993 (ADAMS Accession No. ML022350074)
6. PG&E, Letter DCL-10-114, Revision 1, “Submittal of Diablo Canyon Power Plant Topical Report, Process Protection System Replacement Diversity & Defense-in-Depth Assessment,” September 9, 2010 (ADAMS Accession No. ML102580726)
7. U.S. Nuclear Regulatory Commission, Letter “Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, "Process Protection System Replacement Diversity & Defense-In-Depth Assessment" (TAC Nos. ME4094 and ME4095),” April 19, 2011 (ADAMS Accession No. ML110480845)
8. Triconex Corporation, Triconex Topical Reports 7286-545, Revision 1, “Qualification Summary Report” and 7286-546, “Amendment 1 to Qualification Summary Report,” published as EPRI TR-1000799, “Generic Qualification of the Triconex Corporation TRICON Triple Modular Redundant Programmable Logic Controller System for Safety-Related Applications in Nuclear Power Plants,” November 2000 (ADAMS Accession No. ML003757032)
9. Triconex Corporation, Triconex Topical Report 7286-546, Revision 0, “Amendment 1 to Qualification Summary Report,” March 19, 2001 (ADAMS Accession Number ML010810143)
10. Triconex Corporation, Triconex Topical Report 7286-546, Revision 1, "Amendment 1 to Qualification Summary Report,” June 25, 2001 (ADAMS Accession Number ML011790327)
11. U.S. Nuclear Regulatory Commission, NRC Letter from S. Richards (NRC) to J. Martel (Triconex Corporation), “Review of Triconex Corporation Topical

Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1 (TAC No. MA8283)," December 11, 2001 (published as EPRI TR-1003114) (ADAMS Accession No. ML013470433)

12. Invensys Operations Management, Letter No. NRC-V10-11-001, B. Haynes (Invensys Operations Management) to NRC, "Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and "Application for withholding Proprietary Information from Public Disclosure (TAC No. ME2435),"" dated January 5, 2011 (ADAMS Accession No. ML110140437), supplementing Letter No. NRC-V10-09-01, J. Polcyn (Invensys Operations Management) to NRC, "Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal and "Application for withholding Proprietary Information from Public Disclosure,"" September 9, 2009 (ADAMS Accession No. ML092870628)
13. Invensys Operations Management, Triconex Approved Topical Report 7286-545-1-A, Revision 4, "Triconex Topical Report," May 15, 2012, (ADAMS Accession No. ML12146A005)
14. U.S. Nuclear Regulatory Commission, Letter to Wolf Creek Generating Station, "Issuance of Amendment Re: Modification of the Main Steam and Feedwater Isolation System Controls (TAC NO. MD4839)," March 31, 2009 (ADAMS Accession No. ML090610317)
15. CS Innovations, Letter No. 9200-00021, S. Roberts (CS Innovations) to NRC, "Advanced Logic System Topical Report and Supporting Documents Submittal NRC Project Number 779" dated February 15, 2013, including CS Innovations, Document No. 6002-00301, Revision 4, "Advanced Logic System Topical Report."
16. CS Innovations, Document No. 6002-00031, Revision 2, "ALS Diversity Analysis," July 29, 2010 (ADAMS Accession No. ML102160479)
17. Westinghouse Electric Company, Document No. WNA-DS-02442-PGE, Revision 2, "Diablo Canyon Units 1 & 2 Process Protection System Replacement Project, Advanced Logic System (ALS) - System Requirements Specification (Proprietary)," September 2011, contained in Letter No. LTR-NRC-11-50, from J. Gresham (Westinghouse) to NRC, "Submittal of WNA-DS-02442-PGE, Rev. 2, "Diablo Canyon Units 1 & 2 Process Protection System Replacement Project, Advanced Logic System (ALS) System - Requirements Specification) Proprietary),"" dated September 27, 2011.
18. U.S. Nuclear Regulatory Commission, NRC Letter to Duke Energy Carolinas, LLC, "Oconee, Units 1, 2 & 3, Issuance of Amendment Nos. 366, 368, and 367, Reactor Protective System and Engineered Safeguard Protection System Digital Upgrade," January 28, 2010 (ADAMS Accession No. ML100220016)

19. CS Innovations, Document No. 6116-00011, Revision 1, “Diablo Canyon Process Protection System ALS System Design Specification”

20. CS Innovations, Document No. 6116-10201, Revision 1, “Diablo Canyon Process Protection System ALS-102 FPGA Requirements Specification”

21. Institute of Electrical and Electronic Engineers, IEEE Standard 603-1991, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”

22. U.S. Nuclear Regulatory Commission, 10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants”

23. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems”

24. Invensys Operations Management, Document No. NTX-SER-09-10, Revision 2, “Tricon Applications in Nuclear Reactor Protection Systems - Compliance with NRC ISG-2 & ISG-4,” January 5, 2011 (ADAMS Accession No. ML110140437)

25. Invensys Operations Management, Document No. 993754-1-912 “Diablo Canyon Triconex PPS ISG-04 Conformance Report”

26. PG&E, “Diablo Canyon Updated Final Safety Analysis Report,” Revision 19

27. PG&E, “DCPP Process Protection System Replacement Conceptual Design Document (CDD)”

28. PG&E, “DCPP Units 1 & 2 Process Protection System Replacement Functional Requirements Specification (FRS)”

29. PG&E, “DCPP Units 1 & 2 Process Protection System Replacement Interface Requirements Specification (IRS)”

30. Institute of Electrical and Electronic Engineers, IEEE Standard 308-1980, "Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations"

31. Invensys Operations Management, “Corporate Nuclear Quality Assurance Manual (IOM-Q2)”

32. Invensys Operations Management, Document No. NTX-SER-09-021, “Nuclear System Integration Program Manual”

33. Westinghouse Quality Management System

34. Invensys Operations Management, Document No. 9600164-541, “Triconex System Description,” July 24, 2007

35. Invensys Operations Management, “Planning and Installation Guide for Tricon V9-VI0 Systems, Part No. 97200077-002” (Appendix B to Triconex Topical Report 7286-545-1, Revision 4) (ADAMS Accession No. ML110140443)

36. U.S. Nuclear Regulatory Commission, U.S. NRC Regulatory Guide 1.97, Revision 4, “Criteria for Accident Monitoring Instrumentation of Nuclear Power Plants,” March 28, 2006 (ADAMS Accession No. ML060870349)

37. PG&E, DCPP Human System Interface (HSI) Development Guidelines, Revision 1

38. U.S. Nuclear Regulatory Commission, NUREG-0700, “Human-System Interface Design Review Guidelines,” 2002

39. Westinghouse, Document No. WCAP-11082, Revision 6, “Diablo Canyon: Request for Withholding Information from Public Disclosure,” October 28, 2003 (ADAMS Accession No. ML033020380)

40. U.S. Nuclear Regulatory Commission, Regulatory Information Summary 2006-17, “NRC Staff Position on the Requirements of 10 CFR 50.36, "Technical Specifications,” Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels,” August 24, 2006

41. Technical Specification Task Force, TSTF-493, Revision 4, “Clarify Application of Setpoint Methodology for LSSS Functions,” February 23, 2009 (ADAMS Accession No. ML092150990)

42. PG&E, “Diablo Canyon Power Plant Units 1 & 2Technical Specifications”

43. PG&E, “Diablo Canyon Power Plant Units 1 & 2, Technical Specifications Bases”

44. U.S. Nuclear Regulatory Commission, 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks”

45. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”

46. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Revision 0, “Cyber Security Programs for Nuclear Facilities,” January 2010

47. Nuclear Energy Institute, NEI 08-09, Revision 6, “Cyber Security Plan for Nuclear Reactors”

48. U.S. Nuclear Regulatory Commission, Letter to PG&E, “Diablo Canyon Power Plant, Units Nos. 1 and 2 – Issuance of Amendments RE: Approval of Cyber Security Plan (TAC Nos. ME4290 and ME4291), July 15, 2011, including approved Cyber Security Plan

49. PG&E, DCPP Procedure CF2, Revision 8, “Computer hardware, Software and Database Control”

50. PG&E, DCPP Procedure CF2.ID2, Revision 10, “Software Configuration Management for Plant Operations and Operations Support”

51. PG&E, DCPP Procedure CF2.ID9, Revision 2, “Software Quality Assurance for Software Development”

52. PG&E, DCPP “Process Protection System (PPS) Replacement System Quality Assurance Plan (SyQAP)”, Revision 0

53. PG&E, “Software System V&V Plan (SyVVP) for the PPS Replacement Project,” Revision 0

54. CS Innovations, Document No. 6002-00003, Revision 8, “ALS V&V Plan” (ADAMS Accession No. ML110410380)

55. CS Innovations, Document No. 6002-00004, Revision 8, "ALS EQ Plan"
56. CS Innovations, Document No. 6002-00005, Revision 4, "ALS Test Plan"
57. PG&E, "DCPP Process Protection System Replacement Concept, Requirements, and Licensing Phase 1 Project Plan," Revision 1
58. American National Standards Institute, ANSI NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications," 1994
59. CS Innovations, Document No. 6002-00000, Revision 7, "ALS Management Plan" (ADAMS Accession No. ML110410380)
60. CS Innovations, Document No. 6116-00000, Revision 4, "Diablo Canyon PPS Management Plan"
61. FPGA Development Procedure NA 4.51
62. Westinghouse Level 3 Westinghouse Quality Management System Procedure, Electronics Development Procedure NA 4.50
63. CS Innovations, Document No. 6002-00001, Revision 9, "ALS Quality Assurance Plan"
64. CS Innovations, Document No. 6002-00006, Revision 1, "ALS Security Plan"
65. Institute of Electrical and Electronic Engineers, IEEE Standard 323-1983, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations"
66. CS Innovations, Document No. 6002-00002, Revision 9, "ALS Configuration Management Plan"
67. CS Innovations, Document No. 6116-00005, Revision 2, "Diablo Canyon PPS System Test Plan"
68. CS Innovations, Document No. 6002-00010, Revision 17, "ALS Platform Requirements Specification" (ADAMS Accession No. ML110600671)
69. Invensys Operations Management, Triconex Document No. 993754-1-905, "Process Protection System Replacement DCPP Software Project Management Plan (PMP)"
70. Invensys Operations Management, Triconex Document No. 993754-1-906, "Process Protection System Replacement DCPP Software Development Plan (SDP)"
71. Invensys Operations Management, Triconex Document No. 993754-1-801, "Process Protection System Replacement DCPP Software Quality Assurance Plan (SQAP)"
72. Invensys Operations Management, Triconex Document No. 993754-1-911, "Process Protection System Replacement DCPP Software Safety Plan (SSP)"
73. Invensys Operations Management, Triconex Document No. 993754-1-802, "Process Protection System Replacement DCPP Software V&V Plan (SVVP)"

74. Invensys Operations Management, Triconex Document No. 993754-1-813, “Process Protection System Replacement DCPP Software Validation Test Plan (VTP)”

75. Invensys Operations Management, DCPP Tricon, “SRS”
    a. Triconex Document No. 993754-11-809, “Process Protection System Replacement DCPP Software Requirements Specification Protection Set I”
    b. Triconex Document No. 993754-12-809, “Process Protection System Replacement DCPP Software Requirements Specification Protection Set II”
    c. Triconex Document No. 993754-13-809, “Process Protection System Replacement DCPP Software Requirements Specification Protection Set III”
    d. Triconex Document No. 993754-14-809, “Process Protection System Replacement DCPP Software Requirements Specification Protection Set IV”

76. Invensys Operations Management, Triconex Document No. 993754-1-910, “Process Protection System Replacement DCPP Tricon PPS Software Integration Plan (SIntP)”

77. Invensys Operations Management, Triconex Document No. 993754-1-909, “Process Protection System Replacement DCPP Software Configuration Management Plan (SCMP)”

78. International Society of Automation, ISA 67.04-2006, “Setpoints for Nuclear Safety-Related Instrumentation”

79. EPRI TR-102323, Revision 1, “Guidelines for Electromagnetic Interference Testing in Power Plants”

80. Institute of Electrical and Electronic Engineers, IEEE Standard 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”

81. EPRI, Document No. TR-107330, “Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants”

82. CS Innovations, Document No. 6002-10212, Revision 2,“ALS-102, FPA, FMEA, and Reliability Analysis” (ADAMS Accession No. ML110410380)

83. CS Innovations, Document No. 6002-30212, Revision 2, “ALS-302 FPA, FMEA, and Reliability Analysis” (ADAMS Accession No. ML110410380)

84. CS Innovations, Document No. 6002-31112, Revision 2, “ALS-311 FPA, FMEA, and Reliability Analysis,” Revision 1 (ADAMS Accession No. ML110410380)

85. CS Innovations, Document No. 6002-32112, Revision 2, “ALS-321FPA, FMEA, and Reliability Analysis” (ADAMS Accession No. ML110410380)

86. CS Innovations, Document No. 6002-40212, Revision 2, “ALS-402 FPA, FMEA, and Reliability Analysis” (ADAMS Accession No. ML110410380)

87. CS Innovations, Document No. 6002-42112, Revision 2, “ALS-421 FPA, FMEA, and Reliability Analysis” (ADAMS Accession No. ML110410380)

88. U.S. Nuclear Regulatory Commission, 10 CFR 2.390, "Public Inspections, Exemptions, Requests for Withholding"

89. Institute of Electrical and Electronic Engineers, IEEE Standard 384-1981, "Standard Criteria for Independence of Class 1E Equipment and Circuits"

90. Institute of Electrical and Electronic Engineers, IEEE Standard 420-1982, "Design and Qualification of Class 1E Control Boards, Panels, and Racks Used in Nuclear Power Generating Stations"

91. Institute of Electrical and Electronic Engineers, IEEE Standard 494-1974 (R1990), "Methods for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations"

92. Institute of Electrical and Electronic Engineers, IEEE Standard 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits"

93. Invensys Operations Management, Triconex Document No. 7286-540, "Tricon Nuclear Qualification Program Master Configuration List (MCL)"

94. CS Innovations, Document No. 6002-10202, Revision 3, "ALS-102 Design Specification"

95. CS Innovations, Document No. 6002-00011, Revision 13, "ALS Platform Specification" (ADAMS Accession No. ML110600671)

96. Institute of Nuclear Power Operations, INPO AP 913, "Equipment Reliability Process"

97. PG&E, Letter DCL-92-203, "License Amendment Request 92-05, Eagle 21 Process Protection System Upgrade and Resistance Temperature Detector Bypass Elimination," September 21, 1992

98. U.S. Nuclear Regulatory Commission, Letter to PG&E "Issuance of Amendments for Diablo Canyon Nuclear Power Plant, Unit No. 1 (TAC No. M84580) and Unit No. 2 (TAC No. M84581)" dated October 7, 1993 (ADAMS Accession No. ML022350074)

99. Institute of Electrical and Electronic Engineers, IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Systems"

100. Regulatory Guide 1.62, "Manual Initiation of Protective Actions"

101. Institute of Electrical and Electronic Engineers, IEEE Standard 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems"

102. Institute of Electrical and Electronic Engineers, IEEE Standard 497-1981, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating"

103. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions"

104. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems"

105. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems”
106. CS Innovations, Document No. 6002-30202, “ALS-302 Design Specification”
107. CS Innovations, Document No. 6002-31102, “ALS-311 Design Specification”
108. CS Innovations, Document No. 6002-32102, “ALS-321 Design Specification”
109. CS Innovations, Document No. 6002-40202, “ALS-402 Design Specification”
110. CS Innovations, Document No. 6002-42102, “ALS-421 Design Specification”
111. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.153, Revision 1 “Criteria for Safety Systems,” June,1996
112. U.S. Nuclear Regulatory Commission, NUREG-0800, Branch Technical Position 7-17, “Guidance on Self-Test and Surveillance Test Provisions”
113. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, “Criteria for Programmable Digital Computer System Software in Safety-related Systems in Nuclear Plants,” November 1985
114. Institute of Electrical and Electronic Engineers, IEEE Standard 7-4.3.2, “Application Criteria for Programmable Digital Computer System in Safety Systems of Nuclear Power Generating Stations,” 1982
115. U.S. Nuclear Regulatory Commission, RG 1.153, “Criteria for Power, Instrumentation and Control Portions of Safety Systems,” December 1985
116. Institute of Electrical and Electronic Engineers, IEEE Standard 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” 1980
117. Institute of Electrical and Electronic Engineers, IEEE Standard 323, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” 1974
118. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.100 “Seismic Qualification of Electrical Equipment for Nuclear Power Plants,” March 1996
119. Institute of Electrical and Electronic Engineers, IEEE Standard 344, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations” 1975
120. PG&E, Document No. 10115-J-NPG, Revision 1, “DCPP Units 1 & 2 Process Protection System Replacement Controller Transfer Function Specification”
121. Institute of Electrical and Electronic Engineers, IEEE Standard 352-1987, “Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems”
122. EPRI, Document No. TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants,” December 1996

123. Invensys Operations Management, Triconex Report 9600164-532, Revision 0, "Reliability/Availability Report," November 17, 2009 (ADAMS Accession No. ML093280312)

124. Invensys Operations Management, Triconex Report 9600164-535, Revision 1, "Software Qualification Report," January 5, 2010 (ADAMS Accession No. ML100192059)

125. Invensys Operations Management, Triconex 9600164-539, Revision 1, "Critical Digital Review," October 5, 2009 (ADAMS Accession No. ML092070715)

126. CS Innovations Document No. 6002-00030, Revision 9, "ALS Design Tools" (ADAMS Accession No. ML110410380)

127. Institute of Electrical and Electronic Engineers, IEEE/EIA Standard 12207.0-1996, "Standard for Information Technology-Software Life Cycle Processes"

128. International Electrotechnical Commission, Document No. IEC 60880 (1989-09), "Nuclear Power Plants-Instrumentation and Control Systems Important to Safety-Software Aspects for Computer-Based Systems Performing Category A Functions"

129. Institute of Electrical and Electronic Engineers, IEEE Standard 730 TM, "Software Quality Assurance Plans," 1998

130. Institute of Electrical and Electronic Engineers, IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."

131. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for digital Computer Software Used in Safety Systems of Nuclear Power Plants"

132. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

133. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

134. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

135. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

136. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power"

137. Institute of Electrical and Electronic Engineers, IEEE Standard 1058-1998 "IEEE Standard for Software Project Management Plans."

138. Institute of Electrical and Electronic Engineers, IEEE Standard 1228-1994, "IEEE Standard for Software Safety Plans"

139. U.S. Nuclear Regulatory Commission, NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems"

140. Institute of Electrical and Electronic Engineers, IEEE Standard 828-1998, June 25, 1998, "Software Configuration Management Plans"

141. Institute of Electrical and Electronic Engineers, IEEE Standard 1042-1998, "Software Configuration Management"

142. PG&E, DCPP Final Safety Analysis Report Chapter 17, "Quality Assurance," Revision 19

143. Institute of Electrical and Electronic Engineers, IEEE Standard 830-1993, "IEEE Recommended Practice for Software Requirements Specifications"

144. Invensys Operations Management, Triconex Document No. 993754-11-914, "Protection System Replacement DCPP PPS System Architecture Description"

145. Invensys Operations Management, Triconex Document No. NTX-SER-09-06, "Triconex Development Processes for PLDs in Nuclear Qualified Products"

146. Invensys Operations Management, Triconex Document No. NTX-SER-09-05, "Differences between the Tricon V9.5.3 System and the Tricon V10.2.1 System"

147. Invensys Operations Management, Triconex Document No. 993754-1-913, "Process Protection System Replacement DCPP Regulatory Guide 1.152 Conformance Report"

148. Institute of Electrical and Electronic Engineers, IEEE Standard 379-2000, "Single-Failure Criterion to Nuclear Power Generating Station Safety Systems"

149. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.53, Revision 2, "Application of the Single-Failure Criterion to Safety Systems," November 2003

150. Invensys Operations Management, Triconex Document No. NTX-SER-10-14, Revision 0, "Tricon V10 Conformance to Regulatory Guide 1.152" (ADAMS Accession No. ML102040062)

151. U.S. Nuclear Regulatory Commission, 10 CFR, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power, Plants and Fuel Reprocessing Plants"

152. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.70, Revision 1, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants – LWR Edition"

153. PG&E, Diablo Canyon Power Plant Nuclear Procurement Control Program

154. U.S. Nuclear Regulatory Commission, 10 CFR, Part 21, "Reporting of Defects and Non Compliance"

155. NRC Letter from S. Bahadur (NRC) to Clayton Scott (Invensys Operations Management), June 12, 2012 (ADAMS Accession No. ML12158A403)

156. PG&E Letter DCL-11-104, "License Amendment Request 11-07, Process Protection System Replacement," October 26, 2011 (ADAMS Accession No. ML11307A331)

157. PG&E Letter DCL-12-050, "Submittal of Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," June 6, 2012 (ADAMS Accession No. ML12170A837).

158. NRC Letter from R. A. Nelson (NRC) to Brian Haynes (Invensys Operations Management), "Final Safety Evaluation for Invensys Operations Management "Triconex Topical Report," April 12, 2012 (ADAMS Accession Nos. ML120900889 and ML12093A156)

159. PG&E, Document No. SCM 36-01, "Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Software Configuration Management Plan (SCMP)" (ADAMS Accession No. 12170A838)

160. PG&E Letter DCL-12-069, "Submittal of Quality Assurance Plan and Revised Phase 1 Documents for the License Amendment Request for Digital Process Protection System Replacement," August 2, 2012 (ADAMS Accession No. ML 12222A094)

161. PG&E Letter DCL-12-120, "Submittal of Revised Phase 1 and Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," November 27, 2012 (ADAMS Accession No. ML13004A468)

162. Invensys Operations Management Letter No. 993754-26T, October 26, 2011 (ADAMS Accession No. ML 11319A069)

163. PG&E Letter DCL-12-039, "Submittal of V1 0 Tricon Time Response Calculation for the License Amendment Request for Digital Process Protection System Replacement," April 30, 2012 (ADAMS Accession No. ML 12131A513)

164. PG&E Letter DCL-11-123, "Security-Related Information to Support Process Protection System Replacement License Amendment Request 11-07," December 20, 2011 (ADAMS Accession No. ML 113610541)

165. CS Innovations, Document No. 6116-00054, Revision 0, "Diablo Canyon Process Protection System ISG-04 Matrix," (contained in letter in ADAMS Accession No. ML 12342A149)

166. CS Innovations, Document No. 6002-10206, Revision 1, "ALS-102 FPGA Design Specification"

167. Westinghouse, Document No. WCAP-14333-P-A, Revision 1, “Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times,” October 1998.

168. Westinghouse, Document No, WCAP-15376-P-A, Revision 1, “Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times,” March 2003.

169. U.S. Nuclear Regulatory Commission, Letter J. Donohew (NRC), to G. Rueger, (PG&E), "Diablo Canyon Power Plant, Unit No. 1 (TAC No. MC2042) and Unit No. 2 (TAC No. MC2025) - Issuance of Amendment RE: Plant Protection Test Times, Completion Times, and Surveillance Test Intervals,” January 31, 2005 (ADAMS Accession No. ML 050330315)

170. Westinghouse, Document LTR RAM I 13-002 P-Attachment, Revision 0, “Justification for the Application of Technical Specification Changes in WCAP-14333 and WCAP-15376 to the Tricon/ALS Process Protection System at the Diablo Canyon Power Plant,” January 31, 2013.

171. Westinghouse Document WCAP 17696-P, Revision 0, “Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System”, January 2013,

172. U.S. Nuclear Regulatory Commission, NRC Regulatory Guide 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation,” December 1999.

173. Westinghouse Document WCAP-17706-P, Revision 0, “Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant”, January 2013,

174. International Society of Automation, ISA-RP67.04.02, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation,” December 2010

175. International Society of Automation, ISA-S67.04, "Setpoints for Nuclear Safety-Related Instrumentation." 1994.

176. PG&E Inter-Departmental Administrative Procedure CF6.ID1, "Setpoint Control Program"

177. PG&E Program Directive OM7, "Corrective Action Program," and supporting Inter-Departmental Administrative Procedure OM7.ID1, "Problem Identification and Resolution"

178. PG&E Inter-Departmental Administrative Procedure OM7.ID12, "Operability Determination"

List of New and Revised Regulatory Commitments

List of New Commitments

Commitment 1

The TS1131 tool will not normally be running while the Tricon is performing its safety function as described in Section 3.10.2.9 of the Tricon V10 SER. If the TS1131 workstation is connected during online safety operation for maintenance or troubleshooting purposes, its use will be controlled via administrative controls and qualified maintenance personnel.

Commitment 2

With the keyswitch not in RUN, the PPS application will initiate an alarm on the MAS and the channel for each function processed by the Tricon subsystem protection set within the safety division will be declared inoperable with respect to its safety function.

Commitment 3

The electrical isolation qualification of the Class 1E/non-1E data communication will be qualified with an isolation fault test that will be conducted per IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" and Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems." This will be documented in a supplemental test report to be issued by November 15, 2013.

Commitment 4

The unused MWS and KVM switch ports will be addressed in accordance with the DCPP CSP.

Commitment 5

The local printer for each protection set will also be controlled by the PG&E SCMP.

Commitment 6

KVM firmware update will only be done by procedure.

Commitment 7

Configuring the NVRAM in order to replace an ALS I/O board will be performed by PG&E under an approved plant maintenance procedure.

Commitment 8

Control of operation of the Tricon keyswitch will be included in a procedure to ensure the protection set is declared inoperable when the Tricon keyswitch is not in the RUN position.

Commitment 9

Modification of Tricon application software will always be performed using approved DCPP procedures and will normally not be done with the plant online.

Commitment 10

Using approved DCPP procedures, addressable constants, setpoints, parameters, and other settings utilized in the Tricon portion of the PPS will be changed in one Tricon protection set at a time.

Commitment 11

Modification of ALS FPGA application logic will always be performed using approved DCPP procedures and will normally not be done with the plant online.

Commitment 12

When board replacement requires an ALS chassis to be removed from service, the replacement will be performed using an approved DCPP procedure, and will be administratively controlled to require restoration of the ALS chassis within 30 days.

Commitment 13

The algorithms in WCAP-17706-P used to determine the TS setpoints assume that actions specified in Section 5 of WCAP-17706-P are included in the plant surveillance procedures. The actions specified in Section 5 of WCAP-17706-P will be included in the plant surveillance procedures during implementation of the amendment.

Commitment 14

Although the nominal trip setpints for the RTS and ESFAS PPS functions are not required to be be replaced due to the PPS replacement, in order to ensure appropriate control of the as-found and as-left tolerances associated with the TS setpoints for the RTS and ESFAS PPS functions, the 10 CFR 50.59 controlled surveillance test procedures applicable to SRs 3.3.1.7, 3.3.1.10, 3.3.2.5, and 3.3.2.9 will be updated as required as part of implementation of the amendment for each unit. The Actions for the various potential surveillance outcomes will be required as follows:

(1) The instrument channel setpoint exceeds the as-left tolerance but is within the as-found tolerance:

- Reset the instrument channel setpoint to within the as-left tolerance;
- If the instrument channel setpoint cannot be reset to a value that is within the as-left tolerance around the instrument channel setpoint at the completion of the surveillance, if not already inoperable, the instrument channel shall be declared inoperable.

(2) The instrument channel setpoint exceeds the as-found tolerance but is conservative with respect to the TS Allowable Value (AV):

- Reset the instrument channel setpoint to within the as-left tolerance;
- If the instrument channel setpoint cannot be reset to a value that is within the as-left tolerance around the instrument channel setpoint at the completion of the surveillance, if not already inoperable, the instrument channel shall be declared inoperable;
- Enter the channel's as-found condition in the CAP for prompt verification that the instrument is functioning as required, and for further evaluation. Evaluate the channel performance utilizing available information to verify that it is functioning as required before returning the channel to service. The evaluation may include an evaluation of magnitude of change per unit time, response of instrument for reset, previous history, etc., to provide confidence that the channel will perform its specified safety function;
- Document the condition for continued OPERABILITY.

(3) The instrument channel setpoint is non-conservative with respect to the TS AV:

- If not already inoperable, declare the channel inoperable;
- Reset the instrument channel setpoint to within the as-left tolerance;
- Enter the channel's as-found condition in the Corrective Action Program for evaluation. Evaluate the channel performance utilizing available information to verify that it is functioning as required before returning the channel to service. The evaluation may include an evaluation of magnitude of change per unit time, response of instrument for reset, previous history, etc., to provide confidence that the channel will perform its specified safety function.

These procedure actions will apply until procedure actions consistent with a license amendment for TSTF-493, Revision 4, are implemented for all automatic protective devices related to variables having significant safety functions as delineated by 10 CFR 50.36(c)(1)(ii)(A).

Commitment 15

The "Equipment Control Guidelines" (ECGs) will be updated as part of implementation of the amendment for each unit to identify the methodologies used to determine the as-found and as-left tolerances. The ECGs are documents controlled under 10 CFR 50.59 and are incorporated into the FSAR by reference.

Commitment 16

PG&E will continue to implement the commitments for the RTS and ESFAS reflected in Amendments 179 and 181 to avoid risk-significant plant-specific configurations and will continue to use the DCPP plant-specific configuration risk management program procedure AD7.DC6 “On-Line Maintenance Risk Management,” to provide plant configuration control and management with the PPS replacement.

Commitment 17

The CSAT is collecting and reviewing PPS replacement design information as it becomes available will make recommendations to enhance the cyber security posture of the PPS upgrade throughout the project. The collected documentation will be reviewed in a formal desktop evaluation per the CSP, Section 3.1.5, prior to the PPS replacement installation.

Commitment 18

The offsite testing facility will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to be turned over to operations, per Section 3.1.5 of the security plan.

Commitment 19

The CSAT will make their final recommendations after the system walkdown, per Section 3.1.6 of the CSP.

Commitment 20

Disposition of all controls will be documented in the cyber security assessment tool, CyberWiz. Recommended mitigation will be documented in CyberWiz, and the Corrective Action Program.

Commitment 21

The DCPP Cyber Security Team will interface with NUPIC (Nuclear Procurement Issues Committee) and the NEI/NITSL counterfeit parts task force to address digital equipment supply chain security.

Commitment 22

PG&E will verify that the maximum test voltages applied to the Tricon during Tricon qualification testing envelope the maximum credible voltages for the Non-Class 1E interfaces with the DCPP PPS.

Commitment 23

The Tricon response time will be verified as part of the FAT to verify that Tricon throughput time is bounded by the calculation and in no case exceeds the DCPP PPS replacement allotment (plus contingency) in accordance with the IRS. The results will be documented in the Invensys Operations Management System Response Time Confirmation Report, 993754-1-818, that will be submitted to the staff as part of the ISG-06 Phase 2 submittals at the completion of FAT for the V10 Tricon PPS Replacement architecture.

Commitment 24

The Tricon FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 mA DC analog temperature input signals from ALS; these signals will be generated by a loop simulator or equivalent test equipment.
2. The FAT will verify bidirectional non-safety NET2-port communications from Tricon TCM1 and TCM2 to the Tricon MWS through the two Ethernet media converters, and Ports A and B of the two port aggregator network taps.
3. The FAT will verify continued Multicast transmission from TCM1 and TCM2 in the event of MWS network communication failure.
4. The Tricon FAT configuration will include the MWSs, port aggregator network tap, network switches, KVM switch, printer, and KVM and media converters.
5. The FAT will verify no inbound communication path from Port 1 of the port aggregator network tap to either Port A or Port B exists.
6. The FAT will verify outbound communications from Port 1 of the port aggregator network tap.

Commitment 25

The ALS FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 mA DC analog temperature output signals to Tricon: This interface will be monitored by external equipment to verify conversion and scaling. The ALS analog temperature output channels will be terminated with 250 ohm resistors to simulate the Triconex external termination assembly (ETA) panel. Voltage across the resistors will be measured to verify analog output function.
2. Unidirectional only, non-safety EIA-422 communications from the ALS-102 "A" and ALS-102 "B" TXB1 channels: The TXB1 channels will be monitored during the ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB1 channel to either ALS-102 "A" or "B".
3. Unidirectional only, non-safety EIA-422 communications to the ALS MWS from the ALS-102 "A" and ALS-102 "B" TXB2 channels: The TXB2 channels will be monitored during ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB2 channel to either ALS 102 "A" or "B".
4. The ALS FAT configuration will include the MWS, KVM switch, printer, KVM and media converters.
5. Bidirectional EIA-485 TAB communication between ALS Chassis "A" and Chassis "B" and ASU software running on the ALS MWS can take place only if the communication links are physically connected and enabled. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected and enabled.

Commitment 26

1. The PG&E SAT will be performed on an integrated system, including the Tricon and ALS subsystems, MWSs, port aggregator network tap, network switches, KVM switch, printer, KVM and media converters.
2. The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT.
3. The SAT will verify interfaces that cannot be tested at the Tricon or ALS FAT, including, in part, verification of information that is transmitted to the Gateway computer and the control board display.
4. Additional testing of communications between the Tricon and its MWS (including network failure) will be performed at the SAT.
5. The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

List of Revised Commitments

PG&E Letter DCL-11-104

Commitments 1, 2, and 31 previously made in PG&E Letter DCL-11-104, "License Amendment Request 11-07, Process Protection System Replacement," dated October 26, 2011 (ADAMS Accession No. ML12256A308), are out of date and supersed by this letter and are removed:

Commitment 1

Phase 2 documents that have not been previously submitted to the staff will be submitted within 12 months of the requested approval date, by May 30, 2012, except for the specific Phase 2 documents identified below that require manufacture and factory acceptance testing to complete.

Commitment 2

The following Invensys Operations Management Phase 2 documents will be submitted by December 2012:

Summary Test Reports (including Factory Acceptance Tests)
Summary Test Results (including Factory Acceptance Tests)
Summary of Final Digital Electromagnetic Interference, Temperature, Humidity, and Seismic Testing Results for 3601 TN Module
System Response Time Confirmation
As-Manufactured, System Configuration Documentation

The following Westinghouse Phase 2 documents will be submitted by December 2012:

Summary Test Reports (including Factory Acceptance Tests)
Summary Test Results (including Factory Acceptance Tests)
As-Manufactured, System Configuration Documentation

Commitment 31

The implementation of the as-found tolerance and as-left tolerance guidance from Regulatory Issue Summary 2006-17 and TSTF-493, Revision 4, to all applicable TS setpoints will be addressed as part of the License Amendment Request for TSTF-493.

PG&E Letter DCL-12-083

Commitments 6 through 26, and 34 and 35, previously made in PG&E Letter DCL-12-083, Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement, dated September 11, 2012 (ADAMS Accession No. ML11307A331), are superseded by this letter and are removed:

Commitment 6

The resistance to milliamp conversion will be tested at the ALS FAT to verify that all requirements specified for converting the resistance to current are met. The Tricon FAT will test these channels by injecting the corresponding 4 to 20 mA signals into the Tricon and verifying that all requirements specified for the temperature channels are met.

Commitment 7

After the FAT, the equipment will be shipped to DCPP and then both systems will be integrated to perform the SAT which will test the analog interface directly along with other interfaces that cannot be tested at the FAT.

Commitment 8

The ALS communications with its dedicated MWS computer are via the unidirectional TXB2 communication links from the ALS-102 board. The unidirectional nature of the links will be verified at the FAT.

Commitment 9

Continued Multicast operation in the event of MWS failure will be verified at FAT.

Commitment 10

The ALS FAT will verify that the TAB, when enabled, does not interfere with ALS logic processing.

Commitment 11

The ALS FAT will verify that individual ALS outputs may be bypassed and controlled and individual ALS I/O may be calibrated without affecting adjacent non-bypassed safety channels.

Commitment 12

For the Tricon and ALS FAT, PG&E will provide the MWS computer, port aggregator network tap, network switches, KVMT switch, KVMT and media converters as needed to test the complete interface between the MWS and the Tricon.

Commitment 13

The Tricon FAT will be performed on all four protection sets. Each protection set will be integrated with all equipment necessary to support the FAT.

Commitment 14

The functionality of the Tricon MWS computer will be tested during the FAT to verify requirements specified in the PPS replacement Functional Requirements Specification and the Tricon System Requirements Specification.

Commitment 15

The FAT will verify correct two-way data communications between the Tricon and the MWS through Ports A and B of the port aggregator.

Commitment 16

The FAT will verify that there is no inbound communication path from the network port aggregator tap Port 1 to either Port A or Port B.

Commitment 17

The Tricon FAT will verify operation of the KVMT switch

Commitment 18

PG&E will provide an MWS computer for the ALS FAT.

Commitment 19

The communications from both TxB1 and TxB2 one-way RS-422 ports will be tested to verify all specified data is being transmitted correctly.

Commitment 20

The MWS data display application will be running to display the read only parameters. The ASU software running on the MWS will be tested during the FAT to verify its functionality and to identify any interactions between the ALS ASU software, the ALS MWS data display application, and/or the ALS MWS operating system.

Commitment 21

The two-way EIA-485 TAB port will be tested by physically connecting and disconnecting the TAB interface cable to verify the ability to isolate the MWS from the ALS, to update specified ALS parameters, and to perform troubleshooting and diagnostic tasks.

Commitment 22

The FAT will be performed on each protection set configuration, including power supplies, the ALS MWS computer, and all associated equipment that supports the safety function for the specific protection set. That is, Protection Set 1 will be configured and tested with all the associated sensor inputs and appropriate loads on the digital and analog outputs. Upon completion of testing, the equipment will be reconfigured as Protection Set 2 and tested. The same process will be used for Protection Sets 3 and 4.

Commitment 23

The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT.

Commitment 24

The Tricon FAT will test all specified safety-related functions and will also test the following interfaces:

Safety-related 4-20 mA direct current (DC) analog temperature input signals from ALS; these signals will be generated by a loop simulator or equivalent test equipment.

The FAT will verify bidirectional non-safety NET2-port communications from Tricon TCM1 and TCM2 to the Tricon MWS through the two Ethernet media converters, and Ports A and B of the two port aggregator network taps.

The FAT will verify continued Multicast transmission from TCM1 and TCM2 in the event of MWS network communication failure.

The Tricon FAT configuration will include the MWS computers, port aggregator network tap, network switches, KVMT switch, and KVMT and media converters shown in Figure 1.

The FAT will verify no inbound communication path from Port 1 of the port aggregator network tap to either Port A or Port B exists, as previously stated in Section 4.2.13.1 of LAR 11-07.

Commitment 25

The ALS FAT will test all specified safety-related functions and will also test the following interfaces:

Safety-related 4-20 mA DC analog temperature output signals to Tricon: This interface will be monitored by external equipment to verify conversion and scaling. The ALS analog temperature output channels will be terminated with 250 ohm resistors to simulate the Triconex FTP module. Voltage across the resistors will be measured to verify analog output function.

Unidirectional only non-safety EIA-422 communications from the ALS-102 “A” and ALS-102 “B” TXB1 channels: The TXB1 channels will be monitored during the ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB1 channel to either ALS-102 “A” or “B”.

Unidirectional only non-safety EIA-422 communications to the ALS MWS computer from the ALS-102 “A” and ALS-102 “B” TXB2 channels: The TXB2 channels will be monitored during ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB2 channel to either ALS 102 “A” or “B”.

The ALS FAT configuration will include the MWS computer, KVMT switch, KVMT and media converters shown in Figure 1.

Bidirectional EIA-485 TAB communication between ALS Chassis “A” and Chassis “B” and ASU software running on the ALS MWS computer can take place only if the communication links are physically connected and enabled. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected and enabled.

Commitment 26

SAT Plan Outline

The PG&E SAT will be performed on an integrated system, including the Tricon and ALS subsystems, MWS computers, port aggregator network tap, network switches, KVMT switch, KVMT and media converters shown in Figure 1.

The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT.

The SAT will verify interfaces that cannot be tested at the Tricon or ALS FAT, including, in part, verification of information that is transmitted to the Gateway computer and the control board display.

Additional testing of communications between the Tricon and its MWS computer (including network failure) will be performed at the SAT.

The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

Commitment 34

The System Response Time Confirmation Report, 993754-1-818, will be submitted to the staff as part of the ISG-06 Phase 2 submittals at the completion of factory acceptance testing of the V10 Tricon PPS Replacement.

Commitment 35

The Tricon response time will be verified as part of the FAT and the results will be included in the FAT summary report.

Proposed Technical Specification Change(s)

1.1 Definitions (continued)

CHANNEL FUNCTIONAL TEST (CFT)

A CFT shall be:

a. Analog channels - the injection of a simulated or actual signal into the channel as close to the sensor as practical to verify OPERABILITY of all devices in the channel required for channel OPERABILITY, or

b. Bistable channels - the injection of a simulated or actual signal into the sensor to verify OPERABILITY of all devices in the channel required for channel OPERABILITY, or

c. Digital channels - the injection of a simulated or actual signal into the channel as close to the sensor input to the process racks as practical to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.

The CFT may be performed by means of any series of sequential, overlapping, or total channel steps so that the entire channel is tested.

Insert 1

CHANNEL OPERATIONAL TEST (COT)

A COT shall be the injection of a simulated or actual signal into the channel as close to the sensor as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY. The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. The COT may be performed by means of any series of sequential, overlapping or total channel steps.

CORE ALTERATION

CORE ALTERATION shall be the movement of any fuel, sources, or reactivity control components, within the reactor vessel with the vessel head removed and fuel in the vessel. Suspension of CORE ALTERATIONS shall not preclude completion of movement of a component to a safe position.

CORE OPERATING LIMITS REPORT (COLR)

The COLR is the unit specific document that provides cycle specific parameter limits for the current reload cycle. These cycle specific parameter limits shall be determined for each reload cycle in accordance with Specification 5.6.5. Plant operation within these limits is addressed in individual Specifications.

(continued)

TS Inserts

Insert 1

A COT shall be:

a. Analog, bistable, and Eagle 21 process protection system digital channels - the injection of a simulated or actual signal into the channel as close to the sensor input to the process racks as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.

b. Tricon/Advanced Logic System process protection system digital channels - the use of diagnostic programs to test digital hardware, manual verification that the setpoints and tunable parameters are correct, and the injection of simulated process data into the channel as close to the sensor input to the process racks as practical to verify channel OPERABILITY of all devices in the channel required for OPERABILITY.

The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. The COT may be performed by means of any series of sequential, overlapping or total channel steps.

Enclosure
Attachment 3
PG&E Letter DCL-13-043

Revised Technical Specification Page(s)

Remove Page	Insert Page
1.1-2	1.1-2
	1.1-2a

1.1 Definitions (continued)

CHANNEL FUNCTIONAL TEST (CFT)

A CFT shall be:

a. Analog channels - the injection of a simulated or actual signal into the channel as close to the sensor as practical to verify OPERABILITY of all devices in the channel required for channel OPERABILITY, or

b. Bistable channels - the injection of a simulated or actual signal into the sensor to verify OPERABILITY of all devices in the channel required for channel OPERABILITY, or

c. Digital channels - the injection of a simulated or actual signal into the channel as close to the sensor input to the process racks as practical to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.

The CFT may be performed by means of any series of sequential, overlapping, or total channel steps so that the entire channel is tested.

CHANNEL OPERATIONAL TEST (COT)

A COT shall be:

a. Analog, bistable, and Eagle 21 process protection system digital channels - the injection of a simulated or actual signal into the channel as close to the sensor input to the process racks as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY.

b. Tricon/Advanced Logic System process protection system digital channels - the use of diagnostic programs to test digital hardware, manual verification that the setpoints and tunable parameters are correct, and the injection of simulated process data into the channel as close to the sensor input to the process racks as practical to verify channel OPERABILITY of all devices in the channel required for OPERABILITY.

The COT shall include adjustments, as necessary, of the required alarm, interlock, and trip setpoints required for channel OPERABILITY such that the setpoints are within the necessary range and accuracy. The COT may be performed by means of any series of sequential, overlapping or total channel steps.

(continued)

1.1 Definitions (continued)

CORE ALTERATION

CORE ALTERATION shall be the movement of any fuel, sources, or reactivity control components, within the reactor vessel with the vessel head removed and fuel in the vessel. Suspension of CORE ALTERATIONS shall not preclude completion of movement of a component to a safe position.

CORE OPERATING LIMITS REPORT (COLR)

The COLR is the unit specific document that provides cycle specific parameter limits for the current reload cycle. These cycle specific parameter limits shall be determined for each reload cycle in accordance with Specification 5.6.5. Plant operation within these limits is addressed in individual Specifications.

(continued)

Enclosure
Attachment 4
PG&E Letter DCL-13-043

Technical Specification Bases Change(s)

(For information only)

BASES

BACKGROUND (continued)

The RTS instrumentation is segmented into four distinct but interconnected modules as identified below:

1. Field transmitters or process sensors: provide a measurable electronic signal based upon the physical characteristics of the parameter being measured;
2. Signal Process Instrumentation~~Control~~ and Protection System, including Digital Process Protection System, Nuclear Instrumentation System (NIS), field contacts, and protection channel sets: provides signal conditioning, bistable setpoint comparison, process algorithm actuation, compatible electrical signal output to protection system devices, and control board/control room/miscellaneous indications;
3. Solid State Protection System (SSPS), including input, logic, and output bays: initiates proper unit shutdown and/or ESF actuation in accordance with the defined logic, which is based on the bistable outputs from the signal process instrumentation~~control~~ and protection system; and
4. Reactor trip switchgear, including reactor trip breakers (RTBs) and bypass breakers: provides the means to interrupt power to the control rod drive mechanisms (CRDMs) and allows the rod cluster control assemblies (RCCAs), or "rods," to fall into the core and shut down the reactor. The bypass breakers allow testing of the RTBs at power.

Field Transmitters or Sensors

To meet the design demands for redundancy and reliability, more than one, and often as many as four, field transmitters or sensors are used to measure unit parameters. To account for the calibration tolerances and instrument drift, which are assumed to occur between calibrations, statistical allowances are provided in the Trip Setpoint and Allowable Values. The OPERABILITY of each transmitter or sensor can be evaluated when its "as found" calibration data are compared against its documented acceptance criteria.

Signal Process Instrumentation~~Control~~ and Protection System

Generally, three or four channels of process protection~~control~~ equipment are used for the signal processing of unit parameters measured by the field instruments. The process protection~~control~~ equipment provides signal conditioning, comparable output signals for instruments located on the main control board, and comparison of measured input signals with setpoints established by safety analyses. These setpoints are defined

(continued)

BASES

BACKGROUND

Signal Process Instrumentation~~Control~~ and Protection System (continued)

in the FSAR (References 1, 2, 3, 9, 10, & 11). If the measured value of a unit parameter exceeds the predetermined setpoint, an output from a bistable is forwarded to the SSPS for decision evaluation, except in the case of the seismic, turbine stop valve position, auto stop oil pressure, 12 kV bus and RCP breaker inputs which do not go through signal conditioning. Channel separation is maintained up to and through the input bays. However, not all unit parameters require four channels of sensor measurement and signal processing. Some unit parameters provide input only to the SSPS, while others provide input to the SSPS, the main control board, the unit computer, and one or more control systems.

Generally, if a parameter is used only for input to the protection circuits, three channels with a two-out-of-three logic are sufficient to provide the required reliability and redundancy. If one channel fails in a direction that would not result in a partial Function trip, the Function is still OPERABLE with a two-out-of-two logic. If one channel fails, such that a partial Function trip occurs, a trip will not occur and the Function is still OPERABLE with a one-out-of-two logic.

Generally, if a parameter is used for input to the SSPS and a control function, four channels with a two-out-of-four logic are sufficient to provide the required reliability and redundancy. In the case of the Digital Feedwater Control System (DFWCS), the median/signal select (MSS) feature prevents control/protection interaction even though there are only three inputs and 2-out-of-3 logic. The circuit must be able to withstand both an input failure to the control system, which may then require the protection function actuation, and a single failure in the other channels providing the protection function actuation. Again, a single failure will neither cause nor prevent the protection function actuation. These requirements are described in IEEE-279-1971 (Ref. 4) and IEEE-603-1991 for the Tricon/Advanced Logic System Process Protection System (Ref. 6). The actual number of channels required for each unit parameter is specified in Reference 1.

Insert 1

Two logic channels are required to ensure no single random failure of a logic channel will disable the RTS.

The logic channels are designed such that testing required while the reactor is at power may be accomplished without causing a trip. The ~~p~~Process Protection System is designed to permit any one channel to be tested and maintained at power in a bypass mode. If a channel has been bypassed for any purpose, the bypass is continuously indicated in the control room as required by applicable codes and standards. As an alternative to testing in the bypass mode, testing in the trip mode is also possible and permitted.

(continued)

BACKGROUND (continued)

Trip Setpoints and Allowable Values

The Trip Setpoints are the nominal values at which the bistables are set. Any bistable is considered to be properly adjusted when the "as left" value is within the two sided tolerance band for CHANNEL CALIBRATION tolerance. The calibration tolerance, after conversion, should correspond to the rack comparator setting accuracy defined in the latest setpoint study.

The Trip Setpoints used in the bistables are based on the analytical limits stated in Reference 1. The selection of these Trip Setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors for those RTS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 5), the Trip Setpoints and Allowable Values specified in Table 3.3.1-1 in the accompanying LCO are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the Trip Setpoints, including their explicit uncertainties, is provided in WCAP-11082, "Westinghouse Setpoint Methodology for Protection Systems Diablo Canyon Units 1 & 2, 24 Month Fuel Cycle and Replacement Steam Generator Evaluation," September 2007 (Ref. 17) and calculation NSP-1-20-13F (Ref. 18) and NSP-2-20-13F (Ref. 19). Interlock setpoints are Nominal Values provided in the PLS (Westinghouse Precautions Limitations and Setpoints) and their allowable values are calculated in Calculation J-110 Rev 5 (Ref. 20). The actual nominal Trip Setpoint entered into the bistable is more conservative than that specified by the Allowable Value to account for Rack Drift and Rack Measuring and Test Equipment uncertainties. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

Insert 2

Rack drift in excess of the Allowable Value exhibits the behavior that the rack has not met its allowance. Since there is a small statistical chance that this will happen, an infrequent excessive drift is expected. Rack or sensor drift in excess of the allowance that is more than occasional may be indicative of more serious problems and warrants further investigation. In the event a channel's setpoint is found nonconservative with respect to the specified Trip Setpoint, but more conservative than the Allowable Value, the setpoint must be adjusted consistent with the Trip Setpoint value. When a channel's Trip Setpoint is nonconservative with respect to the Allowable Value, declare the channel inoperable and apply the applicable ACTION statement until the channel is returned to OPERABLE status with its Setpoint adjusted consistent with the Trip Setpoint value.

(continued)

BACKGROUND

Trip Setpoints and Allowable Values (continued)

Setpoints in accordance with the Allowable Value ensure that SLs are not violated during AOOs (and that the consequences of DBAs will be acceptable, providing the unit is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed). Note that in the accompanying LCO 3.3.1, the Allowable Values of Table 3.3.1-1 are the LSSS as defined in 10 CFR 50.36.

Insert 3

~~Each channel of the process control equipment can be tested on line to verify that the signal or setpoint accuracy is within the specified allowance requirements. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal, or in the case of the Power Range channels the test signal is added to the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated. SRs for the channels are specified in the SRs section.~~

The Trip Setpoints and Allowable Values listed in Table 3.3.1-1 are based on the methodology described in Reference 17, 18, 19, and 20, and 33, and 34 for the Tricon/Advanced Logic System Process Protection System which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each Trip Setpoint. The inequality sign only indicates conservative direction. The as-left value will be within a two-sided calibration tolerance band on either side of the nominal value. This also applies to the Overtemperature ΔT and Overpower ΔT K values per reference 16. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

Trip Setpoints may be administratively redefined in the conservative direction for several reasons including startup, testing, process error accountability, or even a conservative response for equipment malfunction or inoperability. Some trip functions have historically been redefined at the beginning of each cycle for purposes of startup testing, e.g. Power Range Newtron Flux High and Overtemperature ΔT. Calibration to within the defined calibration tolerance of an administratively redefined, conservative Tip Setpoint is acceptable. Redefinition at full power conditions for these functions is expected and acceptable.

Solid State Protection System

The SSPS equipment is used for the decision logic processing of outputs from the signal processing equipment bistables. To meet the redundancy requirements, two trains of SSPS, each performing the same functions, are provided. If one train is taken out of service for maintenance or test purposes, the second train will provide reactor trip and/or ESF actuation for the unit. If both trains are taken out of service

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

two-out-of-three configuration are generally required when there is no potential for control system and protection system interaction that could simultaneously create a need for RTS trip and disable one RTS channel. The two-out-of-three and two-out-of-four configurations allow one, channel to be tripped during maintenance or testing without causing a reactor trip. Specific exceptions to the above general philosophy exist and are discussed below.

Insert 4 →

Reactor Trip System Functions

The safety analyses and OPERABILITY requirements applicable to each RTS Function are discussed below:

1. Manual Reactor Trip

The Manual Reactor Trip ensures that the control room operator can initiate a reactor trip at any time by using either of two reactor trip switches in the control room. A Manual Reactor Trip accomplishes the same results as any one of the automatic trip Functions. It is used by the reactor operator to shut down the reactor whenever any parameter is rapidly trending toward its Trip Setpoint.

The LCO requires two Manual Reactor Trip channels to be OPERABLE. Each channel is controlled by a manual reactor trip switch. Each channel activates the reactor trip breaker in both trains. Two independent channels are required to be OPERABLE so that no single random failure will disable the Manual Reactor Trip Function.

In MODE 1 or 2, manual initiation of a reactor trip must be OPERABLE (1-out-of-2 coincidence). These are the MODES in which the shutdown rods and/or control rods are partially or fully withdrawn from the core. In MODE 3, 4, or 5, the manual initiation Function must also be OPERABLE if one or more shutdown rods or control rods are withdrawn or the Rod Control System is capable of withdrawing the shutdown rods or the control rods. In this condition, inadvertent control rod withdrawal is possible. In MODE 3, 4, or 5, manual initiation of a reactor trip does not have to be OPERABLE if the Rod Control System is not capable of withdrawing the shutdown rods or control rods and if all rods are fully inserted. If the rods cannot be withdrawn from the core and all of the rods are fully inserted there is no need to be able to trip the reactor. In MODE 6, neither the shutdown rods nor the control rods are permitted to be withdrawn and the CRDMs are disconnected from the control rods and shutdown rods. Therefore, the manual initiation Function is not required.

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.1.6 (continued)

A Note modifies SR 3.3.1.6. The Note states that this Surveillance is required only if reactor power is ≥ 75% RTP and that 72 hours after thermal power is ≥ 75% RTP is allowed for performing the first surveillance after reaching 75% RTP. The SR is deferred until a scheduled testing plateau above 75% RTP is attained during the post-outage power ascension. During a typical post-refueling power ascension, it is usually necessary to control the axial flux difference at lower power levels through control rod insertion. After equilibrium conditions are achieved at the specified power plateau, a power distribution measurement must be taken and the required data collected. The data is typically analyzed and the appropriate excore calibrations completed within 48 hours after achieving equilibrium conditions. An additional time allowance of 24 hours is provided during which the effects of equipment failures may be remedied and any required re-testing may be performed.

The allowance of 72 hours after equilibrium conditions are attained at the testing plateau provides sufficient time to allow power ascensions and associated testing to be conducted in a controlled and orderly manner at conditions that provide acceptable results and without introducing the potential for extended operation at high power levels with instrumentation that has not been verified to be acceptable for subsequent use.

The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.1.7

SR 3.3.1.7 is the performance of a COT every 184 days.

A COT is performed on each required channel to ensure the entire channel will perform the intended Function.

Insert 5

Setpoints must be within the Allowable Values specified in Table 3.3.1-1.

The difference between the current "as found" values and the previous test "as left" values must be consistent with the drift allowance used in the setpoint methodology. The setpoint shall be left set consistent with the assumptions of the current unit specific setpoint methodology.

The "as found" and "as left" values must also be recorded and reviewed for consistency with the assumptions of Reference 7. The frequency of 184 days is justified in Reference 29.

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.1.8 (continued)

Once the unit is in MODE 3, this surveillance is no longer required. If power is to be maintained < P-10 for more than 12 hours or < P-6 for more than 4 hours, then the testing required by this surveillance must be performed prior to the expiration of the 12 hour or 4 hour limit, as applicable. These time limits are reasonable, based on operating experience, to complete the required testing or place the unit in a MODE where this surveillance is no longer required. This test ensures that the NIS source, intermediate, and power range low channels are OPERABLE prior to taking the reactor critical and after reducing power into the applicable MODE (< P-10 or < P-6) for the periods discussed above. The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.1.9

SR 3.3.1.9 is the performance of a TADOT. The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

The SR is modified by a Note that excludes verification of setpoints from the TADOT. Since this SR applies to RCP undervoltage and underfrequency relays, setpoint verification requires elaborate bench calibration and is accomplished during the CHANNEL CALIBRATION.

SR 3.3.1.10

CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to a measured parameter within the necessary range and accuracy.

CHANNEL CALIBRATIONS must be performed consistent with the assumptions of the DCPP setpoint methodology. The difference between the current "as found" values and the previous test "as left" values must be consistent with the drift allowance used in the setpoint methodology.

Insert 5

Whenever an RTD is replaced in Functions 6, 7, or 14, the next required CHANNEL CALIBRATION of the RTDs is accomplished by an inplace cross calibration that compares the other sensing elements with the recently installed sensing element.

The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.1.10 is modified by a Note stating that this test shall include verification that the time constants are adjusted to the prescribed values where applicable.

(continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.15

SR 3.3.1.15 is the performance of a TADOT of Turbine Trip Functions. This TADOT is performed prior to exceeding the P-9 interlock whenever the unit has been in MODE 3. This Surveillance is not required if it has been performed within the previous 31 days. Verification of the Trip Setpoint does not have to be performed for this Surveillance. Performance of this test will ensure that the turbine trip Function is OPERABLE prior to exceeding the P-9 interlock.

SR 3.3.1.16

SR 3.3.1.16 verifies that the individual channel/train actuation response times are less than or equal to the maximum values assumed in the accident analysis. Response time testing acceptance criteria and the individual functions requiring RESPONSE TIME verification are included in Equipment Control Guideline (ECG) 38.1. Individual component response times are not modeled in the analyses.

The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor to the point at which the equipment reaches the required functional state (i.e., control and shutdown rods fully inserted in the reactor core).

For channels that include dynamic transfer Functions (e.g., lag, lead/lag, rate/lag, etc.), the response time test may be performed with the transfer Function set to one, with the resulting measured response time compared to the appropriate FSAR response time. Alternately, the response time test can be performed with the time constants set to their nominal value, provided the required response time is analytically calculated assuming the time constants are set at their nominal values. The response time may be measured by a series of overlapping tests such that the entire response time is measured.

The response time testing for the SG water level low-low does not include trip time delays. Response times include the transmitters, ~~Eagle-21~~ ~~p~~Process ~~p~~Protection System cabinets, solid state protection system cabinets, and actuation devices only. This reflects the response times necessary for THERMAL POWER in excess of 50 percent RTP. For those functions without a specified response time, SR 3.3.1.16 is not applicable.

(continued)

SURVEILLANCE REQUIREMENTS

SR 3.3.1.16 (continued)

SR 3.3.1.16 is modified by a Note stating that neutron detectors are excluded from RTS RESPONSE TIME testing. This Note is necessary because of the difficulty in generating an appropriate detector input signal. Excluding the detectors is acceptable because the principles of detector operation ensure a virtually instantaneous response. The source range preamplifiers are also excluded. This is acceptable because the principles of operation of the preamplifier have been evaluated and a determination made that there are no credible failure mechanisms that could affect response time that would not be detected during routine testing. Response time of the neutron flux signal portion of the channel shall be measured from detector output or input to the first electronic component in the channel, exclusive of the preamplifier.

REFERENCES

1. FSAR, Chapter 7.
2. FSAR, Chapter 6.
3. FSAR, Chapter 15.
4. IEEE Std. 279-1971.
5. 10 CFR 50.49.
6. IEEE Std. 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations"~~Blank~~
7. WCAP-10271-P-A, Supplement 2, Rev. 1, June 1990.
8. WCAP 13632 - PA-1, Rev. 2 "Elimination of Pressure Sensor Response Time Testing Requirements."
9. FSAR, Chapter 9.2.7 & 9.2.2.
10. FSAR, Chapter 10.3 & 10.4
11. FSAR, Chapter 8.3.
12. DCM S-38A, "Plant Protection System"
13. WCAP-13878, "Reliability of Potter & Brumfield MDR Relays", June 1994.
14. WCAP-13900, "Extension of Slave Relay Surveillance Test intervals", April 1994.
15. WCAP-14117, "Reliability Assessment of Potter and Brumfield MDR Series Relays."
16. WCAP-9226, "Reactor Core Response to Excessive Secondary Steam Releases," Revision 1, January 1978.

(continued)

BASES

REFERENCES (continued)

17. WCAP-11082, "Westinghouse Setpoint Methodology for Protection Systems, Diablo Canyon Units 1 and 2, 24 Month Fuel Cycle Evaluation and Replacement Steam Generator," September 2007.
18. NSP-1-20-13F Unit 1 "Turbine Auto Stop Low Oil Pressure."
19. NSP-2-20-13F Unit 2 "Turbine Auto Stop Low Oil Pressure."
20. J-110 "24 Month Fuel Cycle Allowable Value Determination / Documentation and ITDP Uncertainty Sensitivity."
21. IEEE Std. 338-1977.
22. License Amendment 61/60, May 23, 1991.
23. Westinghouse Technical Bulletin ESBU-TB-92-14-R1, "Decalibration Effects of Calorimetric Power Measurements on the NIS High Power Reactor Trip at Power Levels less than 70% RTP," dated February 6, 1996.
24. DCPP NSSS Calculation N-212, Revision 1.
25. License Amendments 157/157, June 2, 2003.
26. WCAP-12472-P-A, "BEACON Core Monitoring and Operations Support System," August 1994.
27. WCAP-14036-P-A, Revision 1, "Elimination of Periodic Protection Channel Response Time Tests," October 1998.
28. WCAP-14333-P-A, Revision 1, "Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times," October 1998.
29. WCAP-15376-P-A, Revision 1, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," March 2003.
30. WCAP-11394-P-A, "Methodology For The Analysis of the Dropped Rod Event," January, 1990
31. License Amendments 205/206, April 29, 2009

Insert 6

32. WCAP-16769-P Revision 1, "Westinghouse SSPS Universal Logic Board Replacement Summary Report 6D30225G01/G02/G03/G04," July 2008.

Technical Specification Bases Inserts (TS Bases Section 3.3.1)

Technical Specification Bases Section 3.3.1

Insert 1, Background

For the Tricon/Advanced Logic System Process Protection System digital channel, each of the four Process Protection System protection channel sets contains a microprocessor-based Tricon programmable logic controller subsystem comprised of three separate legs and a field programmable gate array-based Advanced Logic System (ALS) subsystem comprised of an A core and a B core. The protection set protection function can be performed by any of the three Tricon legs and by either the ALS A core or B core. At least one Tricon leg and one ALS core are required for a protection set to perform all required protection functions required for that protection set.

Insert 2, Background

Westinghouse Document WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant", January 2013 (Ref. 33) and Westinghouse Document WCAP 17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System", January 2013 (Ref. 34), for Setpoints processed by the Tricon/Advanced Logic System Process Protection System and for the remaining Trip Setpoints in

Insert 3, Background

Each channel of the Process Protection System equipment can be tested on line to verify that the signal or setpoint accuracy is within the specified allowance requirements. Once a designated Eagle 21 Process Protection system channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal, or in the case of the Power Range channels the test signal is added to the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated. SRs for the channels are specified in the SRs section.

For the Tricon/Advanced Logic System Process Protection System digital channel, internal diagnostic programs are performed and simulated process data is injected on a periodic basis while the system is in service to test the digital hardware. This takes the place of injecting a simulated signal or actual signal into the channel. The COT includes manual verification of the setpoints and tunable parameters to verify the setpoints and tunable parameters are correct.

Insert 4, Applicable Safety Analyses, LCO, and Applicability

For the RTS functions processed by the Tricon/Advanced Logic System Process Protection System, at least one Tricon leg and one ALS core are required for a protection set and associated instrumentation channels to be OPERABLE. If all three Tricon legs or both ALS cores in a protection set are out of service, the protection function cannot be performed and the protection set and associated instrumentation channels are inoperable and the applicable Conditions for the Table 3.3.1-1 Functions with an inoperable channel must be entered. One or two-out-of-three Tricon legs and one-out-of-two ALS cores in a protection set are sufficient to provide the protection function. To maintain high reliability of the Process Protection System, the maximum time with one or two Tricon leg(s) out of service in a protection set is administratively controlled. To maintain high reliability and diversity of the Process Protection System, the maximum time with one ALS core out of service in a protection set is administratively controlled.

Insert 5, Surveillance Requirements

Plant procedures verify that the instrument channel functions as required by verifying the "as left" and "as found" settings are consistent with those established by the setpoint methodology.

Technical Specification Bases Inserts (TS Bases Section 3.3.1, continued)

Technical Specification Bases Section 3.3.1 (continued)

Insert 6, References

33. WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," January 2013.
34. Westinghouse Document WCAP 17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," January 2013.

BACKGROUND (continued)

During AOOs, which are those events expected to occur one or more times during the unit life, the acceptable limits are:

1. The Departure from Nucleate Boiling Ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling (DNB).
2. Fuel centerline melt shall not occur, and
3. The RCS pressure SL of 2750 psia shall not be exceeded.

Operation within the SLs of Specification 2.0, “Safety Limits (SLs),” also maintains the above values and assures that offsite dose will be within the 10 CFR 50 and 10 CFR 100 criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the unit life. The acceptable limit during accidents is that offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits. Different accident categories are allowed a different fraction of these limits, based on probability of occurrence. Meeting the acceptable consequences for that event is considered having acceptable consequences for that event. However, these values and their associated NTSPs are not considered to be LSSS as defined in 10 CFR 50.36.

The ESFAS instrumentation is segmented into three distinct but interconnected modules as identified below:

- Field transmitters or process sensors and instrumentation: provide a measurable electronic signal based on the physical characteristics of the parameter being measured;
- Signal processing equipment including ~~d~~Digital Process ~~p~~Protection ~~s~~System, field contacts, and protection channel sets: provide signal conditioning, bistable setpoint comparison, process algorithm actuation, compatible electrical signal output to protection system devices, and control board/control room/miscellaneous indications; and
- Solid State Protection System (SSPS) including input, logic, and output bays: initiates the proper unit shutdown or engineered safety feature (ESF) actuation in accordance with the defined logic and based on the bistable outputs from the signal process instrumentation~~control~~ and protection system. The residual heat removal pump trip or refueling water storage tank level-low signal is not processed by the SSPS. The associated relays are located in the residual heat removal pumps control system.

(continued)

BACKGROUND (continued)

Field Transmitters or Sensors

To meet the design demands for redundancy and reliability, more than one, and often as many as four, field transmitters or sensors are used to measure unit parameters. In many cases, field transmitters or sensors that input to the ESFAS are shared with the Reactor Trip System (RTS). In some cases, the same channels also provide control system inputs. To account for calibration tolerances and instrument drift, which are assumed to occur between calibrations, statistical allowances are provided in the Trip Setpoint and Allowable Values. The OPERABILITY of each transmitter or sensor can be evaluated when its "as found" calibration data are compared against its documented acceptance criteria.

Signal Processing Equipment

Generally, three or four channels of process protection~~control~~ equipment are used for the signal processing of unit parameters measured by the field instruments. The process protection~~control~~ equipment provides signal conditioning, comparable output signals for instruments located on the main control board, and comparison of measured input signals with setpoints established by safety analyses. These setpoints are defined in FSAR, Chapter 6 (Ref. 1), Chapter 7 (Ref. 2), and Chapter 15 (Ref. 3). If the measured value of a unit parameter exceeds the predetermined setpoint, an output from a bistable is forwarded to the SSPS for decision evaluation. Channel separation is maintained up to and through the input bays. However, not all unit parameters require four channels of sensor measurement and signal processing. Some unit parameters provide input only to the SSPS, while others provide input to the SSPS, the main control board, the unit computer, and one or more control systems.

Generally, if a parameter is used only for input to the protection circuits, three channels with a two-out-of-three logic are sufficient to provide the required reliability and redundancy. If one channel fails in a direction that would not result in a partial Function trip, the Function is still OPERABLE with a two-out-of-two logic. If one channel fails such that a partial Function trip occurs, a trip will not occur and the Function is still OPERABLE with a one-out-of-two logic.

(continued)

BASES

BACKGROUND

Signal Processing Equipment (continued)

Generally, if a parameter is used for input to the SSPS and a control function, four channels with a two-out-of-four logic are sufficient to provide the required reliability and redundancy. In the case of the Digital Feedwater Control System (DFWCS), the median/signal select (MSS) feature prevents control/protection interaction even though there are only three inputs and 2-out-of-3 logic. The circuit must be able to withstand both an input failure to the control system, which may then require the protection function actuation, and a single failure in the other channels providing the protection function actuation. Again, a single failure will neither cause nor prevent the protection function actuation.

These requirements are described in IEEE-279-1971 (Ref. 4) and IEEE-603-1991 for the Tricon/Advanced Logic System Process Protection System (Ref. 6). The actual number of channels required for each unit parameter is specified in Reference 2.

For the Tricon/Advanced Logic System Process Protection System, each of the four Process Protection System protection channel sets contains a microprocessor-based Tricon programmable logic controller subsystem comprised of three separate legs and a field programmable gate array-based Advanced Logic System (ALS) subsystem comprised of an A core and a B core. The protection set protection function can be performed by any of the three Tricon legs and by either the ALS A core or B core. At least one Tricon leg and one ALS core are required for a protection set to perform all required protection functions required for that protection set.

The channels are designed such that testing required to be performed at power may be accomplished without causing an ESF actuation. The Process Protection System is designed to permit any one channel to be tested and maintained at power in a bypass mode.

If a channel has been bypassed for any purpose, the bypass is continuously indicated in the control room as required by applicable codes and standards. As an alternate to testing in the bypass mode, testing in the trip mode is also possible and permitted.

(continued)

BASES

BACKGROUND (continued)

Trip Setpoints and Allowable Values

The Trip Setpoints are the nominal values at which the bistables are set. Any bistable is considered to be properly adjusted when the "as left" value is within the two-sided tolerance band for calibration accuracy.

Insert 7

The Trip Setpoints used in the bistables are based on the analytical limits stated in Reference 2. The selection of these Trip Setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 5), the Trip Setpoints and Allowable Values specified in Table 3.3.2-1 in the accompanying LCO are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the Trip Setpoints, including their explicit uncertainties, is provided in WCAP-11082, "Westinghouse Setpoint Methodology for Protection Systems Diablo Canyon Units 1 & 2, 24 Month Fuel Cycle and Replacement Steam Generator Evaluation," September 2007 (Ref. 12), calculation J-54 (Ref. 13) and calculation J-110 (Ref. 14). Interlock setpoints are nominal values provided in the PLS (Westinghouse Precautions Limitations and Setpoints) and their allowable values are calculated in Calculation J-110 Rev. 7 (Ref. 14). For Function 5.b in TS Table 3.3.2-1, the magnitudes of these uncertainties are factored into the determination of the NTSP and corresponding AV. The actual nominal Trip Setpoint entered into the bistable is more conservative than that specified by the Allowable Value to account for Rack Drift and Rack Measuring and Test Equipment uncertainties. The calibration tolerance, after conversion, should correspond to the rack comparator setting accuracy defined in the latest setpoint study. For Function 5.b in TS Table 3.3.2-1, the AV serves as the Technical Specification OPERABILITY limit for purposes of the COT. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint is conservative with respect to the Allowable Value, the bistable is considered OPERABLE. For Function 5.b in TS Table 3.3.2-1, note that, although a channel is OPERABLE under these circumstances, the setpoint must be left adjusted to within the established as-left criteria and confirmed to be operating within the statistical allowances of the uncertainty terms assigned.

(continued)

BASES

BACKGROUND

Trip Setpoints and Allowable Values (continued)

Rack drift in excess of the Allowable Value exhibits the behavior that the rack has not met its allowance. Since there is a small statistical chance that this will happen, an infrequent excessive drift is expected. Rack or sensor drift in excess of the allowance that is more than occasional may be indicative of more serious problems and warrants further investigation.

Setpoints in accordance with the Allowable Value and in conjunction with the use of as-found and as-left tolerances ensure that the consequences of Design Basis Accidents (DBAs) will be acceptable, providing the unit is operated from within the LCOs at the onset of the DBA and the equipment functions as designed. For Function 5.b in Table 3.3.2-1, note that the AV is the least conservative value of the as-found setpoint that a channel can have during a periodic CHANNEL CALIBRATION or COT that requires trip setpoint verification.

Insert 8

~~Certain channels can be tested on line to verify that the signal processing equipment and setpoint accuracy is within the specified allowance requirements for Reference 2. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated. SRs for the channels are specified in the SR section.~~

The Trip Setpoints and Allowable Values listed in Table 3.3.2-1 are based on the methodology described in Reference 12, 13, and 14, and 20, and 21 for the Tricon/Advanced Logic System Process Protection System, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each Trip Setpoint. In the event a channel's setpoint is found nonconservative with respect to the specified Trip Setpoint, but more conservative than the Allowable Value, the setpoint must be adjusted consistent with the Trip Setpoint value. When a channel's Trip Setpoint is nonconservative with respect to the Allowable Value, declare the channel inoperable and apply the applicable ACTION statement until the channel is returned to OPERABLE status with its Setpoint adjusted consistent with the Trip Setpoint value. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

The ESFAS Trip Setpoints may be administratively redefined in the conservative direction for several reasons including startup, testing, process error accountability, or even a conservative response for equipment malfunction or inoperability. ESFAS functions are not historically redefined at the beginning of each cycle for purposes of startup or testing as several reactor Trip functions are. However, calibration to within the defined calibration tolerance of an administratively redefined, conservative Trip Setpoint is acceptable. Redefinition at full power conditions for these functions is expected and acceptable.

(continued)

BASES

APPLICABLE SAFETY ANALYSES, LCO, and APPLICABILITY (continued)

Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

The LCO generally requires OPERABILITY of four or three channels in each instrumentation function and two channels in each logic and manual initiation function. The two-out-of-three and the two-out-of-four configurations allow one channel to be tripped, cut-out or bypassed during maintenance or testing without causing an ESFAS initiation. Two logic or manual initiation channels are required to ensure no single random failure disables the ESFAS.

Insert 9

The required channels of ESFAS instrumentation provide unit protection in the event of any of the analyzed accidents. ESFAS protection functions are as follows:

1. <u>Safety Injection</u>

   Safety Injection (SI) provides two primary functions:

   1. Primary side water addition to ensure maintenance or recovery of reactor vessel water level (coverage of the active fuel for heat removal, clad integrity, and for limiting peak clad temperature to < 2200°F); and
   2. Boration to ensure recovery and maintenance of SDM (k_{eff} < 1.0).

   These functions are necessary to mitigate the effects of high energy line breaks (HELBs) both inside and outside of containment. The SI signal is also used to initiate other Functions such as:

   - Phase A Isolation;
   - Containment Ventilation Isolation;
   - Reactor Trip;
   - Turbine Trip from Reactor Trip with P-9;
   - Feedwater Isolation and Feedwater Pump Turbine Trip;
   - Start of motor driven auxiliary feedwater (AFW) pumps;
   - Control room ventilation to pressurization mode via Phase A isolation, and Auxiliary Building to "Building and Safeguards or Safeguards Only" mode;
   - Start of the diesel generators (DGs) and transfer to the startup bus;
   - Start of the containment fan cooler units (CFCUs) in low speed;
   - Start of the component cooling water and auxiliary salt water pumps;
   - Input to containment spray pump and discharge valve auto start (with containment spray signal);
   - Isolate SG sample blowdown lines.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.2

SR 3.3.2.2 is the performance of an ACTUATION LOGIC TEST. The SSPS is tested using the semiautomatic tester. The train being tested is placed in the bypass condition, thus preventing inadvertent actuation. Through the semiautomatic tester, all possible logic combinations, with and without applicable permissives, are tested for each protection function. In addition, the master relay coil is pulse tested for continuity. This verifies that the logic modules are OPERABLE and that there is an intact voltage signal path to the master relay coils. The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.2.3 - Not used

SR 3.3.2.4

SR 3.3.2.4 is the performance of a MASTER RELAY TEST. The MASTER RELAY TEST is the energizing of the master relay, verifying contact operation and a low voltage continuity check of the slave relay coil. Upon master relay contact operation, a low voltage is injected to the slave relay coil. This voltage is insufficient to pick up the slave relay, but large enough to demonstrate signal path continuity. The time allowed for the testing (4 hours) is justified in Reference 8. The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.2.5

SR 3.3.2.5 is the performance of a COT.

A COT is performed on each required channel to ensure the entire channel will perform the intended Function. Setpoints must be found conservative with respect to the Allowable Values specified in Table 3.3.2-1.

Insert 10

The difference between the current "as found" values and the previous test "as left" values must be consistent with the drift allowance used in the setpoint methodology. The setpoint shall be left set consistent with the assumptions of the current unit specific setpoint methodology.

The "as found" and "as left" values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis (Ref. 8) when applicable.

The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

The next two paragraphs apply only to Function 5.b, an SL-LSSS function, in TS Table 3.3.2-1.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.7 - Not used

SR 3.3.2.8

SR 3.3.2.8 is the performance of a TADOT. This test is a check of the Manual Actuation Functions (except AFW; see SR 3.3.2.13). Each Manual Actuation Function is tested up to, and including, the master relay coils. In some instances, the test includes actuation of the end device (i.e., pump starts, valve cycles, etc.). The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program. The SR is modified by a Note that excludes verification of setpoints during the TADOT for manual initiation Functions. The manual initiation Functions have no associated setpoints.

SR 3.3.2.9

SR 3.3.2.9 is the performance of a CHANNEL CALIBRATION.

CHANNEL CALIBRATION is a complete check of the instrument loop, including the sensor. The test verifies that the channel responds to measured parameter within the necessary range and accuracy.

CHANNEL CALIBRATIONS must be performed consistent with the assumptions of the unit specific setpoint methodology. The difference between the current "as-found" values and the previous test "as-left" values must be consistent with the drift allowance used in the setpoint methodology.

Insert 10

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.12

SR 3.3.2.12 is the performance of an ACTUATION LOGIC TEST. This SR is applied to the RHR Pump Trip on RWST Level-Low actuation logic and relays which are not processed through the SSPS. The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program.

SR 3.3.2.13

SR 3.3.2.13 is the performance of a TADOT. This test is a check of the Manual Actuation Function for AFW. Each Manual Actuation Function is tested up to, and including, the master relay coils. In some instances, the test includes actuation of the end device (i.e., pump starts, valve cycles, etc.). The Surveillance Frequency is based on operating experience, equipment reliability, and plant risk and is controlled under the Surveillance Frequency Control Program. The SR is modified by a Note that excludes verification of setpoints during the TADOT for manual initiation Functions. The manual initiation Functions have no associated setpoints.

REFERENCES

1. FSAR, Chapter 6.
2. FSAR, Chapter 7.
3. FSAR, Chapter 15.
4. IEEE Std.279-1971.
5. 10 CFR 50.49.
6. IEEE Std. 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations"~~Blank~~
7. WCAP-13900, "Extension of Slave Relay Surveillance Test intervals", April 1994
8. WCAP-10271-P-A, Supplement 2, Rev. 1, June 1990.

(continued)

BASES

REFERENCES (continued)

9. WCAP-13878, "Reliability of Potter & Brumfield MDR Relays", June 1994.

10. WCAP-14117, "Reliability Assessment of Potter and Brumfield MDR Series Relays."

11. WCAP-13632-P-A, Revision 2, "Elimination of Pressure Sensor Response Time Testing Requirements," January 1996.

12. WCAP-11082, "Westinghouse Setpoint Methodology for Protection Systems, Diablo Canyon Units 1 and 2, 24 Month Fuel Cycle and Replacement Steam Generator Evaluation," September 2007.

13. Calculation J-54, "Nominal Setpoint Calculation for Selected PLS Setpoints."

14. J-110, "24 Month Fuel Cycle Allowable Value Determination / Documentation and ITDP Uncertainty Sensitivity."

15. License Amendment 61/60, May 23, 1991.

16. WCAP-14036-P-A, Revision 1, "Elimination of Periodic Protection Channel Response Time Tests," October 1998.

17. WCAP-14333-P-A, Revision 1, "Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times," October 1998.

18. WCAP-15376-P-A, Revision 1, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," March 2003.

Insert 11

19. 10 CFR 50.55a(h), "Protection and Safety Systems."

Technical Specification Bases Inserts (TS Bases Section 3.3.2)

Technical Specification Bases Section 3.3.2

Insert 7, Background

Westinghouse Document WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant", January 2013 (Ref. 20) and Westinghouse Document WCAP 17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System", January 2013 (Ref. 21), for Setpoints processed by the Tricon/Advanced Logic System Process Protection System and for the remaining Trip Setpoints in

Insert 8, Background

For the Tricon/Advanced Logic System Process Protection System digital channel, each channel of the Process Protection System equipment can be tested on line to verify that the signal or setpoint accuracy is within the specified allowance requirements. Once a designated Eagle 21 Process Protection system channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal, or in the case of the Power Range channels the test signal is added to the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated. SRs for the channels are specified in the SRs section.

For the Tricon/Advanced Logic System Process Protection System digital channel, internal diagnostic programs are performed and simulated process data is injected on a periodic basis while the system is in service to test the digital hardware. This takes the place of injecting a simulated signal or actual signal into the channel. The COT includes manual verification of the setpoints and tunable parameters to verify the setpoints and tunable parameters are correct.

Insert 9, Applicable Safety Analyses, LCO, and Applicability

For the ESFAS functions processed by the Tricon/Advanced Logic System Process Protection System, at least one Tricon leg and one ALS core are required for a protection set and associated instrumentation channels to be OPERABLE. If all three Tricon legs or both ALS cores in a protection set are out of service, the protection function cannot be performed and the protection set and associated instrumentation channels are inoperable and the appropriate Conditions for the Table 3.3.2-1 Functions with an inoperable channel must be entered. One or two-out-of-three Tricon legs and one-out-of-two ALS cores in a protection set are sufficient to provide the protection function. To maintain high reliability of the Process Protection System, the maximum time with one or two Tricon leg(s) out of service in a protection set is administratively controlled. To maintain high reliability and diversity of the Process Protection System, the maximum time with one ALS core out of service in a protection set is administratively controlled.

Insert 10, Surveillance Requirements

Plant procedures verify that the instrument channel functions as required by verifying the "as left" and "as found" settings are consistent with those established by the setpoint methodology.

Insert 11, References

20. WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," January 2013.
21. Westinghouse Document WCAP 17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," January 2013.

Enclosure
Attachment 5
PG&E Letter DCL-13-043

FSAR Change(s)

(For information only)

operations. The monitoring systems are described in Section 11.4. The offsite radiological monitoring program is described in Section 11.6.

Waste handling systems are incorporated in each facility design for processing and/or retention of normal operation radioactive wastes with appropriate controls and monitors to ensure that releases do not exceed the limits of 10 CFR 20. The facilities are also designed with provisions to monitor radioactivity release during accidents and to prevent releases from causing exposures in excess of the guideline levels specified in 10 CFR 100.

3.1.4.8 Criterion 18, 1967 - Monitoring Fuel and Waste Storage (Category B)

Monitoring and alarm instrumentation shall be provided for fuel and waste storage and handling areas for conditions that might contribute to loss of continuity in decay heat removal and to radiation exposures.

Discussion

The fuel and waste storage and handling areas are provided with monitoring and alarm systems for radioactivity, and the plant vents are monitored for radioactivity during all operations. The monitoring systems are described in Section 11.4.

The spent fuel pool cooling system is equipped with adequate instrumentation for normal operation. Water temperatures in the pool and at the outlet of the heat exchanger are indicated locally, and high pool temperature is alarmed in the control room. The spent fuel pool cooling system is described in Section 9.1.

3.1.5 RELIABILITY AND TESTABILITY OF PROTECTION SYSTEMS

GDCs related to reliability and testing of protection systems are presented in this section. A discussion of conformance follows each criterion.

3.1.5.1 Criterion 19, 1967 - Protection Systems Reliability (Category B)

Protection systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

Discussion

Insert 1

The protection systems are designed for high functional reliability and inservice testability. Each design employs redundant logic trains and measurement and equipment diversity. Sufficient redundancy is provided to enable individual end-to-end channel tests with each reactor at power without compromise of the protective function. Built-in semiautomatic testers provide means to test the majority of system components very rapidly. The protection systems are described in Section 7.2.

3.1.5.2 Criterion 20, 1967 - Protection Systems Redundancy and Independence (Category B)

Redundancy and independence designed into protection systems shall be sufficient to assure that no single failure or removal from service of any component or channel of a system will result in loss of the protection function. The redundancy provided shall include, as a minimum, two channels of protection for each protection function to be served. Different principles shall be used where necessary to achieve true independence of redundant instrumentation components.

Discussion

Sufficient redundancy and independence is designed into the protection systems to ensure that no single failure nor removal from service of any component or channel of a system will result in loss of the protection function. The minimum redundancy is exceeded in each protection function that is active with the reactor at power.

Insert 2

Functional diversity and consequential location diversity are designed into the systems. DCPP uses a ~~the Westinghouse Eagle 21~~ Process Protection System, which is discussed in detail in Section 7.2.

3.1.5.3 Criterion 21, 1967 - Single Failure Definition (Category B)

Multiple failures resulting from a single event shall be treated as a single failure.

Discussion

When evaluating the protection systems, the ESF, and their support systems, multiple failures resulting from a single event are treated as a single failure. The ability of each system to perform its function with a single failure is discussed in the sections describing the individual systems. The single failure criterion is discussed further at the beginning of Section 3.1.1.

3.1.5.4 Criterion 22, 1967 - Separation of Protection and Control Instrumentation Systems (Category B)

Protection systems shall be separated from control instrumentation systems to the extent that failure or removal from service of any control instrumentation system component or channel, or of those common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels.

Discussion

The protection systems, except the Process Protection System, comply with the requirements of IEEE-279, 1971, Criteria for Protection Systems for Nuclear Power

Insert 3

Generating Stations, although construction permits ~~for the~~ DCPP units were issued prior to issuance of the 1971 version of the standard.

Each protection system is separate and distinct from the respective control systems. The control system is dependent on the protection system in that control signals are derived from protection system measurements, where applicable. These signals are transferred to the control system by isolation amplifiers that are classified as protection system components. The adequacy of system isolation has been verified by testing or analysis under conditions of all postulated credible faults. Isolation devices that serve to protect Instrument Class IA instrument loops have all been tested. For certain applications where the isolator is protecting an Instrument Class IB instrument loop, and the isolation device is a simple linear device with no complex failure modes, the analysis was used to verify the adequacy of the isolation device. The failure or removal of any single control instrumentation system component or channel, or of those common to the control instrumentation system component or channel and protection circuitry, leaves intact a system that satisfies the requirements of the protection system. The protection systems and control systems are discussed in Chapter 7.

3.1.5.5 Criterion 23, 1967 - Protection Against Multiple Disability of Protection Systems (Category B)

The effects of adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those of an accident, shall not result in loss of the protection function.

Discussion

Physical separation and electrical isolation of redundant channels and subsystems, functional diversity of subsystems, and safe failure modes are employed in design of the reactors as defenses against functional failure through exposure to common causative factors. The redundant logic trains, reactor trip breakers, and ESF actuation devices are physically separated and electrically isolated. Physically separate channel trays, conduits, and penetrations are maintained upstream from the logic elements of each train.

The protection system components have been qualified by testing under extremes of the normal environment. In addition, components are tested and qualified according to individual requirements for the adverse environment specific to their location that might result from postulated accident conditions. The protection systems are discussed in Section 7.2.

3.1.5.6 Criterion 24, 1967 - Emergency Power for Protection Systems (Category B)

In the event of loss of all offsite power, sufficient alternate sources of power shall be provided to permit the required functioning of the protection systems.

Discussion

The facility is supplied with normal and standby emergency power to provide for the required functioning of the protection systems.

In the event of loss of normal power, emergency ac power is supplied by six diesel generators, as described in Chapter 8. Only four diesels are required to supply the power requirements with one unit in an accident situation and to bring the other to the shutdown condition from full power.

The instrumentation and controls portions of the protection systems are supplied initially from the station batteries and subsequently from the emergency diesel generators. A single failure of any one component will not prevent the required functioning of protection systems.

3.1.5.7 Criterion 25, 1967 - Demonstration of Functional Operability of Protection Systems (Category B)

Means shall be included for testing protection systems while the reactor is in operation to demonstrate that no failure or loss of redundancy has occurred.

<u>Discussion</u>

All reactor protection channels employed in power operation are sufficiently redundant so that individual testing and calibration, without degradation of the protection function or violation of the single failure criterion, can be performed with the reactors at power. Such testing discloses failures or reduction in redundancy that may have occurred. Removal from service of any single channel or component does not result in loss of minimum required redundancy. For example, a two-out-of-three function becomes a one-out-of-two function when one channel is removed.

Insert 4

Semiautomatic testers are built into each of the two logic trains in the reactor protection system. These testers have the capability of testing the major part of the protection system very rapidly while the reactor is at power. Between tests, the testers continuously monitor a number of internal protection system points, including the associated power supplies and fuses. Outputs of the monitors are logically processed to provide alarms for failures in one train and automatic reactor trip for failures in both trains. A self-testing provision is designed into each tester. Additional details can be found in Section 7.2.

3.1.5.8 Criterion 26, 1967 - Protection Systems Fail-Safe Design (Category B)

The reactor protection systems shall be designed to fail into a safe state or into a state established as tolerable on a defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or adverse environments (e.g., extreme heat or cold, fire, steam, or water) are experienced.

<u>Discussion</u>

Final Safety Analysis Report Inserts (FSAR Section 3.1)

Final Safety Analysis Report (FSAR) Section 3.1

Insert 1, Section 3.1.5.1

The Process Protection System contains self-test and self-diagnostic functions that reduce the likelihood of undetected failures.

Insert 2, Section 3.1.5.2

comprised of Invensys Operations Management Tricon subsystem and a CS Innovations Advanced Logic System subsystem,

Insert 3, Section 3.1.5.4

The Process Protection System complies with the requirements of IEEE-603, 1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, and IEEE-7-4.3.2, 2003, Standard Criteria for Digital Computers in Safety Systems for Nuclear Power Generating Stations.

Insert 4, Section 3.1.5.7

The Process Protection System is designed to be rapidly tested at power. The Process Protection System contains self-test and self-diagnostic functions in each channel that continuously verify critical components within the channel are operational and provide indication of faults while the reactor is at power.

The tripping action of the bistable amplifier circuitry was checked after each series of tests to insure that the seismic test input had not impaired this function.

During front-to-back testing of the circuit board, an internal power supply circuit board disengaged from its connector causing complete failure of the module. Restraining clamps were installed on the circuit board and the test was repeated successfully. These clamps have since been installed on all similar modules. All recorded electrical signals performed properly during and after the tests.

In addition, as part of the overall program to demonstrate the adequacy of the seismic test previously conducted, multiple frequency, multiple axis test (Reference 11) were performed on an entire typical channel, including signal conditioning circuits and the bistables, of the process instrumentation system. The results of the bistable tests show that the electrical functions of each bistable module maintained electrical operability both during and after each seismic event. In addition, no spurious bistable actions were observed.

Insert 1

~~Subsequently, the Eagle 21 system replaced the Hagan protection system within the existing racks. The Eagle 21 system has been seismically qualified on a generic basis by Westinghouse (see References 40 through 42) in accordance with requirements from References 43 and 44. A site-specific seismic analysis was also performed to ensure that the Eagle 21 generic testing performed by Westinghouse encompasses the DCPP installed condition (see Reference 45), which included the effects of the top entry conduit stiffness.~~

3.10.2.1.4 Instrument AC Inverters

A prototype UPS and regulating transformer of the DCPP UPS system was tested as described in PG&E engineering seismic file No. ES-68-1.

The UPS and regulating transformer were tested while loaded at 20 kVA; and the ac output voltage, current and frequency were monitored during the seismic test. The presence of a continuous ac output voltage both during and after the test formed the basis for determining the functional integrity of the UPS system.

During seismic testing the static inverter maintained structural integrity and functional operability. No variation or loss of 120 Vac output voltage was observed during or after the test. Therefore, the static inverter will perform its safety related functions during and after the postulated DCPP seismic events.

3.10.2.1.5 Pressure and Differential Pressure Transmitters (Westinghouse)

Originally the safety related pressure transmitters provided by Westinghouse for DCPP were installed to sense the following conditions:

36. Seismic Qualification Test Report of Class IE RTD and Thermocouple Temperature Sensors for Conax Corp., Report No. IPS-1165, Rev. A, June 18, 1984.

37. Rosemount Report D8400102, Qualification Report for Pressure Transmitter Model 1154, (PG&E DC 6000784-117).

38. Rosemount Report D8300040, Qualification Report for Pressure Transmitters Rosemount Model 1153 Series D, (PG&E DC 6000784-7-1).

39. PG&E Seismic Calculation No. IS-35, “Seismic Qualification of Rosemount Transmitters.”

Insert 2

40. ~~Equipment Qualification Test Report, Eagle 21 Process Protection System (Environmental and Seismic Testing), WCAP-8687, Supplement 2-E69A, Revision 0, May 1988.~~

41. ~~Equipment Qualification Test Report, Eagle 21 Process Protection System (Environmental and Seismic Testing), WCAP-8687, Supplement 2-E69B, Revision 0, February 1990.~~

42. ~~Equipment Qualification Test Report, Eagle 21 Process Protection System (Environmental and Seismic Testing), WCAP-8687, Supplement 2-E69C, Revision 0, February 1991.~~Not used.

43. Seismic Qualification of Electrical Equipment for Nuclear Power Plants, NRC Regulatory Guide 1.100, Revision 2, June 1988.

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

45. ~~Seismic Conformation of Eagle 21 Digital Process Protection System Upgrade for Pacific Gas and Electric Company Diablo Canyon Power Plant Units 1 and 2, WCAP-13384, Revision 0, PG&E, September 1992.~~Not used.

46. PG&E Specification 1021-J-NPG, “Specification for Furnishing and Delivering Remote Multiplexer and Visual Annunciator Equipment Associated with the Main Annunciator Systems for Diablo Canyon Power Plant, Units 1 and 2.”

47. Trentec Test Report No. 8Q017.0, dated 11/98.

48. Altran Calculation No. 98250-C-001, Revision 0, dated May 1999.

49. PG&E Seismic Calculation No. ES-66, "Seismic Qualification of Westinghouse Supplied SSPS Cabinets."

Final Safety Analysis Report Inserts (FSAR Section 3.10)

FSAR Section 3.10

Insert 1, Section 3.10.2.1.3

Subsequently, the Process Protection System, comprised of the Invensys Operations Management Tricon subsystem and the CS Innovations Advanced Logic System subsystem, replaced the original Hagan protection system within the existing racks. The Process Protection System Tricon subsystem has been seismically qualified by Invensys Operations Management (see Reference 40) in accordance with requirements from Reference 44 that is endorsed by Reference 33. The Process Protection System Advanced Logic System subsystem has been seismically qualified by CS Innovations (see Reference 41) in accordance with requirements from Reference 44.

Insert 2, Section 3.10.3 References

Reference 40 Triconex Topical Report, Invensys Operations Management Document 7286-545-1, Revision 4, December 20, 2010.

Reference 41 Advanced Logic System Equipment Qualification Results, CS Innovations Document 6002-00200.

CONTENTS (Continued)

(17) *Actuation Accuracy* - Synonymous with trip accuracy, but used where the word "trip" may cause ambiguity.

(18) *Indication Accuracy* - The tolerance band containing the highest expected value of the difference between: (a) the value of a process variable read on an indicator or recorder, and (b) the actual value of that process variable. An indication must fall within this tolerance band. It includes channel accuracy, accuracy of readout devices, and rack environmental effects but not process effects such as fluid stratification.

(19) *Reproducibility* - This term may be substituted for "accuracy" in the above definitions for those cases where a trip value or indicated value need not be referenced to an actual process variable value, but rather to a previously established trip or indication value; this value is determined by test.

7.1.1 IDENTIFICATION OF SAFETY-RELATED SYSTEMS

The instrumentation and control systems and supporting systems discussed in Chapter 7 that are required to function to achieve the system responses assumed in the safety evaluations, and those needed to shut down the plant safely are:

(1) Reactor trip system (RTS)

(2) Engineered safety features actuation system (ESFAS)

(3) Instrumentation and control power supply system

(4) Remote shutdown panel controls and instrumentation

The RTS and the ESFAS are functionally defined systems. The functional descriptions of these systems are provided in Sections 7.2 and 7.3. The trip functions identified in Section 7.2, Reactor Trip System, are provided by the following:

(1) Process instrumentation and ~~control~~ process protection system (PPS)(3, 9, 10, 11)

(2) Nuclear instrumentation system(4)

(3) Solid-state logic protection system (SSPS)(5)

(4) Reactor trip switchgear(5)

(5) Manual actuation circuitry

The actuation functions identified in Section 7.3 are provided by the following:

(1) Process instrumentation and ~~control system~~PPS(3, 9, 10, 11)

(2) SSPS~~olid-state logic protection system~~(5)

(3) Engineered safety features (ESF) test cabinet(6)

(4) Manual actuation circuitry

7.1.2 IDENTIFICATION OF SAFETY CRITERIA

7.1.2.1 Design Bases

The design bases and functional performance for the safety-related systems described in this chapter are provided in Sections 7.1.2.1.1 (RTS), 7.1.2.1.2 (ESFAS), and 7.1.2.1.3 (Instrumentation and Control Power Supply System).

7.1.2.1.1 Reactor Trip System

The RTS acts to limit the consequences of Condition II events (faults of moderate frequency such as loss of feedwater flow) by, at most, a shutdown of the reactor and turbine, with the plant capable of returning to operation after corrective action. The RTS features impose a limiting boundary region to plant operation that ensures that the reactor safety limits are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions.

7.1.2.1.1.1 Functional Performance Requirements

(1) *Reactor Trips* - The RTS automatically initiates reactor trip:

  (a) Whenever necessary to prevent fuel damage for an anticipated malfunction (Condition II)

  (b) To limit core damage for infrequent faults (Condition III)

  (c) So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting faults (Condition IV)

(2) *Turbine Trips* - The RTS initiates a turbine trip signal whenever reactor trip is initiated, to prevent the reactivity insertion that would otherwise result from excessive reactor system cooldown, and to avoid unnecessary actuation of the ESFAS.

7.1.2.1.3.3 Quality Assurance Requirements

A description of the quality assurance program applied to safety-related instrumentation and control system equipment is in Chapter 17.

7.1.2.2 Independence of Redundant Safety-Related Systems

Separation and independence for individual channels of the RTS and ESFAS are discussed in Sections 7.2 and 7.3, respectively. Separation of protection and control systems is discussed in Section 7.7. See Section 8.3 for a discussion of separation and independence of safety-related electrical systems.
For separation requirements for control board wiring, see Section 7.7.

Separation criteria for circuits entering the containment structure are met by providing separate electrical penetrations as follows:

(1) *Reactor Protection Instrumentation* - Each of the ~~Eagle 21~~PPS protection sets (I, II, III, and IV) utilizes one or more penetrations dedicated to that protection set. |

(2) *Isolation Valves (solenoid-operated)* - Each isolation valve inside the containment structure is connected to its respective ESF dc bus, and circuits are run through associated 480 V bus penetrations. All isolation valves inside the containment structure receive train A signals. Redundant isolation valves outside the containment receive train B signals.

(3) *Isolation Valves (motor-operated)* - Each isolation valve utilizes a penetration dedicated to the 480 V ESF bus that provides power to the valve.

(4) *Fan Coolers* - One penetration for each fan cooler motor.

(5) *Nuclear Instrumentation (out-of-core)* - Four separate penetrations are provided for out-of-core nuclear instrumentation.

The installation of other cable complies with the criteria presented in Chapter 8.

7.1.2.3 Physical Identification of Safety-Related Equipment

There are four separate process protection system rack sets. Separation of redundant process channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks to the redundant trains in the protection logic racks. Redundant process channels are separated by locating the electronics in different rack sets. A color-coded nameplate on each rack is used to differentiate between different protective sets. The color coding of the nameplates is:

Protection Set	Color Coding
I	Red with white lettering
II	White with black lettering
III	Blue with white lettering
IV	Yellow with black lettering

Each field wire termination point is tagged to assist identification. However, these tags are not color-coded.

All nonrack-mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on the enclosure that houses them.

Postaccident monitoring instruments and controls are identified "PAMS" as required by RG 1.97.

For further details of the process protection system, see Sections 7.2, 7.3, and 7.7.

There are identification nameplates on the input panels of the logic system. For details of the logic system, see Sections 7.2 and 7.3.

7.1.2.4 Conformance with IEEE Standards

The safety-related control and instrumentation systems comply with the following IEEE standards, only as discussed in the appropriate sections. However, because the IEEE standards were issued after much of the design and testing had been completed, the equipment documentation may not meet the format requirements of the standards.

(1) IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

(2) IEEE Standard 308-1971 or IEEE Standard 308-1980, "Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations."

(3) IEEE Standard 317, April 1971, "IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations."

(4) IEEE Standard 323, April 1971, "IEEE Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations."

(5) IEEE Standard 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

(6) IEEE Standard 334-1971, "Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations."

(7) IEEE Standard 336-1971, "Installation, Inspection, and Testing Requirements for Instrumentation and Electrical Equipment During the Construction of Nuclear Power Generating Stations."

(8) IEEE Standard 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems."

(9) IEEE Standard 344-1971, "Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations."

(10) IEEE Standard 344-1975, "Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."

(11) IEEE Standard 603-1980 or IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

7.1.2.5 Conformance with Other Applicable Documents

In addition to the conformance indicated in the preceding section, the safety-related systems in Chapter 7 comply with the following documents only as discussed in the appropriate sections.

(1) "Proposed General Design Criteria for Nuclear Power Plant Construction Permits," Federal Register, July 11, 1967.

(2) Safety Guide 6, "Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems," USAEC, March 1971.

(3) Safety Guide 22, "Periodic Testing of Protection System Actuation Functions," USAEC, February 1972.

(4) RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," USAEC, May 1973.

(5) RG 1.97, Rev. 3, "Instrumentation For Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," USNRC, May 1983.

(6) RG 1.152, “Criteria for Programmable Digital Computer System Software in Safety Related Systems in Nuclear Plants,” November 1985 (Regulatory Guide 1.152 endorses the guidance of ANSI/IEEE-ANS-7-4.3.2).

(7) Regulatory Guide 1.152, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”

~~(7)~~(8) RG 1.153, “Criteria for Power, Instrumentation and Control Portions of Safety Systems,” December 1985 (RG 1.153 endorses the guidance of IEEE Standard 603-1980).

~~(8)~~(9) ANSI/IEEE-ANS-7-4.3.2, “Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations,” 1982 (ANSI/IEEE-ANS-7-4.3.2, 1982 expands and amplifies the requirements of IEEE Standard 603-1980).

(10) IEEE Standard 7-4.3.2, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” 2003

7.1.3 REFERENCES

1. IEEE Standard, 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

2. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

3. J. A. Nay, Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, WCAP-07671, April 1971.

4. J. B. Lipchak and R. A. Stokes, Nuclear Instrumentation System, WCAP-7669, April 1971.

5. D. N. Katz, Solid State Logic Protection System Description, WCAP-7672, June 1971.

6. J. T. Haller, Engineered Safeguards Final Device or Activator Testing, WCAP-7705, February 1973.

7. IEEE Standard 308-1971, Criteria for Class 1E Electrical Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

8. T. W. T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, WCAP-7306, April 1969.

9. ~~L. E. Erin, Topical Report Eagle 21 Microprocessor-Based Process Protection System, WCAP-12374, September 1989 (W Proprietary Class 2).~~

Insert 1

Final Safety Analysis Report Inserts (FSAR Section 7.1)

FSAR Section 7.1

Insert 1, Section 7.1.3

Reference 9 Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Conceptual Design Document, Revision 4, 2011.

Reference 10 Triconex Topical Report, Invensys Operations Management Document 7286-545-1, Revision 4, December 20, 2010.

Reference 11 Advanced Logic System Topical Report, CS Innovations Document 6002-00301, Revision 2, November 10, 2011.

7.2 REACTOR TRIP SYSTEM

7.2.1 DESCRIPTION

This section provides a system description and the design bases for the reactor trip system (RTS).

7.2.1.1 System Description

The RTS uses sensors that feed the process protection system (PPS) process circuitry consisting of two to four redundant channels, which monitor various plant parameters. The RTS also contains the solid state protection system (SSPS) logic circuitry necessary to automatically open the reactor trip breakers. The logic circuitry consists of two redundant logic trains that receive input from the protection channels.

Each of the two trains, A and B, is capable of opening a separate and independent reactor trip breaker (52/RTA and 52/RTB). The two trip breakers in series connect three-phase ac power from the rod drive motor generator sets to the rod drive power bus, as shown in Figure 7.2-1, Sheet 2. For reactor trip, a loss of dc voltage to the undervoltage coil releases the trip plunger and trips open the breaker. Additionally, an undervoltage trip auxiliary relay provides a trip signal to the shunt trip coil that trips open the breaker in the unlikely event of an undervoltage coil malfunction. When either of the trip breakers opens, power is interrupted to the rod drive power supply, and the control rods fall by gravity into the core. The rods cannot be withdrawn until an operator resets the trip breakers. The trip breakers cannot be reset until the bistable, which initiated the trip, reenergizes. Bypass breakers BYA and BYB are provided to permit testing of the trip breakers, as discussed below.

7.2.1.1.1 Reactor Trips

The various reactor trip circuits automatically open the reactor trip breakers whenever a condition monitored by the RTS reaches a preset level. In addition to redundant channels and trains, the design approach provides an RTS that monitors numerous system variables, thereby providing RTS functional diversity. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is detailed in Reference 1.

Table 7.2-1 provides a list of reactor trips that are described below.

7.2.1.1.1.1 Nuclear Overpower Trips

The specific trip functions generated are:

(1) *Power Range High Nuclear Power Trip* - The power range high nuclear power trip circuit trips the reactor when two of the four power range channels exceed the trip setpoint.

There are two independent bistables each with its own trip setting (a high and a low setting). The high trip setting provides protection during normal power operation and is always active. The low trip setting, which provides protection during startup, can be manually blocked when two of the four power range channels read above approximately 10 percent power (P-10). Three of the four channels sensing below 10 percent power automatically reinstate the trip function. Refer to Table 7.2-2 for a listing of all protection system interlocks.

(2) *Intermediate Range High Neutron Flux Trip* - The intermediate range high neutron flux trip circuit trips the reactor when one of the two intermediate range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup, can be manually blocked if two of the four power range channels are above approximately 10 percent power (P-10). Three of the four power range channels below this value automatically reinstate the intermediate range high neutron flux trip. The intermediate range channels (including detectors) are separate from the power range channels. The intermediate range channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

(3) *Source Range High Neutron Flux Trip* - The source range high neutron flux trip circuit trips the reactor when one of the two source range channels exceeds the trip setpoint. This trip, which provides protection during reactor startup and plant shutdown, can be manually blocked when one of the two intermediate range channels reads above the P-6 setpoint value and is automatically reinstated when both intermediate range channels decrease below the P-6 value. This trip is also automatically bypassed by two-out-of-four logic from the power range interlock (P-10). This trip function can also be reinstated below P-10 by an administrative action requiring manual actuation of two control board-mounted switches. Each switch will reinstate the trip function in one of the two ~~protection~~SSPS logic trains. The source range trip point is set between the P-6 setpoint (source range cutoff flux level) and the maximum source range flux level. The channels can be individually bypassed at the nuclear instrumentation racks to permit channel testing during plant shutdown or prior to startup. This bypass action is annunciated on the control board.

(4) *Power Range High Positive Nuclear Power Rate Trip* - This circuit trips the reactor when an abnormal rate of increase in nuclear power occurs in two of the four power range channels. This trip provides protection against rod ejection and rod withdrawal accidents of low worth from middle to low power conditions and is always active.

the turbine and steam piping from excessive moisture carryover caused by high-high steam generator water level. Other turbine trips are discussed in Chapter 10.

The logic for this trip is shown in Figure 7.2-1, Sheets 2, 4, 10 and 16.

The analog portion of the trip shown in Figure 7.2-1, Sheet 16, is represented by dashed lines. When the turbine is tripped, turbine autostop oil pressure drops, and the pressure is sensed by three pressure sensors. A logic output is provided from each sensor when the oil pressure drops below a preset value. These three outputs are transmitted to two redundant two-out-of-three logic matrices, either of which trips the reactor if above P-9.

The autostop oil pressure signal also dumps the emergency trip fluid, closing all of the turbine steam stop valves. When all stop valves are closed, a reactor trip signal is initiated if the reactor is above P-9. This trip signal is generated by redundant (two each) limit switches on the stop valves.

7.2.1.1.1.7 Safety Injection Signal Actuation Trip

A reactor trip occurs when the safety injection system (SIS) is actuated. The means of actuating the SIS are described in Section 7.3. Figure 7.2-1, Sheet 8, shows the logic for this trip.

7.2.1.1.1.8 Manual Trip

The manual trip consists of two switches with four outputs on each switch. Each switch provides a trip signal for both trip breakers and both bypass breakers. (Operating a manual trip switch also removes the voltage from the undervoltage trip coil.)
There are no interlocks that can block this trip. Figure 7.2-1, Sheet 3, shows the manual trip logic.

7.2.1.1.1.9 Seismic Trip

The seismic trip system operates to shut down reactor operations should ground accelerations exceed a preset level in any two of the three orthogonal directions monitored (one vertical, two horizontal). The preset level is indicated in the Technical Specifications (Reference 4).

Three triaxial sensors (accelerometers) are anchored to the containment base in three separate locations 120 degrees apart (Figure 7.2-6). Each senses acceleration in three mutually orthogonal directions. Output signals are generated when ground accelerations exceed the preset level. These signals, lasting from 6 to 20 seconds (adjustable), are transmitted to the Trains A and B ~~solid state protection system (~~SSPS~~)~~. If two of the three sensors in any direction produce simultaneous outputs, the logic produces trains A and B reactor trip signals. The PPS channels are designed so that upon loss of electrical power to any channel, the output of that channel is a trip signal. The seismic trip channels are an exception to the fail-safe design. Since no credit is taken in accident analyses for the seismic trip, the seismic trip channels are designed energize-to-actuate to eliminate the possibility of spurious trips.

7.2.1.1.1.10 Automatic Trip Logic

The general alarm system, described in Reference 5, maintains a check on each train of the ~~solid-state logic protection system~~SSPS for the existence of certain undesirable conditions. Both trains are tripped if an abnormal condition occurs simultaneously in both trains. Reference 5 states that SSPS printed circuit boards (PCBs) use Motorola High Threshold Logic (MHTL). MHTL based PCBs are obsolete and are being replaced with PCBs which are not based on MHTL (reference 33). The replacement universal logic, safeguards driver, or under voltage driver PCBs have diagnostic features that can activate a general warning alarm when there is a critical board problem.

7.2.1.1.1.11 Reactor Trip Breakers

The reactor trip breakers are equipped for automatic actuation of both the undervoltage trip device and the shunt trip device. The reactor trip breakers are also equipped to permit manual trip of the breakers at the switchgear cabinet.

7.2.1.1.2 Reactor Trip System Interlocks

7.2.1.1.2.1 Power Escalation Permissives

The overpower protection provided by the out-of-core nuclear instrumentation consists of three discrete, but overlapping, levels. Continuation of startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

A one-out-of-two intermediate range permissive signal (P-6) is required prior to source range level trip blocking and detector high voltage cutoff. Source range level trips are automatically reactivated and high voltage restored when both intermediate range channels are below the permissive (P-6) levels. There is a manual reset switch for administratively reactivating the source range level trip and detector high voltage when between the permissive P-6 and P-10 level, if required. Source range level trip block and high voltage cutoff are always maintained when above the permissive P-10 level.

The intermediate range level trip and power range (low setpoint) trip can be blocked only after satisfactory operation and permissive information are obtained from two-out-of-four power range channels. Individual blocking switches are provided so that the low range power range trip and intermediate range trip can be independently blocked. These trips are automatically reactivated when any three of the four power range channels are below the permissive (P-10) level, thus ensuring automatic activation to more restrictive trip protection.

The development of permissives P-6 and P-10 is shown in Figure 7.2-1, Sheet 4. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

See Table 7.2-2 for the list of protection system interlocks.

7.2.1.1.2.2 Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip at low power (below approximately 10 percent of full power) on a low reactor coolant flow or reactor coolant pump open breaker signal in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, and pressurizer high water level on both units. See Figure 7.2-1, Sheets 5 and 6 for permissive applications. The low power signal is derived from three-out-of-four power range neutron flux signals below the setpoint in coincidence with one-out-of-two turbine impulse chamber pressure signals below the setpoint (low plant load). The P-8 interlock blocks a reactor trip when the plant is below a preset level specified in the Technical Specifications on a low reactor coolant flow in any one loop. The block action (absence of the P-8 interlock signal) occurs when three-out-of-four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor is allowed to operate with one inactive loop, and trip will not occur until two loops are indicating low flow. See Figure 7.2-1, Sheet 4, for derivation of P-8, and Sheet 5 for the applicable logic.

The P-9 interlock blocks a reactor trip below the maximum value of 50 percent of full power on a turbine trip signal. See Figure 7.2-1, Sheets 2, 4, and 16 for the application logic. The reactor trip on turbine trip is actuated by two-out-of-three logic from emergency trip fluid pressure signals or by all closed signals from the turbine steam stop valves.

See Table 7.2-2 for the list of protection system blocks.

7.2.1.1.3 Coolant Temperature Sensor Arrangement and Calculational Methodology

The individual narrow range cold and hot leg temperature signals required for input to the reactor trip circuits and interlocks are obtained using resistance temperature detectors (RTDs) installed in each reactor coolant loop.

Insert 1

The cold leg temperature measurement on each loop is accomplished with a dual element narrow-range RTD mounted in a thermowell. ~~The cold leg sensors are inherently redundant in that either sensor can adequately represent the cold leg temperature measurement.~~ Temperature streaming in the cold leg is not a concern due to the mixing action of the reactor coolant pump.

Insert 2

The hot leg temperature measurement on each loop is accomplished with three dual element narrow-range RTDs mounted in thermowells spaced 120 degrees apart around the circumference of the reactor coolant pipe for spatial variations. ~~One of the elements in each thermowell is an installed spare.~~

Insert 3

~~These cold and hot leg narrow-range RTD signals are input to the protection system digital electronics and processed as follows:~~

~~The two filtered cold leg temperature input signals $T^f c_j$ for each loop i are processed to determine a group average value $T^f cave_i$. The 2-input redundant sensor algorithm (RSA) calculates the group average value based on the number of good input signals.~~

~~If both input signals are BAD, the group value is set equal to the average of the two bad sensor values. If one signal is BAD and the other is DISABLED, the group value is set equal to the value of the bad sensor. The group quality is set to BAD in either case.~~

~~If one of the input signals is BAD and the other is GOOD, the group value is set equal to the GOOD value. A consistency check is not performed. The group quality is set to POOR.~~

~~If neither of the input signals is BAD, a consistency check is performed. If the deviation of these two signals is within an acceptance tolerance (±DELTAC), the group quality is set to GOOD and the group value is set equal to the average of the two inputs. If the difference exceeds ±DELTAC, the group quality is set to BAD, and the individual signal qualities are set to POOR. The group value is set equal to the average of the two inputs.~~

~~DELTAC is a fixed input parameter based on operating experience. One DELTAC value is required for each protection set.~~

~~Estimates of hot leg temperature are derived from each T_{hot} input signal as follows:~~

~~$\overline{T}_{hestij} = T^f_{hij} - P_{B_iS^o_{ij}}$ (7.2-4)~~

~~where:~~

~~T^f_{hij} is the filtered T_{hot} signal for the jth RTD (j = 1 to 3) in the ith loop (i = 1 to 4)~~

~~P_{B_i} = power fraction being used to correct the bias value being used for any power level~~

~~$P_{B_i} = \left(T^f_{have_i} - T^f_{cave_i}\right) / \Delta T^\circ_i$ (7.2-5)~~

~~where:~~

~~ΔT^o_i is the full power ΔT in the ith loop~~

~~S_{ij}^{o} = manually input bias that corrects the individual T_{hot} RTD value to the loop average.~~

~~The three hot leg temperature estimates $T_{hest_{ij}}$ for each loop i are processed to determine a group average value $T^{f}_{have_i}$. The 3-input RSA calculates the group value $T^{f}_{have_i}$ based on the available number of good input values.~~

~~If all three inputs are BAD, the group value is set to the average of the three input sensor values. The group value quality is set to BAD. If only one input is GOOD, the group value is set equal to the value of the good sensor. The group quality is set to BAD.~~

~~If two inputs are good, the difference between the two sensors is compared to DELTAH. If the inputs do not agree within ±DELTAH, the group quality is set to BAD and the quality of both inputs is set to POOR. If the inputs agree, the group quality is set to GOOD. The group value is set equal to the average of the two inputs in either case.~~

~~If all three inputs are good, an average of the three estimated hot leg temperatures is computed and the individual signals are checked to determine if they agree within ± DELTAH of the average value. If all of the signals agree within ± DELTAH of the average value, the group quality is set to GOOD. The group value ($T^{f}_{have_i}$) is set to the average of the three estimated average hot leg temperatures.~~

~~If the signal values do not all agree within ± DELTAH of the average, the RSA will delete the signal value that is furthest from the average. The quality of this signal will be set to POOR and a consistency check will then be performed on the remaining GOOD signals. If these signals pass the consistency check, the group value will be taken as the average of these GOOD signals and the group quality will be set to POOR. However, if these signals again fail the consistency check (within ± DELTAH), then the group value will be set to the average of these two signals; but the group quality will be set to BAD. All of the individual signals will have their quality set to POOR.~~

~~DELTAH is a fixed input parameter based upon temperature fluctuation within the hot leg. One DELTAH value is required for each protection set.~~

DELTA T and T Average are calculated as follows:

$$\Delta T_i = T^{f}_{have_i} - T^{f}_{cave_i} \qquad (7.2\text{-}4\cancel{6})$$

$$T_{avg_i} = (T^{f}_{have_i} + T^{f}_{cave_i})/2.0 \qquad (7.2\text{-}5\cancel{7})$$

Insert 4

~~The calculated values for DELTA T and T_{avg} are then utilized for both the remainder of the Overtemperature and Overpower DELTA T protection channel and channel outputs for control purposes.~~

~~A similar calculation of DELTA T is performed for and used by the steam generator low-low level trip time delay (TTD) function.~~

~~Alarms are generated from a group status that is based on the quality of T^{f}_{havei} and T^{f}_{cavei} out of the RSA. If the quality of either group is BAD and all of the inputs for that group are not offscale low, then the group status is set to TROUBLE and RTD FAILURE. If either quality is POOR and all of its inputs are not offscale low, then the group status is set to TROUBLE. Otherwise, the group status is set to GOOD.~~

7.2.1.1.4 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation includes a slight modification of the usual tank level arrangement using differential pressure between an upper and a lower tap. The modification shown in Figure 7.2-4 consists of the use of a sealed reference leg instead of the conventional open column of water. Refer to Section 7.2.2.3.4 for an analysis of this arrangement.

7.2.1.1.5 Process Protection System (PPS)

The process protection system is described in References 3, 34, 35, and 36.

Insert 5

7.2.1.1.6 Solid State (Digital) Logic Protection System (SSPS)

The ~~solid-state logic protection system~~SSPS takes binary inputs, (voltage/no voltage) from the PPS~~process~~ and nuclear instrument channels and direct inputs corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils of the reactor trip circuit breakers and an undervoltage auxiliary relay when the necessary combination of signals occurs. The undervoltage auxiliary relay sends a trip signal (125 Vdc) to the shunt trip coils of the reactor trip breakers. The system also provides annunciator, status light, and computer input signals that indicate the condition of bistable input signals, partial- and full-trip functions, and the status of the various blocking, permissive, and actuation functions. In addition, the system includes means for semiautomatic testing of the logic circuits. A detailed description of this system is provided in Reference 6. Reference 6 is based on SSPS printed circuit boards (PCBs) that use Motorola High Threshold Logic (MHTL). MHTL based PCBs are obsolete and are being replaced with PCBs which are not based on MHTL (reference 33).

7.2.1.1.7 Isolation Devices

In certain applications, it is advantageous to employ control signals provided~~derived~~ from individual protection channels through isolation devices contained in the protection channel, as permitted by IEEE-279 (Reference 7) and IEEE-603 (Reference 28).

In all of these cases, signals provided~~derived~~ from protection channels for nonprotective functions are obtained through isolation devices located in the process protection racks.

By definition, nonprotective functions include those signals used for control, remote process indication, and computer monitoring.

Isolation devices qualification type tests are described in References ~~8,~~ 9, 35, 36, and 52~~32~~.

7.2.1.1.8 Energy Supply and Environmental Qualification Requirements

The energy supply for the reactor trip system, including the voltage and frequency variations, is described in Section 7.6. The environmental qualification requirements are identified in Section 3.11.

7.2.1.1.9 Reactor Trip System Instrumentation Trip Setpoints

The functions that require trip action are identified in the Technical Specifications.

7.2.1.1.10 Seismic Design

The seismic design considerations for the RTS are discussed in Section 3.10. The design meets the requirements of Criterion 2 of the General Design Criteria (GDC) (Reference 10). A discussion of the seismic testing of the RTS equipment is presented in Section 3.10.

The monitoring circuitry, sensors and signal electronics, for several variables that provide inputs to the reactor trip system are not seismically qualified, and in some cases, are not seismically mounted or classified as Design Class I. Those circuits are:

(1) Source range (SR) nuclear instrumentation - sensors and electronics (Design Class I)

(2) Intermediate range (IR) nuclear instrumentation - sensors and electronics (Design Class I)

(3) Main turbine stop valve closed limit switches (Design Class II)

(4) Main turbine auto-stop oil pressure switches (Design Class II)

(5) 12 kV bus underfrequency relays, potential transformers and test switches (Design Class II)

(6) 12 kV bus undervoltage relays, potential transformers and test switches (Design Class II)

(7) 12 kV reactor coolant pump circuit breaker open position switches (Design Class II)

and breaker position switch monitoring circuits and the equipment in which they are mounted have been seismically analyzed to confirm that their structural integrity is such that no seismically induced common mode failures of the monitoring circuits or the equipment in which they are mounted exist that could degrade a primary RTS safety function.

7.2.1.2 Design Basis Information

The RTS meets IEEE criteria as set forth in IEEE-279 as described in Section 7.2.2.2.1.

Insert 6

The following are the generating station conditions requiring reactor trip (see Section 7.1.2):

(1) DNBR approaching the applicable limit value (see Section 4.4.1.1 and Section 4.4.2.3)

(2) Power density (kilowatts per foot) approaching rated value for Condition II faults (see Sections 4.2.1, 4.3.1, and 4.4.1 for fuel design limits)

(3) RCS overpressure creating stressing approaching the limits specified in Sections 5.2 and 5.5

The following are the variables required to be monitored in order to provide reactor trips (see Figure 7.2-1 and Table 7.2-1):

(1) Neutron flux

(2) Reactor coolant temperature

(3) RCS pressure (pressurizer pressure)

(4) Pressurizer water level

(5) Reactor coolant flow

(6) Reactor coolant pump operational status (bus voltage and frequency, and breaker position)

(7) Steam generator water level

(8) Turbine operational status (autostop oil pressure and stop valve position)

Reactor coolant temperature is a spatially dependent variable. (See Section 7.3.1 for discussion.)

demonstrated in Table 7.2-3, which lists the various trips of the RTS, the corresponding Technical Specifications on safety limits and safety system settings, and the appropriate accidents discussed in the safety analyses in which the trip could be utilized.

The RTS design, except the PPS, ~~-~~was evaluated in detail with respect to common mode failure and is presented in References 1 and 11. The evaluation for common mode failure in the PPS is presented in Reference 37 and was approved in References 38 and 53. The design meets the requirements of GDC 19, 22, and 23. Preoperational testing was performed on RTS components and systems to determine equipment readiness for startup. This testing served as a further evaluation of the system design.

Analyses of the results of Conditions I, II, III, and IV events, including considerations of instrumentation installed to mitigate their consequences, are presented in Chapter 15. The instrumentation installed to mitigate the consequences of load reduction and turbine trip is identified in Section 7.4.

With the installation of the RTD bypass elimination functional upgrade ~~as part of the Eagle 21 process protection system upgrade~~, the following plant operating concerns are addressed:

(1) The possibility of loss of flow or reduced flow through the common return line of the hot and cold RTD bypass manifold, as a result of transport time of the temperature measurements for the RTD loop, affecting the design basis for the overtemperature, overpower and control channels monitoring associated with the affected RTD bypass loop is eliminated.

(2) Operator indication of the loop Tavg, Tavg, and Delta-T deviation alarms is maintained, providing the operator the same detecting signals as with bypass loops.

Insert 7

(3) ~~The potential for a failed Thot RTD affecting the loop Tavg, Tavg, and ΔT measurements is reduced due to the algorithms provided in the Eagle 21 process protection system software that automatically detect a failed RTD and eliminate the failed RTDs measurement from affecting these plant parameters.~~

The seismic trip is provided to automatically shut down the reactor in the event of a seismic occurrence that causes the ground acceleration to exceed a preset level. No credit was taken for operation of the seismic trip in the safety analysis; however, its functional capability at the specified trip settings is required to enhance the overall reliability of the reactor protection system.

Checks and tests of these functional units will be made as required by the Technical Specifications.

7.2.2.2 Evaluation of Compliance with Applicable Codes and Standards

7.2.2.2.1 Evaluation of Compliance with IEEE-279

The RTS~~reactor trip system~~ meets the requirements of IEEE-279 as indicated below._ The PPS portion of the RTS is designed to meet the later IEEE-603 (Reference 28) and IEEE Standard 7-4.3.2 (Reference 31) standards. Evaluation of the PPS compliance with these standards is contained in Section 7.2.2.2.9.

7.2.2.2.1.1 Single Failure Criterion

The protection system is designed to provide two, three, or four instrumentation channels for each protective function and redundant (two) logic trains. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective action at the system level when required. This meets the requirements of Criterion 20 of the GDC. The PPS channels are designed so that upon loss of electrical power to any channel, the output of that channel is a trip signal (see Sections 7.2.1.1.1.4 and 7.2.1.1.1.9 for exceptions). This meets the requirements of GDC 26.

To prevent the occurrence of common mode failures, such additional measures as functional diversity, physical separation, testing, as well as administrative control during design, production, installation, and operation are employed, as discussed in Reference 11, for protection logic. Standard reliability engineering techniques were used to assess the likelihood of trip failure due to random component failures. Common mode failures were also qualitatively investigated. It was concluded from the evaluation that the likelihood of no trip following initiation of Condition II events is extremely small (2×10^{-7} derived for random component failures). The solid-state protection system design has been evaluated by the same methods as used for the relay system and the same order of magnitude of reliability is provided.

7.2.2.2.1.2 Quality of Components and Modules

For a discussion on the quality assurance program for the components and modules used in the RTS, refer to Chapter 17. The quality used meets the requirements of Criterion 1 of the GDC.

7.2.2.2.1.3 Equipment Qualification

For a discussion of the tests made to verify the performance requirements, refer to Section 3.11. The test results demonstrate that the design meets the requirements of GDC 23.

7.2.2.2.1.4 Independence

Each individual channel is assigned to one of four channel designations, e.g., Channel I, II, III, or IV. See Figure 7.2-5. Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant process equipment is separated by locating electronics in different protection rack sets. Each redundant channel is energized from a separate ac power feed. This meets the requirements of GDC 20.

~~*Position Regarding Separation of Isolated Signal Outputs within Process Protection Racks*~~

~~It is PG&E's position that specific physical separation is not required within the process protection racks between the protection circuits and isolated nonprotection circuits, and that the degree of electrical separation plus the physical separation associated with the insulation on the wires is sufficient to meet the requirements of IEEE-279.~~

~~The justification for this position is that IEEE-279 covers this situation in three paragraphs quoted below:~~

~~4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protective action at the system level when required.~~

~~4.6 Channel Independence. Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.~~

~~4.7.2 Isolated Devices. The transmission of signals from protection system equipment for control system use shall be through isolation devices, which shall be classified as part of the protection system and shall meet all the requirements of this document. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design base.~~

~~Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible ac and dc potential. A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the protection system.~~

~~The intent of 4.2 and 4.6 with regard to protection signals is handled through a combination of electrical and physical separation. The electrical separation is handled by supplying each protection rack set with separate independent sources of power.~~

~~Physical separation is provided by locating redundant channels in separate racks sets. Thus separation, both electrical and physical, outside the rack is ensured. The intent of 4.7.2 is met within the process protection racks by the provision of qualified isolators that have been tested and verified to perform properly under the credible failures listed in 4.7.2. The isolator is designed to be an electrical barrier between protection and nonprotection and, as such, the degree of physical separation provided within the modules is that which is consistent with the voltages involved.~~

~~The question of whether or not specific physical separation is required is best addressed by reviewing the potential hazards involved. There are three general categories of hazards that must be protected against. These are missiles, electrical faults, and fire. Missiles external to the rack can be ruled out on the basis that the racks are located in general plant areas where it is not credible to assume missiles capable of penetrating the steel rack. Missiles within the rack can be ruled out on the basis that there is no mechanism within the racks for the generation of missiles with sufficient energy to cause damage to the hardware or wiring.~~

~~Electrical faults within a rack constitute a single failure. Since there is no internal mechanism capable of simultaneously causing such a failure in more than one protection set, the result is acceptable. The plant remains safe with three out of the four protection sets remaining in operation. A few very specific electrical faults external to the protection racks on the signals derived from protection channels may have access to the outputs of all protection set simultaneously. However, the isolators have been shown to prevent these disturbances from entering the protection circuits; thus the results are acceptable.~~

~~Fire external to the racks is a potential hazard; however, fire retardant paint and wiring, fire barriers at the rack entrances, and adequate separation external to the racks provide a satisfactory defense against the hazard. For further discussions on fire protection, see Sections 8.3.1 and 9.5.1. A potential cause of fire within more than one protection set is an electrical fault involving the nonprotection outputs from these sets; however, it has been verified during the isolator tests that the fault current is terminated by the failure of certain components with no damage occurring in the wiring leading to the module. Thus, a fire within a rack set due to high current igniting or otherwise damaging the wiring is not possible.~~

~~The remaining source of fire within the racks - a short circuit within the protection wiring-effects only one protection set and thus is acceptable since three of the four protection sets remain.~~

~~It is thus established that no credible failure associated with the isolator output wiring violates the single failure criterion; therefore, the present method of rack wiring is entirely adequate.~~

7.2.2.2.1.5 Separation of Multiplexed, Isolated Solid-State Protection System Signals

Information from both SSPS logic trains is transmitted to the plant control boards and computer using a multiplex system. To ensure separation of the signals from each train, each signal is passed through an optically-coupled isolator. Verification tests on these isolators using voltages of 118 Vac and 250 Vdc are described in Reference 12.

To provide physical separation between input and output circuits in the solid-state protection system racks, physical barriers have been provided to separate input and output wire bundles. This meets the requirements of GDC 22 and 24. Independence of the SSPS logic trains is discussed in Reference 6. Two reactor trip breakers are actuated by two separate logic matrices that interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all control rod drive mechanisms, permitting the rods to free-fall into the core. The design philosophy is to make maximum use of a wide variety of measurements. The protection system continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in Reference 1. Generally, two or more diverse protection functions would terminate the accident conditions before intolerable consequences could occur. This meets the requirements of Criteria 21 and 23 of the GDC.

7.2.2.2.1.6 Control and Protection System Interaction

The protection system is designed to be independent of the control system. In certain applications, the control signals and other nonprotective functions are derived from individual protective channels through isolation devices. The isolation devices are classified as part of the protection system and are located in the process protection racks. Nonprotective functions include those signals used for control, remote process indication, and computer monitoring. The isolation devices are designed so that a short circuit, open circuit, or the application of 118 Vac or 140 Vdc on the isolated output portion of the circuit (i.e., the nonprotective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation devices are never returned to the protective racks. This meets the requirements of Criterion 22 of the GDC.

A detailed discussion of the design and testing of the isolation devices is provided in References ~~8,~~9, 35, 36, and 52~~32~~. These reports include the results of applying various malfunction conditions on the output portion of the isolation devices. The results show that no significant disturbance to the isolation devices input signal occurred. This meets the requirements of Criterion 31 of the GDC.

To provide additional assurance that the electrical wiring to and from the SSPS isolators, as installed, would not permit control-side faults to enter the protection system through input-output electrical coupling, tests were conducted at Diablo Canyon using voltages of

118 Vac, 250 Vdc, 460 Vac, 580 Vac and electrical noise. A description of these tests is provided in Reference~~s~~ ~~8,~~ 12~~, and 32~~.

Where failure of a protection system component can cause a process excursion that requires protective action, the protection system can withstand another independent failure without loss of protective action. This is normally achieved by means of two-out-of-four (2/4) trip logic for each of the protective functions except steam generator protection. The steam generator low-low water level protective function relies upon two-out-of-three (2/3) trip logic and a control system median signal selector (MSS). The use of a control system MSS prevents any protection system failure from causing a control system reaction resulting in a need for subsequent protective action. For details refer to Reference 27.

7.2.2.2.1.7 Capability for Testing

The RTS is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to ensure complete system operation. The ~~process protection~~PPS equipment is designed to permit any channel to be maintained in a bypassed condition and, when required, tested during power operation without initiating a protective action at the system level. This is accomplished without lifting electrical leads or installing temporary jumpers.

If a protection channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room.

The operability of the process sensors is ascertained by comparison with redundant channels monitoring the same process variables or those with a fixed known relationship to the parameter being checked. The in-containment process sensors can be calibrated during plant shutdown, if required.

Surveillance testing of the ~~process protection system~~PPS is performed with the use of a Tricon maintenance workstation (MWS) and ALS MWS dedicated to each Protection Set~~Man Machine Interface (MMI) test system~~. The MWS~~MMI~~ is used to enter instructions to the installed test processor in the ~~process protection~~PPS rack being tested which then generates the appropriate test signals to verify proper channel operation. The capability is provided to test in either partial trip mode or bypass mode where the channel comparators are maintained in the not-tripped state during the testing. Testing in bypass is allowed by the plant Technical Specifications. The bypass condition is continuously indicated in the control room via an annunciator.

The power range channels of the nuclear instrumentation system are tested by superimposing a test signal on the actual detector signal being received by the channel at the time of testing. The output of the bistable is not placed in a tripped condition prior to testing. Also, because the power range channel logic is two-out-of-four, bypass of this reactor trip function is not required. Note, however, that the source and intermediate-range high neutron flux trips must be bypassed during testing.

To test a power range channel, a TEST-OPERATE switch is provided to require deliberate operator action. Operation of the switch initiates the CHANNEL TEST annunciator in the control room. Bistable operation is tested by increasing the test signal level up to its trip setpoint and verifying bistable relay operation by control board annunciator and trip status lights.

It should be noted that a valid trip signal would cause the channel under test to trip at a lower actual reactor power level. A reactor trip would occur when a second bistable trips. No provision has been made in the channel test circuit for reducing the channel signal level below that signal being received from the nuclear instrumentation system detector. A nuclear instrumentation system channel that causes a reactor trip through one-out-of-two protection logic (source or intermediate range) is provided with a bypass function, which prevents the initiation of a reactor trip from that particular channel during the short period that it is undergoing testing. These bypasses initiate an alarm in the control room.

For a detailed description of the nuclear instrumentation system, see Reference 2.

The SSPS logic trains of the RTS are designed to be capable of complete testing at power, except for those trips listed in Section 7.2.3.2. Annunciation is provided in the control room to indicate when a train is in test, when a reactor trip is bypassed, and when a reactor trip breaker is bypassed. Details of the SSPS~~logic system~~ testing are provided in Reference 6.

The reactor coolant pump breakers cannot be tripped at power without causing a plant upset by loss of power to a coolant pump. However, the reactor coolant pump breaker trip logic and continuity through the shunt trip coil can be tested at power. Manual trip cannot be tested at power without causing a reactor trip, because operation of either manual trip switch actuates both trains A and B. Note, however, that manual trip could also be initiated from outside the control room by manually tripping one of the reactor trip breakers. Initiating safety injection cannot be done at power without upsetting normal plant operation. However, the logic for these trips is testable at power.

Testing of the SSPS logic trains of the RTS includes a check of the input relays and a logic matrix check. The following sequence is used to test the system:

(1) *Check of Input Relays* - During testing of the process instrumentation system and nuclear instrumentation system comparators, each channel comparator is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. The contact that creates the reactor trip also causes a status lamp and an annunciator on the control board to operate.

Either train A or B input relay operation lights the status lamp and sounds the annunciator.

Each train contains a multiplexing test switch. This switch is normally configured such that train A is in the A+B position, while train B is in the Normal position. Administrative controls are used to control this configuration and may be changed to other configurations as necessary to meet plant conditions. The A+B position alternately allows information to be transmitted from the two trains to the control board. A steady-status lamp and annunciator indicates that input relays in both trains have been deenergized. A flashing lamp means that both input relays in the two trains did not deenergize. Contact inputs to the logic protection system, such as reactor coolant pump bus underfrequency relays, operate input relays that are tested by operating the remote contacts as previously described and using the same indications as those provided for bistable input relays.

Actuation of the input relays provides the overlap between the testing of the SSPS~~logic protection system~~ and the testing of those systems supplying the inputs to the SSPS~~logic protection system~~. Test indications are status lamps and annunciators on the control board. Inputs to the SSPS~~logic protection system~~ are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two-out-of-four channels trip becomes a one-out-of-three trip when one channel is placed in the trip mode. Both trains of the SSPS~~logic protection system~~ remain in service during this portion of the test.

(2) *Check of Logic Matrices* - Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semiautomatic test panel in the train. Details of semiautomatic tester operation are provided in Reference 6. At the completion of the logic matrix tests, one bistable in each channel of process instrumentation or nuclear instrumentation is tripped or is verified in the tripped state to check closure of the input error inhibit switch contacts.

With the exception of the P-8 blocking function, the logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and nontrip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same points electrically that connect to the input relay contacts. Thus, there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature should not respond mechanically.

Because the P-8 block of the one of four RCS low flow trip is not connected to the semiautomatic tester, it is tested using the manual input function pushbuttons. The P-8 block function is verified using only one loop of RCS low flow on a staggered monthly frequency and all loops on a refueling frequency.

Test indications that are provided are an annunciator in the control room indicating that reactor trips from the train have been blocked and that the train is being tested, and green and red lamps on the semiautomatic tester to indicate a good or bad logic matrix test. Protection capability provided during this portion of the test is from the train not being tested.

The general design features and details of the testability of the SSPS~~logic system~~ are described in Reference 6. The testing capability meets the requirements of Criteria 19 and 25 of the GDC.

(3) *Testing of Reactor Trip Breakers* - Normally, reactor trip breakers 52/RTA and 52/RTB are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers, thereby eliminating the need to bypass them during the testing, although the associated bypass breaker is closed to preclude an inadvertent reactor trip and to allow reactor trip breaker testing. The following procedure describes the method used for testing the trip breakers:

(a) Bypass breaker 52/BYB is racked to test position and closed

(b) With bypass breaker 52/BYA racked out (test position), manually close and trip it to verify its operation

(c) Rack in and close 52/BYA (bypasses 52/RTA)

(d) While blocking 52/RTA shunt trip, manually trip 52/RTA and 52/BYB through a protection system logic matrix

(e) Reset 52/RTA

(f) Manually trip 52/RTA using the shunt trip coil only with the shunt trip test push button

(g) Reset 52/RTA

(h) Rack out 52/BYB

(i) Trip and rack out 52/BYA

(j) Repeat above steps to test trip breaker 52/RTB and bypass breaker 52/BYA using bypass breaker 52/BYB to bypass 52/RTB

Auxiliary contacts of the bypass breakers are connected so that if either train is placed in test while the bypass breaker of the other train is fully racked in and closed, both reactor trip breakers and the bypass breaker automatically trip.

Auxiliary contacts of the bypass breakers are also connected in such a way that if an attempt is made to fully rack in and close the bypass breaker in one train while the bypass breaker of the other train is already fully racked in and closed, both bypass breakers automatically trip. Additionally, trip signals will be sent to both reactor trip and bypass breakers through the ~~protection system~~SSPS logic.

The train A and train B alarm systems operate an annunciator in the control room. The two bypass breakers also operate an annunciator in the control room. Bypassing of a protection train with either the bypass or the test switches results in audible and visual indications.

The complete RTS is normally required to be in service. However, to permit on-line testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, a Technical Specification defining the minimum number of operable channels and the minimum degree of channel redundancy has been formulated. This Technical Specification also defines the required restriction to operation in the event that the channel operability and degree of redundancy requirements cannot be met.

The RTS is designed in such a way that some components' response time tests can only be performed during shutdown. However, the safety analyses utilize conservative numbers for trip channel response times. The measured channel response times are compared with those used in the safety evaluations. On the basis of startup tests conducted on several plants, the actual response times measured are less than the times used in the safety analyses.

(4) *Bypasses* - The ~~Eagle 21 process protection system~~PPS is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. Use of the bypass mode disables the individual channel comparator trip circuitry that forces the associated logic input relays to remain in the non-tripped state until the "bypass" is removed. If the ~~process protection~~PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room. During such operation, the ~~process protection system~~PPS continues to satisfy the

single failure criterion. This is acceptable since there are 4 channels and the two-out-of-four trip logic reduces to two-out-of-three during the test. For functions that use two-out-of-three logic, it is implicitly accepted that the single failure criterion is met because of the results of the system reliability study. From the results of this it was concluded that the ~~Eagle 21~~ digital PPS system availability is equivalent to the original~~respective~~ analog process PPS~~protection system~~ availability even without the incorporation of the redundancy, automatic surveillance testing, self calibration and self diagnostic features of the ~~Eagle 21~~digital PPS~~process protection system~~.

EXCEPTIONS:

(a) "One-out-of-two" functions are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated and bypass time interval is short.

(b) Containment spray actuation channels are tested by bypassing or negating the channel under test. This is acceptable since there are 4 channels and the two-out-of-four trip logic reduces to two-out-of-three during the test.

INTERLOCK CIRCUITS

A listing of the operating bypasses is included in Table 7.2-2. These bypasses meet the intent of the requirements of Paragraph 4.12 of IEEE-279.

Where operating requirements necessitate automatic or manual bypass* of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed in accordance with the criteria of this section. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service.

*Note: The term "bypass" is defined as the meeting of the coincident permissive (interlock) logic to permit the protective logic to become enabled/disabled as required. The term "bypass," in this section is not intended to be defined as the disabling of the individual channel comparator trip circuitry during routine test or surveillance that forces the associated logic input relays to remain in the non-tripped state until the "bypass" is removed.

(5) *Multiple Setpoints* - For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the protective system circuits are designed to provide positive means or administrative control to ensure that the more restrictive trip setpoint is used. The devices used to prevent improper use of less restrictive trip settings are considered part of the protective system and are designed in accordance with the criteria of this section.

(6) *Completion of Protective Action* - The RTS is so designed that, once initiated, a protective action goes to completion. Return to normal operation requires action by the operator.

(7) *Manual Initiation* - Switches are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment. Additionally, the reactor trip and bypass breakers can be operated locally.

(8) *Access* - The design provides for administrative control of access to all setpoint adjustments, module calibration adjustments, test points, and the means for bypassing channels or protective functions. ~~For details refer to Reference 23~~.

(9) *Information Readout* - The RTS provides the operator with complete information pertinent to system status and safety. All transmitted signals (flow, pressure, temperature, etc.) that cause a reactor trip are either indicated or recorded for every channel including all neutron flux power range currents (top detector, bottom detector, algebraic difference, and average of bottom and top detector currents).

Any reactor trip actuates an annunciator.

Annunciators are also used to alert the operator of deviations from normal operating conditions so that he may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel actuates an annunciator.

(10) *Identification* - The identification described in Section 7.1.2.3 provides immediate and unambiguous identification of the protection equipment.

7.2.2.2.2 Evaluation of Compliance with IEEE-308 (Reference 13)

See Section 7.6 and Chapter 8 for a discussion on the power supply for the RTS and compliance with IEEE-308 (Reference 13).

7.2.2.2.3 Evaluation of Compliance with IEEE-323

Refer to Section 3.11 for a discussion on Class I electrical equipment environmental qualification and compliance to IEEE-323 (Reference 14). Documentation of the Environmental and Seismic qualification of the RTS~~process protection system~~ is provided in References ~~23,~~ 24, 25, and 26, and for the PPS in References 35, 36, and 39.

7.2.2.2.4 Evaluation of Compliance with IEEE-334

There are no Class I motors in the RTS; therefore, IEEE-334 (Reference 15) does not apply.

7.2.2.2.5 Evaluation of Compliance with IEEE-338

The periodic testing of the RTS conforms to the requirements of IEEE-338 (Reference 16), with the exception that~~following comments:~~

~~(1)T~~the periodic test frequency is in accordance with ~~specified in~~ the Technical Specification~~s~~ Section 5.5.18 Surveillance Frequency Control Program~~was conservatively selected, using the considerations discussed in paragraph 4.3 of Reference 16, to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements.~~

~~The test interval discussed in Paragraph 5.2 of Reference 16 is developed primarily on past operating experience and modified, if necessary, to ensure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.~~

7.2.2.2.6 Evaluation of Compliance with IEEE-344

The seismic testing, as discussed in Section 3.10, conforms to IEEE-344 (Reference 17) except the format of the documentation may not meet the requirements because testing was completed prior to issuance of the standard. Documentation of the Environmental and Seismic qualification of the PPS~~process protection system~~ is provided in References ~~23,~~ 35, 36, and 39~~24, 25, and 26~~.

7.2.2.2.7 Evaluation of Compliance with IEEE-317

The electrical penetrations are designed and built in accordance with IEEE-317 (Reference 18) with the following exceptions:

(1) Prototype tests were not made with all of the physical conditions of the accident environment applied simultaneously with the electrical tests, although they were successfully made separately. For example, the momentary current tests on power penetrations are not run under simulated accident conditions. It is felt that such tests need not be made

simultaneously because the construction of the penetration assemblies is such that the outer seal is located about 4-1/2 feet away from the inner seal and the containment liner and, therefore, will not be exposed to accident environmental conditions. The integrity of the containment is, therefore, maintained at the penetration assemblies during a loss-of-coolant accident (LOCA).

(2) Dielectric strength tests were conducted in accordance with the National Electrical Manufacturers Association (NEMA) standard that permits testing of this type of equipment at 20 percent higher than twice-rated voltage plus 1000 V for 1 second.

(3) Wire and cable splice samples used at the containment penetrations were tested under conditions simulating a LOCA environment. Refer to Section 3.11 for a discussion on Class I electrical equipment environmental qualification.

7.2.2.2.8 Evaluation of Compliance with IEEE-336

Diablo Canyon is in conformance with IEEE-336 (Reference 19), with the following exceptions:

(1) Paragraph 2.4 - "Data sheets shall contain an evaluation of acceptability." The evaluation of acceptability is indicated on the results and data sheets by the approval signature.

(2) Paragraph 3(4) - "Visual examination of contact corrosion." No visual examination for contact corrosion is made on breaker and starter contacts unless there is evidence of water damage or condensation. Contact resistance tests are made on breakers rated at 4 kV and above. No contact resistance test is made of lower voltage breakers or starters.

(3) Paragraph 6.2.2 - "Demonstrate freedom from unwanted noise." No system test incorporates a noise measurement. If the system under test meets the test criteria, then noise is not a problem.

Insert 8

7.2.2.2.9 Evaluation of PPS Compliance with IEEE-603 and IEEE 7-4.3.2~~Eagle 21 Design, Verification and Validation Plan~~

~~The standards that are applicable to the Eagle 21 Design, Verification, and Validation Plan are IEEE Standard 603-1980 (Reference 28), Regulatory Guide 1.152~~

~~(Reference 29), Regulatory Guide 1.153 (Reference 30), and ANSI/IEEE-ANS-7-4.3.2 (Reference 31)~~.

7.2.2.2.10 Evaluation of Compliance with AEC General Design Criteria

The RTS meets the requirements of the GDC wherever appropriate. Specific cases are noted in this chapter.

7.2.2.3 Specific Control and Protection Interactions

7.2.2.3.1 Nuclear Power

Four power range nuclear power channels are provided for overpower protection. An additional control input signal is derived by auctioneering of the four channels for automatic rod control. If any channel fails producing a low output, that channel is incapable of proper overpower protection but does not cause control rod movement because of the auctioneer. Two-out-of-four overpower trip logic ensures an overpower trip, if needed, even with an independent failure in another channel.

In addition, a deviation signal gives an alarm if any nuclear power channel deviates significantly from any of the other channels. Also, the control system responds only to rapid changes in nuclear power; slow changes or drifts are compensated by the temperature control signals. Finally, an overpower signal from any nuclear power range channel will block manual and automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.2.3.2 Coolant Temperature

The accuracy of the RTD temperature measurements is demonstrated during plant startup tests by comparing temperature measurements from all RTDs with one another. The comparisons are done with the RCS in an isothermal condition. The linearity of the ΔT measurements obtained from the hot leg and cold leg RTDs as a function of plant power is also checked during plant startup tests.

The absolute value of ΔT versus plant power is not important as far as reactor protection is concerned. Reactor trip system setpoints are based on percentages of the indicated ΔT at nominal full power, rather than on absolute values of ΔT. For this reason, the linearity of the ΔT signals as a function of power is of importance rather than the absolute values of the ΔT. As part of the plant startup tests, the loop RTDs signals are compared with the core exit thermocouple signals. Note also that reactor control is based on signals derived from protection system channels after isolation by isolation devices so that no feedback effect can perturb the protection channels.

Because control is based on the average temperature of the loop having the highest average temperature, the control rods are always moved based on the most conservative temperature measurement with respect to margins to DNB. A spurious low

Periodic surveillance of the RTS is performed to ensure proper protective action. This surveillance consists of checks, calibrations, and functional testing that are summarized in the following sections.

7.2.3.1.1 Channel Checks

A channel check consists of a qualitative assessment of channel behavior during operation by observation. This determination shall include, where possible, comparison of the channel indication and/or status with other indications and/or status derived from independent instrument channels measuring the same parameters.

7.2.3.1.2 Channel Calibration

A channel calibration shall be the adjustment, as necessary, of the channel such that it responds within the required range and accuracy to known values of input. The channel calibration shall encompass the entire channel including the sensors and alarm, interlock and/or trip functions, and may be performed by any series of sequential, overlapping, or total channel steps such that the entire channel is calibrated.

7.2.3.1.3 Actuation Logic Test

An actuation logic test shall be the application of various simulated input combinations in conjunction with each possible interlock logic state and verification of the required logic output. The actuation logic test shall include a continuity check, as a minimum, of output devices.

7.2.3.1.4 Process Protection System Channel Operational Test

A channel operational test shall be the injection of a simulated signal into the channel as close to the sensor as practicable to verify operability of alarm, interlock, and/or trip functions. The channel operational test shall include adjustments, as necessary, of the alarm, interlock, and/or trip setpoints such that the setpoints are within the required range and accuracy.

7.2.3.1.5 Trip Actuating Device Operational Test

A trip actuating device operational test shall consist of operating the trip actuating device and verifying operability of alarm, interlock, and/or trip functions. The trip actuating device operational test shall include adjustment, as necessary, of the trip actuating device such that it actuates at the required setpoint within the required accuracy.

7.2.3.1.6 Reactor Trip System Response Time

The RTS response time shall be the time interval from when the monitored parameter exceeds its trip setpoint at the channel sensor until loss of stationary gripper coil voltage.

7.2.3.2 Compliance with Safety Guide 22

Periodic testing of the RTS actuation functions, as described, complies with AEC Safety Guide 22 (Reference 22). Under the present design, there are protection functions that are not tested at power. These are:

(1) Generation of a reactor trip by tripping the reactor coolant pump breakers

(2) Generation of a reactor trip by tripping the turbine

(3) Generation of a reactor trip by use of the manual trip switch

(4) Generation of a reactor trip by actuating the safety injection system

(5) Generation of a reactor trip by general warning circuitry (both redundant trains)

(6) Generation of a reactor trip by closing both reactor trip bypass breakers

The actuation logic for the functions listed is tested as described in Section 7.2.2. As required by Safety Guide 22, where equipment is not tested during reactor operation, it has been determined that:

(1) There is no practicable system design that would permit operation of the equipment without adversely affecting the safety or operability of the plant.

(2) The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, acceptably low without testing the equipment during reactor operation.

(3) The equipment can be routinely tested when the reactor is shut down.

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the main control room by a separate annunciator for the SSPS train in test. Test circuitry does not allow two SSPS trains to be tested at the same time so that extension of the bypass condition to redundant systems is prevented.

7.2.4 REFERENCES

1. T. W. T. Burnett, Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors, WCAP-7306, April 1969.

2. J. B. Lipchak, and R.A. Stokes, Nuclear Instrumentation System, WCAP-7669, April 1971.

3. J. A. Nay, Process Instrumentation for Westinghouse Nuclear Steam Supply Systems, WCAP-7671, April 1971.

4. Technical Specifications, Diablo Canyon Power Plant Units 1 and 2, Appendix A to License Nos. DPR-80 and DPR-82, as amended.

5. D. N. Katz, Solid State Logic Protection System Description, WCAP-7488L, January 1971.

6. D. N. Katz, Solid State Logic Protection System Description, WCAP-7672, June 1971.

7. IEEE Standard 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers.

Insert 9

8. ~~J. P. Doyle, Noise, Fault, Surge, and Radio Frequency Interference Test Report for Westinghouse Eagle 21 Process Protection Upgrade System, WCAP-11733, June 1988 (W Proprietary Class 2)~~.

9. R. Bartholomew and J. Lipchak, Test Report, Nuclear Instrumentation System Isolation Amplifier, WCAP-7819, Rev. 1, January 1972.

10. Proposed General Design Criteria for Nuclear Power Plant Construction Permits, Federal Register, July 11, 1967.

11. W. C. Gangloff, An Evaluation of Anticipated Operational Transients in Westinghouse Pressurized Water Reactors, WCAP-7486, May 1971.

12. D. N. Katz, et al., Westinghouse Protection Systems Noise Tests, WCAP-12358, Revision 2, October 1975 (W Proprietary Class 3).

13. IEEE Standard 308-1971, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 323-1971, Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 334-1971, Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems, The Institute of Electrical and Electronics Engineers Inc.

17. IEEE Standard 344-1971, Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

18. IEEE Standard 317-1971, Electric Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

19. IEEE Standard 336-1971, Installation, Inspection and Testing Requirements for Instrumentation and Electrical Equipment during the Construction of Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

20. Deleted in Revision 15.

21. IEEE Standard 344-1975, Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

22. Safety Guide 22, Periodic Testing of Protection System Actuation Functions, USAEC, February, 1972.

Insert 10

23. ~~L. E. Erin, Topical Report Eagle 21 Microprocessor Based Process Protection System, WCAP-12374, September 1989.~~

24. R. B. Miller, Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety-Related Electrical Equipment, WCAP-8587, W Proprietary Class 3.

25. Equipment Qualification Data Package, WCAP-8587, Supplement 1, EQDP-SE-9A and 69B, W Proprietary Class 3.

26. Equipment Qualification Test Report, WCAP-8687, Supplement 2-E69A and 69B, W Proprietary Class 2.

27. Advanced Digital Feedwater Control System Input Signal Validation for Pacific Gas and Electric Company Diablo Canyon Units 1 and 2, WCAP-12221 W Proprietary Class 3, April 1997 (PGE-97-540) and WCAP-12222 W Proprietary Class 3, March 1989.

28. IEEE Standard 603-1991~~1980~~, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

Insert 11

29. Regulatory Guide 1.152, Criteria for Use of ~~Programmable Digital~~ Computers ~~System Software~~ in Safety~~-Related~~ Systems ~~in~~of Nuclear Power Plants, Revision 3, July~~November~~ ~~1985~~2011.

30. ~~Regulatory Guide 1.153, Criteria for Power, Instrumentation and Control Portions of Safety Systems, December 1985.~~

31. ANSI/IEEE-ANS 7-4.3.2, ~~Application~~Standard Criteria for ~~Programmable~~ Digital Computers ~~Systems~~ in Safety Systems of Nuclear Power Generating Stations, 2003~~1982~~.

32. ~~C. N. Nasrallah, Noise, Fault, Surge, and Radio Frequency Interference Test Report - Westinghouse Eagle-21 Digital Family as Used in QDPS, PSMS, RVLIS, and ICCM, WCAP-11340, November 1986~~.

33. DCP 1000000354, Allow Replacement of SSPS Printed Circuit Boards, June 2010.

Insert 12

7.2.5 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

FSAR Section 7.2

Insert 1, Section 7.2.1.1.3

Both RTDs are averaged electronically using a two sensor quality algorithm (SQA2) to develop the cold leg average temperature for the loop.

Insert 2, Section 7.2.1.1.3

The RTDs in each thermowell are identified as "A" and "B." The three "A" RTDs and the three "B" RTDs are averaged electronically using three sensor quality algorithms (SQA3A and SQA3B) to develop the hot leg average temperature signal for the loop.

Insert 3, Section 7.2.1.1.3

The SQA algorithms are contained in Reference 51. The SQA algorithms determine the status of the input signals and, based on the determined status, define how to develop the cold leg and hot leg average temperature signals for use by the ΔT/Tave (DTTA) channels in the PPS. In addition to determining cold leg and hot leg average temperature signals, the SQA algorithms detail the requirements for alarming abnormal conditions through the use of the channel level "PPS Trouble" and "RTD Failure" alarms.

All hot let temperature input signals are adjusted by a compensation signal to account for temperature streaming effects present in the reactor coolant hot legs prior to being used by the SQA3A and SQA3B algorithms. The method for determining the appropriate streaming factors to apply to the hot leg temperature signals is detailed in Reference 51.

Insert 4, Section 7.2.1.1.3

The calculated values for ΔT and Tavg are used by the Overtemperature and Overpower ΔT protection functions and are output for use by the rod speed and direction control system.

The calculated ΔT signal is also used to provide the power signal for use in the Steam Generator Water Level Low-Low Level Trip Time Delay calculation discussed in Section 7.2.1.1.1.5.

Insert 5, Section 7.2.1.1.5

The PPS provides signals to the SSPS that will result in automatic shutdown the reactor when the limits of safe operation are approached. The safe operating region is defined by several considerations, such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. The PPS monitors plant parameters, compares them against setpoints, and provides binary inputs (voltage/no voltage) to the SSPS.

The PPS is comprised of four Protection Channel (Channel I, II, III, or IV) Sets (also referred to as "protection rack sets," "protection sets," or "protection racks"). Each protection channel set is further comprised of various process "channels". Each of the four PPS protection channel sets contains a microprocessor-based Tricon programmable logic controller subsystem (Reference 35) comprised of three separate legs and a field programmable gate array (FPGA) based Advanced Logic System (ALS) subsystem (Reference 36) comprised of an A core and a B core. The use of the PPS composed of the microprocessor-based Tricon subsystem and FPGA based ALS subsystem was approved by the NRC in License Amendment No. x/y (Reference 53).

The PPS Tricon subsystem is triple modular redundant (TMR) from input terminal to output terminal. The TMR architecture allows continued system operation in the presence of any single point of failure within the system. The Tricon subsystem contains power supply modules, input modules, main processor modules, communications modules, and output modules and each input and output module includes three separate and independent input or output circuits or legs. These legs communicate independently with the three main processor modules. Standard firmware is resident on the main processor modules for all three microprocessors as well as on the input, output, and communication modules. The PPS Tricon subsystem protection channel protection function can be performed by any of the three Tricon legs. The TMR architecture also allows the Tricon to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault within the TMR architecture, the Tricon self-diagnostics will alarm the condition, remove the affected portion of the faulted module from operation, and continues to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

The diverse ALS PPS subsystem utilizes FPGA hardware logic rather than a microprocessor and therefore has no software component required for operation of the system. The built-in diversity provided by the ALS A core and B core subsystems ensures that the PPS will perform the required PPS safety functions automatically in the presence of a postulated common cause software failure (References 37 and 38). The PPS ALS subsystem protection channel protection function can be performed by either the ALS A core or B core. At least one Tricon leg and one ALS core are required for a PPS protection set to perform all required protection functions required for that protection set. The ALS consists of a chassis containing core logic, input, and output cards and peripheral equipment consisting of cabinets, power supplies, control panels, and assembly panels. The ALS contains self-diagnostics capability to diagnose failures should they occur and self-test capability to support efficient surveillance testing.

The PPS meets the criteria in IEEE Standard 308-1980 (Reference 8), IEEE Standard 603-1991 (Reference 28), IEEE Standard 7-4.3.2-2003 Reference 31), and RG 1.152, Revision 3 (Reference 29).

The PPS replacement has been designed to meet NRC Digital Instrumentation and Controls Interim Staff Guidance 04, Revision 1 (Reference 23), except for Section 1, "Interdivisional Communications," Staff Position 10. The PPS replacement has been designed to an alternative justification for this position based on the combination of redundancy within the Tricon subsystem and both redundancy and diversity in the ALS subsystem, along with administrative controls.

The PPS Tricon programmable logic controller subsystem was qualified in accordance with EPRI TR-107330 (Reference 30), with exceptions and clarifications identified in Table 2-2 of Reference 35. Compliance of the PPS with IEEE Standard 308-1980 (endorsed by IEEE Standard 603-1991 Clause 8) and IEEE Standard 603-1991 is described in Section 7.2.2.2.9. Compliance of the PPS with IEEE Standard 7-4.3.2-2003 (endorsed by Regulatory Guide 1.152 (Reference 29) is contained in Section of 3.11 of Reference 47 for the Tricon subsystem and in Section 12.2 of Reference 36 for the ALS subsystem. Compliance of the PPS with RG 1.152, Revision 3, is contained in Reference 48 for the Tricon subsystem and in Section 12.6 of Reference 36 for the ALS subsystem. Compliance of the PPS with NRC Digital Instrumentation and Controls Interim Staff Guidance 04, Revision 1, is contained in Reference 49 for the Tricon subsystem and in Reference 50 for the ALS subsystem.

Insert 6, Section 7.2.1.2

The PPS portion of the RTS is designed to meet the latter IEEE Standard 603 (Reference 28) and IEEE Standard 7-4.3.2 (Reference 31) standards as described in Section 7.2.2.2.9.

Insert 7, Section 7.2.2.1.2

The potential for a failed Thot RTD affecting the loop Tavg, Tavg, and ΔT measurements is reduced by application of the SQA3A and SQA3B algorithms provided in the PPS software as discussed in Section 7.2.1.1.3 and detailed in Reference 51.

Insert 8, Section 7.2.2.2.9

The PPS portion of the RTS is designed to comply with IEEE Standard 603-1991 (Reference 28) and IEEE Standard 7-4.3.2-2003 Reference 31).

Compliance of the PPS with IEEE Standard 7-4.3.2-2003 (endorsed by Regulatory Guide 1.152 (Reference 29) is contained in Section of 3.11 of Reference 47 for the Tricon subsystem and in Section 12.2 of Reference 36 for the ALS subsystem.

IEEE Standard 603-1991 contains safety related system criteria in five clauses (Clauses 4, 5, 6, 7 and 8). The compliance of the PPS portion of RTS to these five clauses and their sub-clauses is described in the subsections below.

7.2.2.2.9.1 IEEE Standard 603-1991 Clause 4, Design Basis

IEEE Standard 603-1991, Clause 4.1, Identification of the Design Basis Events, includes criteria to identify the design basis events applicable to each mode of operation and the initial conditions and allowable limits of plant conditions for each such event. This information is contained in the FSAR Update Sections 7.2.1.2 and 15. The PPS diversity and defense-in-depth analysis (References 37 and 38) evaluated a common cause software failure in the PPS and determined the built-in diversity provided by the PPS ALS subsystem ensures that all accidents and events that credit automatic PPS mitigation in the FSAR Update Section 15 accident analyses are mitigated automatically by the PPS.

IEEE Standard 603-1991, Clause 4.2, Identification of Safety Functions and Protective Actions, includes criteria to identify the safety functions and corresponding protective actions of the execute features for each design basis event. FSAR Update Sections 7.2.1.1 and 7.2.1.2 identify the safety function and protective actions performed by the PPS portion of the RTS. The RTS reactor trips are listed in Table 7.2-1 and the RTS reactor trips credited by the FSAR Update Section 15 accident analyses are listed in Table 7.2-7.

IEEE Standard 603-1991, Clause 4.3, Permissive Conditions for Operating Bypasses, includes criteria to identify the permissive conditions for each operating bypass capability that is to be provided. The RTS permissives and associated functions are identified in Table 7.2-2 and are described in FSAR Update Sections 7.2.1.1.2.1 and 7.2.1.1.2.2.

IEEE Standard 603-1991, Clause 4.4, Variables monitored, includes criteria to identify the variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured. The variables monitored by the RTS, the criteria to identify the variables, and the ranges of the variables is contained in the FSAR Update Section 7.2.1.2. The analytical limit for the variables is identified in the FSAR Update Section 15. The rates of change of the RTS variables is identified in FSAR Update Sections 7.2.1.1.1.1 and 7.2.1.1.1.2.

IEEE Standard 603-1991, Clause 4.5, Minimum Criteria for Manual Protective Actions, includes criteria to identify the points in time and the plant conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed, and the variables that shall be displayed for the operator to use in taking manual action. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation. Manual initiation of the RTS is not required, however manual trip capability exists as described in Section 7.2.1.1.1.8.

IEEE Standard 603-1991, Clause 4.6, Identification of the Minimum Number and Location of Sensors, includes criteria for those variables that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes. The basis for the required number and location of RTS sensors is contained in References 1 and 3. The only variable sensed by the RTS that has special dependence is reactor coolant temperature and this is addressed by taking multiple samples from the reactor coolant system hot leg and averaging the sample temperatures in the PPS.

IEEE Standard 603-1991, Clause 4.7, Range of Transient and Steady-State Conditions, includes criteria to identify the range of transient and steady-state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the safety system shall perform. Section 3 of Reference 40 contains this information for the PPS. The environmental and seismic qualification of the PPS is provided in References in References 35, 36, and 39.

IEEE Standard 603-1991, Clause 4.8, Conditions Causing Functional Degradation, includes criteria to evaluate the conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems). These conditions are addressed for the RTS in Section 7.2.1.2.

IEEE Standard 603-1991, Clause 4.9, Methods Used to Determine Reliability, includes criteria to identify the methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design. The reliability of the RTS is addressed in Section 7.2.1.2. The reliability of the PPS Tricon subsystem is evaluated in Reference 44 and the reliability of the PPS ALS subsystem is evaluated in Reference 41.

IEEE Standard 603-1991, Clause 4.10, Critical Points in Time or Plant Conditions, includes criteria to identify the critical points in time or the plant conditions, after the onset of a design basis event, including the point in time or plant conditions for which the protective actions of the safety system shall be initiated, the point in time or plant conditions that define the proper completion of the safety function, the points in time or plant conditions that require automatic control of protective actions, and the point in time or plant conditions that allow returning a safety system to normal. This information is contained in Section 15.

IEEE Standard 603-1991, Clause 4.11, Equipment Protective Provisions, includes criteria to identify the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. There are no equipment protective provisions associated with the PPS that would prevent the safety systems from accomplishing their safety functions.

IEEE Standard 603-1991, Clause 4.12, Special Design Bases, includes criteria to identify any other special design basis that may be imposed on the system design (example: diversity, interlocks, and regulatory agency criteria). The PPS is a digital instrument and control system and therefore has been designed to meet the criteria of IEEE Standard 7-4.3.2-2003 (Reference 31), and RG 1.152, Revision 3 (Reference 29). The PPS has been designed to meet NRC Digital Instrumentation and Controls Interim Staff Guidance 04, Revision 1 (Reference 23), except for Section 1, "Interdivisional Communications," Staff Position 10 in which the PPS replacement has been designed to an alternative justification for this position based on the combination of redundancy within the Tricon subsystem and both redundancy and diversity in the ALS subsystem, along with administrative controls.

7.2.2.2.9.2 IEEE Standard 603-1991 Clause 5, System

IEEE Standard 603-1991, Clause 5.1, Single-Failure Criterion, includes criteria that the safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. The PPS is designed such that no single failure will impact the ability of the equipment to perform the safety function. Single failure for the PPS Tricon subsystem is addressed in Section 2.2.11 of Reference 35 and for the PPS ALS subsystem is addressed in Section 12.1.2 of Reference 36. The failure modes and effects analysis for the PPS Tricon subsystem is contained in Reference 42 and for the PPS ALS subsystem is contained in Reference 41.

IEEE Standard 603-1991, Clause 5.2, Completion of Protective Action, includes criteria that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. The PPS architecture is such that, once initiated, the protective action proceeds to completion. Interrupts are not used and return to normal operation requires deliberate operator action.

IEEE Standard 603-1991, Clause 5.3, Quality, includes criteria that the components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program. The PPS was designed, manufactured, and inspected in accordance with vendor QA programs. The PPS was installed and is tested, operated, and maintained in accordance with the Section 17 Quality Assurance Program and the PPS specific QA requirements in Reference 43.

IEEE Standard 603-1991, Clause 5.4, Equipment Qualification, includes criteria that safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. The equipment testing and analysis for the PPS Tricon subsystem is contained in Section 2 of Reference 35. The equipment testing and analysis for the PPS ALS subsystem is contained in Section 4 of Reference 36 and Reference 39.

IEEE Standard 603-1991, Cause 5.5, System Integrity, includes criteria that safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. The PPS has been designed and tested to confirm the equipment demonstrates system performance adequate to ensure completion of protective actions over the full range of applicable transient and steady-state plant conditions. The functional requirements for the PPS are contained in Reference 40. The PPS consists of four separate and isolated Protection Channels with adequate instrumentation to monitor the required reactor plant parameters and provide signals to the SSPS for use in determining when required protective actions are required.

IEEE Standard 603-1991, Clause 5.6, Independence

IEEE Standard 603-1991, Clause 5.6.1, Independence between Redundant Portions of a Safety System, includes criteria that redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish safety function during and following any design basis event requiring that safety function. The PPS consists of four independent Protection Channels. Each Protection Channel is physically separated and electrically isolated from the other sets. Each PPS Protection Channel is powered from a separate 120 V AC vital bus via a Class 1E uninterruptible power supply.

IEEE Standard 603-1991, Clause 5.6.2, Independence between Safety Systems and Effects of Design Basis Event, includes criteria that safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. The PPS consists of four independent Protection Channels. Each Protection Channel is physically separated and electrically isolated from the other sets. The functional requirements for the PPS considering effects of design basis events are contained in Reference 40. The equipment testing and analysis for the PPS Tricon subsystem is contained in Section 2 of Reference 35. The equipment testing and analysis for the PPS ALS subsystem is contained in Section 4 of Reference 36. There are no credible missiles that can penetrate the PPS cabinets containing the Tricon and ALS subsystem processing equipment. Protection of the PPS cabinets against external fire events is accomplished through use of fire retardant paint, fire retardant wiring, fire barriers, an area fire suppression system, and through physical separation of the PPS cabinets. IEEE Standard 603-1991, Clause 5.6.3, Independence between Safety Systems and Other Systems, includes criteria that safety system design shall be such that credible failures in and consequential actions by other systems, as documented in the design basis, shall not prevent the safety systems from meeting the requirements of this standard. Clause 5.6.3.1, Interconnected Equipment, (1) Classification, states equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems, isolation devices used to effect a safety system boundary shall be classified as part of the safety system. The PPS equipment used for both safety and non-safety functions is classified as part of the PPS.

Clause 5.6.3.1, (2) Isolation, includes criteria that no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system. The PPS consists of four independent Protection Channels to ensure that the PPS protection function can be performed with failure of one Protection Channel. The effect of failure of isolation devices is considered in the system level failure modes and effects analysis for the PPS contained in Reference 45. The PPS Tricon and ALS subsystem processing equipment is protected from high current in the interfacing non-safety systems.

Clause 5.6.3.2 Equipment in Proximity, (1) Separation, includes criteria that equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981. The PPS equipment is physically separated from equipment in other systems by locating the redundant PPS Protection Channels in separate cabinets. The requirement for physical separation is provided in Section 1.2 of Reference 40.

Clause 5.6.3.2, (2) Barriers, includes criteria that physical barriers used to effect a safety system boundary shall meet the requirements of Clauses 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4.7 and 4.8 of the design basis. The PPS isolation devices that provide an electrical barrier meet the requirements of IEEE Standard 603-1991, Clauses 5.3, 5.4 and 5.5 for the applicable conditions specified in IEEE Standard 603-1991 Clause 4.7 and 4.8 of the design basis. The isolation devices meet the functional requirements for the PPS contained in Reference 40.

Clause 5.6.3.3, Effects of a Single Random Failure, includes criteria that where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. The PPS consists of four independent Protection Channels that are physically separated and electrically isolated from each other. The functional requirements for the PPS considering effects of design basis events are contained in Reference 40.

Clause 5.7, Capability for Test and Calibration, includes criteria that capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. The PPS is capable of being tested online using the bypass capability of a channel while retaining the capability to perform the PPS safety function. Simulated signal inputs into a channel can be applied using measuring and test equipment. Indication of channel bypass status is indicated in the control room.

Clause 5.8, Information Displays, Clause 5.8.1, Displays for Manually Controlled Actions, includes criteria that the display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems. The PPS is designed to provide automatic initiation for all FSAR Update

Section 15 accidents and events that credit automatic PPS mitigation. Manual initiation of the RTS is not required, however manual trip capability exists as described in Section 7.2.1.1.1.8.

Clause 5.8.2 System Status Indication, includes criteria that display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The PPS includes display instrumentation that indicates and identifies protective actions of the sense and command features and execute features. A "postage stamp" indicator lamp on the panel illuminates to indicate that a Protection Channel has been activated.

Clause, 5.8.3 Indication of Bypasses, .includes criteria that if the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room. The PPS is designed such that if a Protection Channel has been bypassed for any purpose, a signal is automatically provided to allow this condition to be continuously indicated in the control room.

Clause 5.8.4, Location, includes criteria that informational displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions. The PPS display instrumentation that indicates and identifies protective actions of the sense and command features is located in the control room and is visible from the location of the controls.

Clause 5.9, Control of Access, includes criteria that the design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof. The PPS equipment is located in a controlled area secured by the plant security system in a manner that only allows authorized personnel access. This limits the means to bypass safety system functions, via access controls, to authorized plant personnel.

Clause 5.10, Repair, includes criteria that the safety systems shall be designed to facilitate timely recognition, location, replacement, repair and adjustment of malfunctioning equipment. The PPS is designed with system diagnostics and self-testing features to detect both hardware and software faults and to assist in diagnostic and repair activities. Most failures are detectable within each Protection Channel including the processors, I/O modules, power supplies and the communication features. The PPS equipment is contained in racks that allow removal and replacement of all cards and modules at power with the system on-line without adverse effect on the PPS safety function.

Clause 5.11, Identification, includes criteria that to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met; safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEEE Std 384-1981 and IEEE Std 420-1982; components for modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification; Identification of safety system equipment shall be distinguishable from identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables); identification of safety system equipment and its divisional assignment shall not require frequent use of reference material, and the associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974. For the PPS, a color coded nameplate on each rack is used to differentiate between different Protection Channels. All non-rack-mounted protective equipment and components are provided with an identification tag or nameplate. Additional details are contained in Section 7.1.2.3.

Clause, Clause 5.12, Auxiliary Features, includes criteria that auxiliary supporting features shall meet all requirements of the standard. Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. The PPS Tricon subsystem and PPS ALS subsystem are safety-related and do not contain auxiliary features that support performance of the automatic PPS safety function. The communication architecture provides the ability to transmit PPS information to the non-safety related PDN Gateway Computer. The PPS Tricon subsystem utilizes a port aggregator tap device to prevent communication from the PDN Gateway Computer to the Tricon subsystem. The PPS ALS subsystem utilizes a communication channel that is inherently one-way to the PDN Gateway Computer to prevent communication from the PDN Gateway Computer to the ALS subsystem.

Separate and independent non-safety-related MWSs are provided for the Tricon subsystem and ALS subsystems for each Protection Set to allow PPS information processing and display, and to facilitate testing, maintenance, and troubleshooting. The two MWSs in each Protection Set share common peripheral devices such as the keyboard, video display, mouse, touchscreen interface, and printer through a Keyboard-Video-Mouse switch. The Tricon MWS is dedicated to the Tricon PPS subsystem in the respective set and the ALS MWS is dedicated to the ALS PPS subsystem in that set. The two MWSs cannot communicate with each other nor can they communicate with the MWSs in redundant protection sets.

The PPS Tricon subsystem utilizes a fiber optic media connection between the Tricon subsystem and the Tricon communications module to provide electrical isolation. The PPS Tricon subsystem prevents communication from the Tricon MWS to the Tricon subsystem from affecting the safety function by preventing data input while a safety-related instrument-loop-specific out of service switch is determined to be open by the application software. Two-way communication from the Tricon MWS to the Tricon subsystem is only permitted when the safety-related instrument-loop-specific out of service switch is determined to be closed by the application software. The PPS ALS subsystem utilizes a communication channel that is inherently one-way to the ALS MWS. The PPS ALS subsystem also utilizes a test ALS bus communication channel that provides two-way communications between the ALS maintenance software in the ALS MWS and the ALS subsystem. The communication path between the ALS MWS and the ALS subsystem is normally disabled by physically disconnecting the communication link from the Test ALS Bus to the ALS MWS. Two-way communication is only permitted when the communication link is physically connected (enabled) between the TAB and the ALS MWS to allow surveillance testing, maintenance, and trouble-shooting.

Clause 5.13, Multi-Unit Stations, includes criteria that the sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. The PPS does not share any PPS components between the units.

Clause 5.14, Human Factors Considerations, includes criteria that human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988. Human factors are considered in the PPS design. The PPS uses devices located on the control room vertical boards and control console. To support operation, a human system interface located on the control room control console provides PPS system health and status displays via a connection to the Plant Data Network (PDN) Gateway Computer. To support maintenance and engineering, the ALS (MWS) and Tricon MWSs provide display of PPS functions. The PPS Tricon and ALS system cards and modules display the results of operation and self-diagnostic information.

Clause 5.15, Reliability, includes criteria for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. The PPS is designed to be highly reliable and exceeds the EPRI TR-107330 reliability goal of 99.0 percent reliability analysis as documented for the Tricon subsystem in Reference 44 and for the ALS subsystem in Reference 41.

7.2.2.2.9.3 Clause 6, Sense and Command Features

Clause 6.1, Automatic Control, includes criteria that means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5. The PPS performs sense and command functions by providing trip and actuation signals to the SSPS for use by the RTS, and ESFAS, which performs the execute functions. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation.

Clause 6.2, Manual Control, Clause 6.2.1, includes criteria that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1. Manual RTS capability is provided as described in Section 7.2.1.1.1.8. Means are provided in the control room for manual initiation of a reactor trip at the division level (SSPS Train "A" and Train "B") of the automatically initiated protective actions. These means are provided at the SSPS actuation level, downstream of the PPS, and are independent of any PPS hardware or software.

Clause 6.2.2, includes criteria that means shall be provided in the control room to implement manual initiation and control of the protective actions identified in Clause 4.5 that have not been selected for automatic control under Clause 6.1. The displays provided for these actions shall meet the requirements of Clause 5.8.1. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation.

Clause 6.2.3, includes criteria that means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action. The required PPS information and PPS devices is located on the control room vertical boards and control console and are accessible and suitable for the operator to maintain safe conditions after PPS protective actions are initiated.

Clause 6.3, Interaction with Other Systems, Clause 6.3.1 includes criteria that where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis, or equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Clause 6.3.2 includes criteria that provisions shall be included so that the requirements in Clause 6.3.1 can be met in conjunction with the requirements of Clause 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

The PPS diversity and defense-in-depth analysis (References 37 and 38) evaluated the capability of the RTS functions to be performed for FSAR Update Section 15 accidents and included evaluation of a common cause software failure in the PPS. PPS diversity and defense-in-depth analysis, determined the built-in diversity provided by the PPS ALS subsystem ensures that all accidents that credit automatic PPS mitigation in the FSAR Update Section 15 accident analyses are mitigated automatically by the PPS. FSAR Update Section 15 accident analyses include consideration of the impact of the accidents on the performance of non-safety systems. For other events such as earthquakes, fire, missiles, flood, and wind, the PPS components are protected from applicable events or sufficient component redundancy is available such that the PPS safety function can be performed. The failure modes and effects analysis for the PPS Tricon subsystem is contained in Reference 42, for the PPS ALS subsystem is contained in Reference 41, and for the PPS system is contained in Reference 45. The failure modes and effects analysis determined the PPS can perform the safety function considering a failure of a PPS Protection Channel. The failure of a PPS Protection Channel is equivalent to the effect of a PPS channel being placed in maintenance bypass.

The PPS is designed to minimize the possibility of occurrence of events that can potentially cause a non-safety system action that results in a condition requiring PPS protective action and concurrently prevents the PPS from providing protection for the event. Transmitter (sensor) inputs required by both the PPS and the control system are provided to the control system via qualified isolation devices (independent of the PPS) located on the transmitter input circuit. The analog signal for use by the control system is not processed by the PPS equipment and thus is not subject to PPS software common cause failure. RTD inputs to PPS channels are an exception. RTD inputs are conditioned (resistance to temperature) by the ALS and output to the Tricon as analog signals for processing by wide range temperature channels, pressurizer vapor temperature channel, and ΔT/Tavg channels. The ΔT/Tavg channels provide analog outputs to the rod speed and direction control system.

Clause 6.4, Derivation of System Inputs, includes criteria that to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. The process variables and derived parameters used for the PPS RTS actuation functions identified in FSAR Update Section 7.2.1.2 are derived from signals that are direct measures of the variables.

Clause 6.5, Capability for Testing and Calibration, Clause 6.5.1, contains criteria that means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation; and Clause 6.5.2 contains criteria that one of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period, checking the operational availability of sensors by use of the methods described in Clause 6.5.1; or specifying equipment that is stable and retains its calibration during the post-accident time period. The PPS incorporates self-testing diagnostic features as well as range checking on all sensor inputs. A trouble alarm is generated upon detection of an input failure or an out-of-range low or out-of-range high input condition at -5 percent (low) and 105 percent (high) of span. The PPS has the capability for channel checks using indications provided in the control room.

Clause 6.6, Operating Bypasses, includes criteria that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall accomplish one of the following actions, remove the appropriate active operating bypass(es), restore plant conditions so that permissive conditions once again exist, or initiate the appropriate safety function(s). FSAR Update Table 7.2-2 lists the operating bypasses for the RTS. Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions for the bypass are not satisfied. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed accordingly. The ability to initiate appropriate safety functions is available at all times. Indication is provided in the control room if some part of the protection system has been administratively bypassed or taken out of service.

Clause 6.7, Maintenance Bypass, includes criteria that capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of Clause 5.1 and Clause 6.3. An exception is one-out-of-two portions of the sense and command features are not required to meet Clause 5.1 and Clause 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated) that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability). FSAR Update Section 7.2.2.2.1.7 discusses testing in bypass and presents the normal method for removing channels for maintenance. The PPS is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. Use of the bypass mode disables the individual channel comparator trip circuitry that forces the associated logic input relays to remain in the non-tripped state until the bypass' is removed. If the PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room. The PPS system failure modes and effects analysis contained in Reference 45 assumes an initial condition that a PPS channel is placed in the bypass and determines the overall effect of an evaluated failure on the safety system's capability to perform the required safety functions in this configuration. The PPS system failure modes and effects analysis demonstrates the PPS has sufficient redundancy, independence and other required design fundamentals such that the safety function can be performed even with a channel in the bypass.

Clause 6.8, Setpoints, includes criteria that the allowance for uncertainties between the process analytical limit and the device setpoint shall be determined using a documented methodology, and that where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features. The calculations for the PPS setpoints are contained in Reference 46 and include allowance for uncertainties between the process analytical limit and the device setpoint. The PPS does not utilize multiple setpoints for any parameter in any one direction.

7.2.2.2.9.4 Clause 7, Execute Features

Clause 7.1, Automatic Control, includes criteria that capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4.4 of the design basis. The PPS performs sense and command functions by providing trip and actuation signals to the SSPS for use by the RTS. PPS protection outputs provide ON/OFF (partial trip) signals to the two trains of the SSPS whenever measured parameters indicate that safety limits are being approached (a pre-established setpoint is exceeded). The SSPS initiates a reactor trip when the requisite number of PPS channels have tripped (designed coincidence logic is satisfied). The execute features for the RTS are performed by the SSPS. The RTS, once initiated either automatically or manually, proceeds to completion because the mechanical action of the reactor trip circuit breakers require an external electrical reset command to reclose the breakers.

Clause 7.2, Manual Control, includes criteria that If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of Clause 5.1 and Clause 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation. Manual RTS capability is provided as described in Section 7.2.1.1.1.8. Means are provided in the control room for manual initiation at the division level (SSPS Train "A" and Train "B") of the automatically initiated protective actions Manual RT. These means are provided at the SSPS actuation level, downstream of the PPS, and are independent of any PPS hardware or software. The required PPS information and PPS devices is located on the control room vertical boards and control console.

Clause 7.3, Completion of Protective Action, includes criteria that the design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function. All PPS execute features are performed by the SSPS. The PPS monitors plant parameters and sends partial trip/actuation signals to the SSPS when predetermined setpoints are exceeded. The SSPS provides sealed-in reactor trip actuation signals when the coincidence logic for a particular trip/actuation function is satisfied. The SSPS does not require manual intervention or acknowledgement of actuation commands to complete a protective function. The SSPS reactor trip actuation signal requires manual action to reset following completion of the protective action and only after the PPS initiating signals have reset.

Clause 7.4, Operating Bypasses, includes requirements that whenever the applicable conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions; remove the appropriate active operating bypass(es), restore plant conditions so that permissive conditions once again exist, or initiate the appropriate safety function(s). The operating bypasses associated with the PPS are performed by the SSPS and are not performed by the PPS. The operating bypasses are automatically removed when plant conditions change to an operating mode in which protective actions are required to be operable so that a design basis event can be mitigated.

Clause 7.5, Maintenance Bypass, includes criteria that the capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability. FSAR Update Section 7.2.2.2.1.7 discusses testing in bypass and presents the normal method for removing channels for maintenance. Alternatively, for various PPS RTS functions, the Technical Specifications allow an inoperable channel and one additional channel to be surveillance tested with one channel in bypass and one channel in trip for up to 12 hours, or both the inoperable and the additional channel to be surveillance tested in bypass for up to 12 hours. During the period the PPS RTS functions are in the bypass configurations allowed by the Technical Specifications, the PPS is still capable to accomplish its safety function if a valid reactor trip signal occurs.

7.2.2.2.9.5 Clause 8, Power Source

Clause 8.1, Electrical Power Sources, provides criteria that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1980. The PPS portion of the protection system is designed to conform to IEEE-308-1980 (Reference 8). The PPS utilizes Class 1E power sources. Each PPS Protection Channel is powered from a separate 120 V AC vital bus via a Class 1E uninterruptible power supply. The Class 1E power sources are described in Section 8.1.1.4.

Clause 8.2, Non-Electrical Power Sources, includes criteria that non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. The PPS does not rely on non-electrical power sources for performance of its safety related functions.

Clause 8.3, Maintenance Bypass, includes criteria that the capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability. Each PPS Protection Channel is powered from a separate 120 V AC vital bus. If an external power source for a safety-related Protection Channel fails, the remaining safety-related Protection Channel will ensure that the safety system remains capable of performing the assigned safety function. Additional power source redundancy to assure reliability is provided within the Protection Channel. The Tricon subsystem chassis contains two redundant chassis power supplies that are qualified Class 1E power modules that are supplied from separate external power sources. Each ALS subsystem chassis contains two redundant chassis power supplies that are qualified Class 1E power supplies that are supplied from separate external power supplies. Each chassis power supply is capable of supplying full chassis load in the event of failure (or bypass) of the other power supply.

Insert 9, Section 7.2.4

Reference 8 IEEE Standard 308-1980, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

Insert 10, Section 7.2.4

Reference 23 NRC Digital Instrumentation and Controls Interim Staff Guidance, Digital I&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms - Communications Issues (HICRc), Revision 1," March 6, 2009.

Insert 11, Section 7.2.4

Reference 30 EPRI TR-107330, Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, 1997.

Insert 12, Section 7.2.4

Reference 34 J. W. Hefler, Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Conceptual Design Document, Revision 4, 2011, Altran Solutions.

Reference 35 Triconex Topical Report, Invensys Operations Management Document 7286-545-1-A, Revision 4, May 15, 2012.

Reference 36 Advanced Logic System Topical Report, CS Innovations Document 6002-00301, Revision 4, February, 2013.

Reference 37 S. B Patterson, Diablo Canyon Power Plant Process Protection System Replacement Diversity & Defense-in-Depth Assessment, Revision 1, August, 2010, PG&E Proprietary Report.

Reference 38 Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, "Process Protection System Replacement Diversity & Defense-In-Depth Assessment (TAC Nos. ME4094 and ME4095), US NRC, April 19, 2011.

Reference 39 ALS EQ Results, 6002-00200, CS Innovations proprietary.

Reference 40 Functional Requirement Specification, Process Protection System Replacement, MONTH YEAR.

Reference 41 Diablo Canyon ALS Reliability Analysis and Failure Mode and Effects Analysis, CS Innovations Document 6116-00029, Revision 1, April 2012.

Reference 42 Failure Modes and Effects Analysis, Invensys Operations Management Document 993754-1-811.

Reference 43 Process Protection System (PPS) Replacement System Quality Assurance Plan (SyQAP), Revision 1, March 2013.

Reference 44 Reliability Analysis, Invensys Operations Management Document 993754-1-819.

Reference 45 Process Protection System (PPS) Replacement System Level Failure Modes and Effects Analysis, Revision 0, 201x.

Reference 46 C. R. Tuley, et. al., Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant, WCAP-17706-P, Revision 0, January 2013, and Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System, WCAP 17696-P, Revision 0, January 2013.

Reference 47 Final Safety Evaluation For Invensys Operations Management "Triconex Topical Report", NRC Office of Nuclear Reactor Regulation, April 12, 2012.

Reference 48 Process Protection System Replacement Diablo Canyon Power Plant Regulatory Guide 1.152 Conformance Report, Invensys Operations Management Document 993754-1-913-P, Revision 0, September 2011.

Reference 49 Process Protection System Replacement Diablo Canyon Power Plant DI&C-ISG-04 Conformance Report, Invensys Operations Management Document No. 993754-1-912-P, Revision 0, September 2011.

Reference 50 Diablo Canyon PPS ISG04 Matrix, CS Innovations Document 6116-00054, Revision 0, November 2012.

Reference 51 Process Protection System Controller Transfer Functions Design Input Specification, PG&E Specification No. 10115-J-NPG, Revision 1, March 2011.

Reference 52 Dataforth Module Qualification Test Report, MONTH YEAR.

Reference 53 License Amendments No. x (Unit 1) and y (Unit 2), TITLE, dated DATE.

7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

7.3.1 DESCRIPTION

7.3.1.1 System Description

The engineered safety features actuation system (ESFAS) senses selected plant parameters and the process protection system (PPS) process circuitry determines whether or not predetermined safety limits are being exceeded. If so, signals are combined into logic matrices by the solid state protection system (SSPS) that are sensitive to combinations indicative of primary or secondary system boundary ruptures (Conditions III or IV faults). Once the required logic combination is completed, the SSPS~~system~~ sends actuation signals to those engineered safety features (ESF) components whose aggregate function best serves the requirements of the accident. This conforms to Criteria 12 and 15 of the General Design Criteria (GDC) (Reference 1). Included in this section are the electrical schematic diagrams for all ESF systems circuits and supporting systems. Figure 7.3-52 shows containment electrical penetrations, cable trays, and supports.

7.3.1.1.1 Functional Design

The following summarizes those generating station conditions requiring protective action:

(1) Primary system

(a) Rupture in small pipes or crack in large pipes

(b) Rupture of a reactor coolant pipe - loss-of-coolant accident (LOCA)

(c) Steam generator tube rupture

(2) Secondary system

(a) Minor secondary system pipe break resulting in steam release rates equivalent to the actuation of a single dump, relief, or safety valve

(b) Rupture of a major steam pipe

The following summarizes the generating station variables required to be monitored for each accident:

(1) Rupture in small pipes or crack in large primary system pipes

(a) Pressurizer pressure

(b) Pressurizer water level

(c) Containment pressure

(2) Rupture of a reactor coolant pipe LOCA

(a) Pressurizer pressure

(b) Pressurizer water level

(c) Containment pressure

(3) Steam generator tube rupture

(a) Pressurizer pressure

(b) Pressurizer water level

(4) Minor secondary system pipe break or major steam pipe rupture

(a) Pressurizer pressure

(b) Pressurizer water level

(c) Steam line pressures

(d) Steam line pressure rate

(e) Reactor coolant average temperature (Tavg)

(f) Containment pressure

7.3.1.1.2 Signal Computation

The ESFAS consists of two discrete portions of circuitry: (a) a PPS process ~~protection~~ portion consisting of three to four redundant channels that monitor various plant parameters such as the reactor coolant system (RCS) and steam system pressures, temperatures and flows, and containment pressures, and (b) a SSPS logic portion consisting of two redundant logic trains that receive inputs from the PPS~~process protection~~ channels and perform the needed logic to actuate the ESF. Each SSPS ~~logic~~ train is capable of actuating the ESF equipment required. The intent is that any single failure within the ESFAS shall not prevent system action when required.

The redundant concept is applied to the PPS process ~~protection~~ and SSPS logic portions of the system. Separation of redundant PPS~~process protection~~ channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and PPS~~process protection~~ racks, terminating at the redundant groups of ESF SSPS~~logic~~ racks as shown in Figure 7.3-50. This conforms to GDC 19.

Section 7.2 provides further details on protection instrumentation. The same design philosophy applies to both systems and conforms to GDC 19, 20, 22, and 23.

The variables are sensed by the PPS process ~~protection~~ circuitry, as discussed in Reference 2 and in Section 7.2. The outputs from the PPS~~process protection~~ channels are combined into actuation logic by the SSPS as shown on Sheets 5, 6, 7, and 8 of Figure 7.2-1. Tables 7.3-1 and 7.3-2 provide additional information pertaining to the SSPS logic and function.

The interlocks associated with the ESFAS are outlined in Table 7.3-3. These interlocks satisfy the functional requirements discussed in Section 7.1.2.

Manual controls are also provided to switch from the injection to the recirculation phase after a LOCA.

7.3.1.1.3 Devices Requiring Actuation

The following are the actions that the ESFAS initiates when performing its function:

(1) Safety injection

(2) Reactor trip

(3) Feedwater line isolation by closing all main control valves, feedwater bypass valves, feedwater pump trip, and closure of main feedwater isolation valves

(4) Auxiliary feedwater system actuation

(5) Auxiliary saltwater pump start

(6) Automatic containment spray

(7) Containment isolation

(8) Containment fan coolers start

(9) Emergency diesel generator startup

(10) Main steam line isolation

(11) Turbine and generator trips

(12) Control room isolation

(13) Component cooling water pump start

(14) Trip RHR pumps on low RWST level

7.3.1.1.4 Implementation of Functional Design

7.3.1.1.4.1 Process Protection System (PPS) Circuitry

The ~~process protection~~ PPS sensors and racks for the ESFAS are covered in References 2, 28, 29, and 30~~17~~. Discussed in these reports are the parameters to be measured including pressures, flows, tank and vessel water levels, and temperatures, as well as the measurement and signal transmission considerations. These latter considerations include the basic current transmission system, transmitters, orifices and flow elements, resistanc temperature detectors (RTDs), and pneumatics. Other considerations covered are automatic calculations, signal conditioning, and location and mounting of the devices.

Insert 1

The sensors monitoring the primary system are located as shown on the piping schematic diagram, Figure 3.2-7. The secondary system sensor locations are shown on the piping schematic diagram, Figure 3.2-4, Turbine Steam Supply System.

Containment pressure is sensed by four physically separated differential pressure transmitters mounted outside of the containment. The transmitters are connected to containment atmosphere by filled and sealed hydraulic transmission systems similar to the sealed pressurizer water level reference leg described in Section 7.2.2.3.4. This arrangement, with the pressure sensors external to the containment, forms a double barrier and conforms to Reference 1 and AEC Safety Guide 11 (Reference 3). See Section 6.2 for additional information on instrument lines penetrating containment.

Three water level instrumentation channels are provided for the refueling water storage tank (RWST). Each channel provides independent indication on the main control board, thus meeting the requirements of Paragraph 4.20 of IEEE-279 (Reference 4). Two-out-of-three logic is provided for residual heat removal (RHR) pump trip and low-level alarm initiation. One channel provides low-low-level alarm initiation; another channel provides a high-level alarm to alert the operator of overfill and potential spillage of radioactive material.

The following is a description of those process channels not included in the reactor trip system (RTS) or ESFAS that enable additional monitoring of in-containment conditions in the post-LOCA recovery period. These channels are located outside of the containment (with the exception of sump instrumentation).

(1) *High-head Safety Injection Pumps Discharge Pressure* - These channels show that the safety injection pumps are operating. The transmitters are outside the containment, with indicators on the control board.

(2) *Pump Energization* - Pump motor power feed breakers indicate that they have closed by energizing indicating lights on the control board.

(3) *Valve Position* - All ESF remotely operated valves have position indication on the control board in two places. Red and green indicator lights are

7.3.1.1.4.2 Solid State Protection System (SSPS) ~~Logic~~ Circuitry

The ESF SSPS~~logic~~ racks are discussed in detail in Reference 5. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference 5 also covers certain aspects of on-line test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separation, and provisions for ensuring instrument qualification. The outputs from the PPS~~process protection~~ channels are combined into actuation logic by the SSPS, as shown on Sheets 5 (T_{avg}), 6 (pressurizer pressure), 7 (steam pressure rate and steamline pressure), and 8 (engineered safety features actuation) of Figure 7.2-1.

To facilitate ESF actuation testing, two SSPS cabinets (one per train) are provided that enable operation, to the maximum practical extent, of safety features loads on a group-by-group basis until actuation of all devices has been checked. Final actuation testing is discussed in detail in Section 7.3.2.

7.3.1.1.4.3 Final Actuation Circuitry

The outputs of the ~~solid-state logic protection system~~SSPS (the slave relays) are energized to actuate, as are most final actuators and actuated devices. These devices are:

(1) *Safety Injection System Pumps and Valve Actuators* - See Section 6.3 for flow diagrams and additional information.

(2) *Containment Isolation* - Phase A - T signal isolates all nonessential (to reactor operation) process lines on receipt of safety injection signal; Phase B - P signal isolates remaining process lines (which do not include safety injection lines) on receipt of a two-out-of-four high-high containment pressure signal. For further information, see Section 6.2.4.

(3) *Containment Fan Coolers* - See Section 6.2.

(4) *Component Cooling Pumps and Valves* - See Section 9.2.2.

(5) *Auxiliary Saltwater Pumps* - See Section 9.2.7.

(6) *Auxiliary Feedwater Pumps Start* - See Section 6.5.

(7) *Diesel Generators Start* - See Section 8.3.

(8) *Feedwater Isolation* - See Section 10.4.

(9) *Ventilation Isolation Valve and Damper Actuators* - See Section 6.2.

(10) *Steam Line Isolation Valve Actuators* - See Section 10.3.

(g) Hot shutdown panel open
(h) Hot shutdown panel in control

(i) Heat tracing fault (boric acid systems)

(j) Radiation monitoring system failure

(k) Radiation monitoring system in test

(l) Diesel generator system

(m) NIS reactor trip bypass

(n) NIS rod stop bypass

(o) Containment high-high pressure in test

(p) Process protection system (PPS) channel in bypass

(q) PPS channel set failure

(r) PPS trouble

(s) PPS RTD failure

(t) Steam generator trip time delay timer actuated

In addition to the status lights and annunciator displays just described, system control switches on the control board are provided with indicating lights to display valve position and motor status with power potential indicating lights provided where equipment power is 480 V or higher.

The features described above, supplemented with administrative procedures, provide the operator with safety system status information, by means of which the status of bypassed or inoperable systems is available to the operator, in accordance with the intent of RG 1.47 (Reference 6).

7.3.1.2 Design Basis Information

The generating station conditions that require protective action are discussed in Section 7.3.1.1.1. The generating station variables that are required to be monitored in order to provide protective actions are also summarized in Section 7.3.1.1.1.

The only variable sensed by the ESFAS, which has spatial dependence, is reactor coolant temperature. The effect on the measurement is negated by taking multiple samples from the reactor coolant hot leg and electronically averaging these samples in the PPS~~process protection system~~.

Containment pressure	-5 to 55 psig

(b) The ranges required in generating the required actuation signals for steam break protection are:

Steam line pressure	0 to 1200 psig
Pressurizer pressure	1250 to 2500 psig
Containment pressure	-5 to 55 psig

7.3.1.3 Current System Drawings

The schematic diagrams and logic diagrams for ESF circuits and supporting systems are presented at the end of Chapter 7 (see Figures 7.3-1 through 7.3-49).

7.3.2 ANALYSIS

The minimum performance for each of the ESFAS components to be specified in terms of time response, accuracy, and range is in accordance with the requirements set forth in this document.

Insert 2

7.3.2.1 Evaluation of Compliance with IEEE-279

The ESFAS meets the criteria as set forth in IEEE-279, as indicated below.~~follows:~~

7.3.2.1.1 Single Failure Criteria

The discussion presented in Section 7.2.2 is applicable to the ESFAS, with the following exception:

In the ESF, a loss of instrument power to a specific channel/rack/or protection set will call for actuation of ESF equipment controlled by the specific channel that lost power (exceptions to the fail-safe design requirement are the containment spray and the radiation monitoring channels that initiate containment ventilation isolation). The actuated equipment in some cases must have power to comply. The power supply for the protection systems is discussed in Chapter 8. The containment spray function is energized to trip in order to avoid spurious actuation. In addition, manual containment spray requires simultaneous actuation of both manual controls. This is considered acceptable because spray actuation on high-high containment pressure signal provides automatic initiation of the system via protection channels, meeting the criteria in Reference 4. When the construction permits for the Diablo Canyon units were issued in April 1968 and December 1970, manual initiation at the system level was in compliance with paragraph 4.17 of IEEE-279 (Reference 8). No single random failure in the manual initiation circuits can prevent automatic initiation. Failure of manual initiation at the system level is not considered a significant safety problem because the operator can initiate operation manually at the component level.

The design conforms to GDC 21 and 26.

7.3.2.1.2 Equipment Qualification

The ability of the equipment inside the containment required to function for post-LOCA operation in the adverse environment associated with the LOCA or in-containment steam break, has been evaluated in Section 3.11.

Sensors for measurement of pressurizer pressure, pressurizer level, T_{avg}, and steam line flows are located inside the containment and will be exposed to the post-LOCA environment.

7.3.2.1.3 Channel Independence

The discussion presented in Section 7.2.2 is applicable. The ESF outputs from the ~~solid-state logic protection~~SSPS cabinets are redundant, and the actuations associated with each train are energized to actuate, up to and including the final actuators, by the separate ac power supplies that power the respective SSPS~~logic~~ trains. Mutually redundant ESF circuits utilize separate relays in separate racks.

7.3.2.1.4 Control and Protection System Interaction

The discussions presented in Section 7.2.2 are applicable.

7.3.2.1.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in Section 7.2.2 are applicable to the sensors, analog circuitry and SSPS~~logic~~ trains of the ESFAS.

The following discussions cover those areas in which the testing provisions differ from those for the RTS.

7.3.2.1.5.1 Testing of Engineered Safety Features Actuation System

The ESFAS is tested to ensure that the systems operate as designed and function properly in the unlikely event of an accident. The testing program, which conforms with Criteria 25, 38, 46, 48, and 57 of the GDC, and to the AEC Safety Guide 22 (Reference 9), is as follows:

(1) Prior to initial plant operations, ESFAS tests will be conducted.

(2) Subsequent to initial startup, ESFAS tests will be conducted as required in the Technical Specifications.

(3) During on-line operation of the reactor, the ESF PPS ~~process~~ and SSPS~~logic~~ circuitry are fully tested. In addition, essentially all of the engineered safety features final actuators can be fully tested. The few final actuators whose operation is not compatible with continued on-line plant

operation are checked during refueling outages. Slave relays are tested on an interval defined in the Technical Specifications.

(4) During normal operation, the operability of testable final actuation devices of the ESF actuation system are tested by manual initiation from the test control panel.

The discussions presented in Section 7.2.2.2.1.7 are applicable.

7.3.2.1.5.2 Performance Test Acceptability Standard for the "S" (Safety Injection Signal) and the "P" (Automatic Demand Signal for Containment Spray Actuation) Actuation Signals Generation

During reactor operation, the acceptability of the ESFAS is based on the successful completion of the overlapping tests performed on the initiating system and the ESFAS. Checks of process indications verify operability of the sensors. Process checks and tests verify the operability of the PPS process circuitry from the input of these circuits through the SSPS logic input relays and the inputs to the logic matrices. ~~Solid-state logic~~SSPS testing checks the signal path through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays. Final actuator testing can be performed by operating the output slave relays and verifying the required ESF actuation. Actuators whose testing is not compatible with on-line operation will be tested during refueling outages, except those actuators normally in their required positions, which will not be tested. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves have completed their travel.

The basis for acceptability for the ESF interlocks is receipt of proper indication upon introducing a trip.

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground of signal cables in radiation environments, are based on qualification test data that identify what constitutes acceptable degradation, e.g., radiation and thermal.

7.3.2.1.5.3 Frequency of Performance of Engineered Safety Features Actuation Tests

During reactor operation, complete system testing (excluding sensors or those devices whose operation would cause plant upset) is performed as required by the Technical Specifications. Testing, including the sensors, is also performed during scheduled plant shutdown for refueling.

7.3.2.1.5.4 Engineered Safety Features Actuation Test Description

The following sections describe the testing circuitry and procedures for the on-line portion of the testing program. The guidelines used in developing the circuitry and procedures are:

(1) The test procedures must not involve the potential for damage to any plant equipment.

(2) The test procedures must minimize the potential for accidental tripping.

(3) The provisions for on-line testing must minimize complication of ESF actuation circuits so that their reliability is not degraded.

7.3.2.1.5.5 Description of Initiation Circuitry

Several systems comprise the total ESFAS, the majority of which may be initiated by different process conditions and reset independently of each other.

The remaining functions (listed in Section 7.3.1) are initiated by a common signal (safety injection), which in turn may be generated by different process conditions.

In addition, operation of all other vital auxiliary support systems, such as auxiliary feedwater, component cooling water, and auxiliary saltwater, is initiated via the ESF starting sequence actuated by the safety injection signal.

Each function is actuated by a logic circuit that is duplicated for each of the two redundant trains of ESF initiation circuits.

The output of each of the initiation circuits consists of a master relay, which drives slave relays for contact multiplication as required. The logic, master, and slave relays are mounted in the ~~solid-state logic protection~~SSPS cabinets designated trains A and B, respectively, for the redundant counterparts. The master and slave relay circuits operate various pump and fan circuit breakers or starters, motor-operated valve contactors, solenoid-operated valves, emergency generator starting, etc.

7.3.2.1.5.6 PPS~~Process Protection~~ Testing

PPS~~Process protection~~ testing is identical to that used for reactor trip circuitry and is described in Section 7.2.3. Briefly, in the PPS~~process protection~~ racks, a dedicated Tricon maintenance workstation (MWS)~~man machine interface (MMI) unit~~ and ALS MWS that is provided to~~used together with a rack mounted test panel to~~ facilitate testing in each protection set.

Section 7.2.2.2.1.7 discusses testing in bypass which is the normal method. Alternatively, administrative control allows, during channel testing, that the channel output be put in a trip condition that de-energizes (operates) the input relays in train A and train B cabinets. Of necessity this is done on one channel at a time. Status lights and single channel trip alarms in the main control room verify that the SSPS logic input relays have been deenergized and the channel outputs are in the trip mode. An exception to this is containment spray, which is energized to actuate two-out-of-four logic and reverts to two-out-of-three logic when one channel is in test.

7.3.2.1.5.7 ~~Solid-State Logic~~SSPS Testing

After the individual ~~process~~PPS channel testing is complete, the SSPS logic matrices are tested from the trains A and B logic rack test panels. This step provides overlap between the PPS~~process protection~~ and logic portions of the test program. During this test, each of the logic inputs is actuated automatically in all combinations of trip and nontrip logic. Trip logic is not maintained long enough to permit master relay actuation - master relays are "pulsed" to check continuity. Following the logic testing, the individual master relays are actuated electrically to test their mechanical operation. Actuation of the master relays during this test applies low voltage to the slave relay coil circuits to allow continuity checking, but not slave relay actuation. During logic testing of one train, the other train can initiate the required ESF function. For additional details, see Reference 5.

7.3.2.1.5.8 Actuator Testing

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. Slave relays do not operate because of reduced voltage.

In the next step, operation of the slave relays and the devices controlled by their contacts can be checked. For this procedure, control switches mounted in the safeguards test cabinet (STC) near the SSPS~~logic~~ rack area are provided for most slave relays. These controls require two deliberate actions on the part of the operator to actuate a slave relay. By operation of these relays one at a time through the control switches, all devices that can be operated on-line without risk to the plant can be tested.

Devices are assigned to the slave relays to minimize undesired effects on plant operation. This procedure minimizes the possibility of upset to the plant and again ensures that overlap in the testing is continuous, since the normal power supply for the slave relays is utilized.

During this last procedure, close communication between the main control room operator and the person at the test panel is required. Before energizing a slave relay, the operator in the control room ensures that plant conditions will permit operation of the equipment that will be actuated by the relay. After the tester has energized the slave relay, the control room operator observes that all equipment has operated as indicated by appropriate indicating lamps, monitor lamps, and annunciators on the control board. The test director, using a prepared check list, records all operations. The operator then resets all devices and prepares for operation of the next slave relay-actuated equipment.

By means of the procedure outlined above, all devices actuated by ESFAS initiation circuits can be operated by the test circuitry during on-line operation, with the following exceptions:

(1) Main steam isolation - During cold shutdowns, these valves are full stroke tested.

(2) Feedwater isolation - Air-operated, spring-closed regulating control valves and feedwater bypass valves are provided for each main feedwater line. Operation of these valves is continually monitored by normal operation.

7.3.2.1.5.9 Actuator Blocking and Continuity Test Circuits

The limited number of components that cannot be operated on-line are assigned to slave relays separate from those assigned to components that can be operated on-line. For some of these components, additional blocking relays are provided that allow operation of the slave relays without actuation of the associated ESF devices. Interlocking prevents blocking the output of more than one slave relay at a time. The circuits provide for monitoring of the slave relay contacts, the devices control circuit cabling, control voltage, and the devices actuating solenoids. These slave relays and actuators may be tested using the blocking and continuity test circuits while the unit is on line; however, use of these circuits can increase the risk associated with testing, since failure of the blocking circuits may result in a reactor trip.

7.3.2.1.5.10 Time Required for Testing

The system design includes provisions for timely testing of both the PPS~~process protection~~ and SSPS~~logic~~ sections of the system. Testing of actuated components (including those which can only be partially tested) is a function of control room operator availability. It is expected to require several shifts to accomplish these tests. During this procedure, automatic actuation circuitry will override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time, the redundant devices in the other trains would be functional.

7.3.2.1.5.11 Safety Guide 22

Periodic testing of the ESF actuation functions, as described, complies with AEC Safety Guide 22. Under the present design, those protection functions that are not tested at power are listed in Section 7.3.2.1.5.9.

As required by Safety Guide 22, where actuated equipment is not tested during reactor operation, it has been determined that:

(1) There is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant.

(2) The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation.

(3) The actuated equipment can be routinely tested when the reactor is shut down.

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed, for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the control room by a common "ESF testing" annunciator for the train in test. Test circuitry does not allow two ESF trains to be tested at the same time so that extension of the bypass condition to redundant systems is prevented.

The discussion on "bypass" in Section 7.2.2.2.1.7 is applicable.

7.3.2.1.5.12 Summary

The testing program and procedures described provide capability for checking completely from the process signal to the SSPS~~logic~~ cabinets and from these to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc., including all field cabling actually used in the circuitry called upon to operate for an accident condition. For those devices whose operation could affect plant or equipment operation, the same procedure provides for checking from the process signal to the SSPS~~logic~~ rack. To check the final actuation device, the device itself is tested during shutdown conditions. All testing is performed as required by the Technical Specifications.

The procedures require testing at various locations:

(1) Process channel testing and verification of setpoints are accomplished at the PPS~~process protection~~ racks. Verification of SSPS logic input relay operation is done at the control room status lights.

(2) Logic testing through operation of the master relays and low voltage application to slave relays is done at the SSPS~~logic~~ rack test panel.

(3) Testing of pumps, fans, and valves is done at a test panel located in the vicinity of the SSPS~~logic~~ racks, in combination with the control room operator.

(4) Continuity testing for the circuits that cannot be operated is done at the same test panel mentioned in (3) above.

7.3.2.1.6 Testing During Shutdown

Emergency core cooling system (ECCS) components and the system, including emergency power supplies, will be tested in accordance with the Technical Specifications.

Containment spray system tests are performed at each major fuel reloading. The tests will be performed with the isolation valves in the spray supply lines at the containment and spray additive tank blocked closed, and are initiated manually or by using an actual or simulated actuation signal.

All final actuators can be tested during a refueling outage. The final actuators that cannot be tested during on-line operation are tested during each major fuel reloading. All testing is performed as required by the Technical Specifications.

7.3.2.1.7 Periodic Maintenance Inspections

Periodic maintenance on the system equipment is accomplished and documented according to the maintenance procedures contained in the Plant Manual.

The balance of the requirements listed in Reference 4 (Paragraphs 4.11 through 4.22) is discussed in Sections 7.2.2 and 7.2.3. Paragraph 4.20 receives special attention in Section 7.5.

7.3.2.2 Evaluation of Compliance with IEEE-308 (Reference 10)

The power supplies for the ESF equipment conform to IEEE 308 (Reference 10).

See Section 7.6 and Chapter 8, which discuss the power supply for the protection systems, for additional discussions on compliance with this criteria.

7.3.2.3 Evaluation of Compliance with IEEE-323 (Reference 11)

Refer to Section 3.11 for a discussion on ESF electrical equipment environmental qualification and compliance to IEEE-323 (Reference 11). Documentation of the Environmental and Seismic qualification of the ESFAS~~process protection system~~ is provided in References 18, 19, and 20, and ~~21~~ for the PPS in References 29, 30, and 33.

7.3.2.4 Evaluation of Compliance with IEEE-334

The only continuous duty Class I motors in containment are part of the containment fan coolers, which have been tested in the manner set forth in IEEE-334 (Reference 12).

7.3.2.5 Evaluation of Compliance with IEEE-338

The periodic testing of the ESFAS ~~actuation system~~ conforms to the requirements of IEEE-338 (Reference 13), with the exception that the periodic test frequency is in accordance with the Technical Specification Section 5.5.18 Surveillance Frequency Control Program.~~following comments:~~

~~(1) The periodic test frequency specified in the Technical Specifications was conservatively selected, using considerations in paragraph 4.3 of Reference 13, to ensure that equipment associated with protection functions has not drifted beyond its minimum performance requirements.~~

~~The test interval discussed in Paragraph 5.2 of Reference 13 is primarily developed on past operating experience, and modified, as necessary, to ensure that system and subsystem protection is reliably provided. Analytic methods for determining reliability are not used to determine test interval.~~

7.3.2.6 Evaluation of Compliance with IEEE-344

The seismic testing, as set forth in Section 3.10, conforms to the testing requirements of IEEE-344 (Reference 14), except that some tests may not conform to the guidelines of IEEE-344 since testing was completed prior to issuance of the standard. Documentation of the environmental and seismic qualification of the PPS~~process protection system~~ is provided in References ~~18, 19, 20, and 21~~29, 30, and 33.

7.3.2.7 Evaluation of Compliance with IEEE-317

See Section 7.2.2 for a discussion of conformance with IEEE-317 (Reference 15). The same applies to penetrations for systems described in Section 7.3.

7.3.2.8 Evaluation of Compliance with IEEE-336

See Section 7.2.2 for a discussion of conformance with IEEE-336 (Reference 16).

7.3.2.9 Evaluation of PPS Compliance with IEEE-603 and IEEE 7-4.3.2~~Eagle 21 Design, Verification, and Validation~~

~~The standards that are applicable to the Eagle 21 Design, Verification and Validation Plan are IEEE Standard 603-1980 (Reference 21), Regulatory Guide 1.152 (Reference 22), Regulatory Guide 1.153 (Reference 23), and ANSI/IEEE-ANS-7-4.3.2 (Reference 24).~~

Insert 3

7.3.2.10 Summary

The effectiveness of the ESFAS is evaluated in Chapter 15 based on the ability of the system to contain the effects of Conditions III and IV faults including loss of coolant and steam break accidents. The ESFAS parameters are based on the component performance specifications that are provided by the manufacturer, or verified by test for each component. Appropriate factors to account for uncertainties in the data are factored into the constants characterizing the system.

The ESFAS must detect Conditions III and IV faults and generate signals that actuate the ESF. The system must sense the accident condition and generate the signal actuating the protection function reliably, and within a time determined by, and consistent with, the accident analyses in Chapter 15.

The time required for the generation of the actuation signal of ESFAS is relatively short. The remainder of the time is associated with the actuation of the mechanical and fluid system equipment associated with ESF. This includes the time required for switching, bringing pumps and other equipment to speed, and the time required for them to take load.

Operating procedures normally require that the complete ESF actuation system be operable. However, redundancy of system components is such that the system operability

11. IEEE Standard 323-1971, Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

12. IEEE Standard 334-1971, Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

13. IEEE Standard 338-1971, Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems, The Institute of Electrical and Electronics Engineers, Inc.

14. IEEE Standard 344-1971, Trial-Use Guide for Seismic Qualifications of Class I Electric Equipment for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

15. IEEE Standard 317-1971, Electric Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

16. IEEE Standard, 336-1971, Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

17. ~~L. E. Erin, Topical Report Eagle 21 Microprocessor Based Process Protection System, WCAP-12374, September 1989.~~

Insert 4

18. R. B. Miller, Methodology for Qualifying Westinghouse WRD Supplied NSSS Safety Related Electrical Equipment, WCAP-8587, Westinghouse Proprietary Class 3.

19. Equipment Qualification Data Package, WCAP-8587, Supplement 1, EQDP-ESE-69A and 69B, Westinghouse Proprietary Class 3.

20. Equipment Qualification Test Report, WCAP-8687, Supplement 2-E69A and 69B, Westinghouse Proprietary Class 2.

21. IEEE Standard 603-1991~~1980~~, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

22. Regulatory Guide 1.152, Criteria for Use of~~Programmable Digital~~ Computers ~~System Software~~ in Safety~~-Related~~ Systems ~~in~~of Nuclear Power Plants, Revision 3, July~~November~~ ~~1985~~2011.

23. ~~Regulatory Guide 1.153, Criteria for Power, Instrumentation and Control Portions of Safety Systems, December 1985.~~

Insert 5

24. ANSI/IEEE-ANS-7-4.3.2, ~~Application~~ Standard Criteria for ~~Programmable~~ Digital Computers ~~Systems~~ in Safety Systems of Nuclear Power Generating Stations, 2003~~1982~~.

25. Reliability Assessment of Potter & Brumfield MDR Relays, WCAP-13878, Rev. 0, Westinghouse Proprietary Class 2C, June 1994.

26. Extension of Slave Relay Surveillance Test Intervals, WCAP-13900, R Westinghouse Proprietary Class 3, April 1994.

Insert 6

7.3.4 REFERENCE DRAWINGS

Figures representing controlled engineering drawings are incorporated by reference and are identified in Table 1.6-1. The contents of the drawings are controlled by DCPP procedures.

FSAR Section 7.3

Insert 1, Section 7.3.1.1.4.1

The PPS provides signals to the SSPS that will result in automatic actuation of ESFAS components when the limits of safe operation are approached. The safe operating region is defined by several considerations, such as mechanical/hydraulic limitations on equipment and heat transfer phenomena. The PPS monitors plant parameters, compares them against setpoints, and provides binary inputs (voltage/no voltage) to the SSPS.

The PPS is comprised of four Protection Channel (Channel I, II, III, or IV) Sets (also referred to as “protection rack sets,” “protection sets,” or “protection racks”). Each protection channel set is further comprised of various process “channels”. Each of the four PPS protection channel sets contains a microprocessor-based Tricon programmable logic controller subsystem (Reference 29) comprised of three separate legs and a field programmable gate array (FPGA) based Advanced Logic System (ALS) subsystem (Reference 30) comprised of an A core and a B core. The use of the PPS composed of the microprocessor-based Tricon subsystem and FPGA based ALS subsystem was approved by the NRC in License Amendment No. x/y (Reference 45).

The PPS Tricon subsystem is triple modular redundant (TMR) from input terminal to output terminal. The TMR architecture allows continued system operation in the presence of any single point of failure within the system. The Tricon subsystem contains power supply modules, input modules, main processor modules, communications modules, and output modules and each input and output module includes three separate and independent input or output circuits or legs. These legs communicate independently with the three main processor modules. Standard firmware is resident on the main processor modules for all three microprocessors as well as on the input, output, and communication modules. The PPS Tricon subsystem protection channel protection function can be performed by any of the three Tricon legs. The TMR architecture also allows the Tricon to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault within the TMR architecture, the Tricon self-diagnostics will alarm the condition, remove the affected portion of the faulted module from operation, and continues to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

The diverse ALS PPS subsystem utilizes FPGA hardware logic rather than a microprocessor and therefore has no software component required for operation of the system. The built-in diversity provided by the ALS A core and B core subsystems ensures that the PPS will perform the required PPS safety functions automatically in the presence of a postulated common cause software failure (References 31 and 32). The PPS ALS subsystem protection channel protection function can be performed by either the ALS A core or B core. At least one Tricon leg and one ALS core are required for a PPS protection set to perform all required protection functions required for that protection set. The ALS consists of a chassis containing core logic, input, and output cards and peripheral equipment consisting of cabinets, power supplies, control panels, and assembly panels. The ALS contains self-diagnostics capability to diagnose failures should they occur and self-test capability to support efficient surveillance testing.

The PPS meets the criteria in IEEE Standard 308-1980 (Reference 17), IEEE Standard 603-1991 (Reference 21), IEEE Standard 7-4.3.2-2003 (Reference 24), and RG 1.152, Revision 3 (Reference 22).

The PPS replacement has been designed to meet NRC Digital Instrumentation and Controls Interim Staff Guidance 04, Revision 1 (Reference 23), except for Section 1, "Interdivisional Communications," Staff Position 10. The PPS replacement has been designed to an alternative justification for this position based on the combination of redundancy within the Tricon subsystem and both redundancy and diversity in the ALS subsystem, along with administrative controls.

The PPS Tricon programmable logic controller subsystem was qualified in accordance with EPRI TR-107330 (Reference 27), with exceptions and clarifications identified in Table 2-2 of Reference 29. Compliance of the PPS with IEEE Standard 308-1980 (endorsed by IEEE Standard 603-1991 Clause 8) and IEEE Standard 603-1991 is described in Section 7.3.2.9. Compliance of the PPS with IEEE Standard 7-4.3.2-2003 (endorsed by Regulatory Guide 1.152 (Reference 22) is contained in Section of 3.11 of Reference 41 for the Tricon subsystem and in Section 12.2 of Reference 30 for the ALS subsystem. Compliance of the PPS with RG 1.152, Revision 3, is contained in Reference 42 for the Tricon subsystem and in Section 12.6 of Reference 30 for the ALS subsystem. Compliance of the PPS with NRC Digital Instrumentation and Controls Interim Staff Guidance 04, Revision 1, is contained in Reference 43 for the Tricon subsystem and in Reference 44 for the ALS subsystem.

Insert 2, Section 7.3.2.1

The PPS portion of the ESFAS is designed to meet the later IEEE-603 (Reference 21) and IEEE 7-4.3.2 (Reference 24) standards. Evaluation of the PPS compliance with the IEEE-603 and IEEE 7-4.3.2 standards is contained in Section 7.3.2.9.

Insert 3, Section 7.3.2.9

The PPS portion of the ESFAS is designed to comply with IEEE Standard 603-1991 (Reference 21) and with IEEE Standard 7-4.3.2-2003.

Compliance of the PPS with Standard IEEE 7-4.3.2 (endorsed by Regulatory Guide 1.152 (Reference 22) is contained in Section of 3.11 of Reference 41 for the Tricon subsystem and in Section 12.2 of Reference 30 for the ALS subsystem.

IEEE Standard 603-1991 contains safety related system criteria in five clauses (Clauses 4, 5, 6, 7 and 8). The compliance of the PPS portion of ESFAS to these five clauses and their sub-clauses is described in the subsections below.

7.3.2.9.1 IEEE Standard 603-1991 Clause 4, Design Basis

IEEE Standard 603-1991, Clause 4.1, Identification of the Design Basis Events, includes criteria to identify the design basis events applicable to each mode of operation and the initial conditions and allowable limits of plant conditions for each such event. This information is contained in the FSAR Update Sections 7.3.1.2 and 15. The PPS diversity and defense-in-depth analysis (References 31 and 32) evaluated a common cause software failure in the PPS and determined the built-in diversity provided by the PPS ALS subsystem ensures that all accidents and events that credit automatic PPS mitigation in the FSAR Update Section 15 accident analyses are mitigated automatically by the PPS.

IEEE Standard 603-1991, Clause 4.2, Identification of Safety Functions and Protective Actions, includes criteria to identify the safety functions and corresponding protective actions of the execute features for each design basis event. FSAR Update Sections 7.3.1.1 to 7.3.1.1.4 identify the safety function and protective actions performed by the PPS portion of the ESFAS. The ESFAS component actuation functions that are credited by the FSAR Update Section 15 accident analyses are listed in Table 7.3-1 and the component isolation functions are listed in Table 7.3-2.

IEEE Standard 603-1991, Clause 4.3, Permissive Conditions for Operating Bypasses, includes criteria to identify the permissive conditions for each operating bypass capability that is to be provided. The ESFAS permissives and associated functions are identified in Table 7.3-3.

IEEE Standard 603-1991, Clause 4.4, Variables monitored, includes criteria to identify the variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured. The variables monitored by the ESFAS, the criteria to identify the variables, and the ranges of the variables is contained in the FSAR Update Sections 7.3.1.1.1 and 7.3.1.2. The analytical limit for the variables is identified in the FSAR Update Section 15. The rates of change of the ESFAS steam line pressure function is identified in FSAR Update Sections 15.

IEEE Standard 603-1991, Clause 4.5, Minimum Criteria for Manual Protective Actions, includes criteria to identify the points in time and the plant conditions during which manual control is allowed, the justification for permitting initiation or control subsequent to initiation solely by manual means, the range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed, and the variables that shall be displayed for the operator to use in taking manual action. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation. Manual initiation of the ESFAS is not required, however manual trip capability exists as described in Section 7.3.2.1.1.

IEEE Standard 603-1991, Clause 4.6, Identification of the Minimum Number and Location of Sensors, includes criteria for those variables that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes. The basis for the required number and location of ESFAS sensors is contained in Reference 2. The only variable sensed by the ESFAS that has special dependence is reactor coolant temperature and this is addressed by taking multiple samples from the reactor coolant system hot leg and averaging the sample temperatures in the PPS.

IEEE Standard 603-1991, Clause 4.7, Range of Transient and Steady-State Conditions, includes criteria to identify the range of transient and steady-state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the safety system shall perform. Section 3 of Reference 34 contains this information for the PPS. The environmental and seismic qualification of the PPS is provided in References in References 29, 30, and 33.

IEEE Standard 603-1991, Clause 4.8, Conditions Causing Functional Degradation, includes criteria to evaluate the conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems). These conditions are addressed for the ESFAS in Section 7.3.1.2.

IEEE Standard 603-1991, Clause 4.9, Methods Used to Determine Reliability, includes criteria to identify the methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design. The reliability of the PPS Tricon subsystem is evaluated in Reference 38 and the reliability of the PPS ALS subsystem is evaluated in Reference 35.

IEEE Standard 603-1991, Clause 4.10, Critical Points in Time or Plant Conditions, includes criteria to identify the critical points in time or the plant conditions, after the onset of a design basis event, including the point in time or plant conditions for which the protective actions of the safety system shall be initiated, the point in time or plant conditions that define the proper completion of the safety function, the points in time or plant conditions that require automatic control of protective actions, and the point in time or plant conditions that allow returning a safety system to normal. This information is contained in Section 15.

IEEE Standard 603-1991, Clause 4.11, Equipment Protective Provisions, includes criteria to identify the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. There are no equipment protective provisions associated with the PPS that would prevent the safety systems from accomplishing their safety functions.

IEEE Standard 603-1991, Clause 4.12, Special Design Bases, includes criteria to identify any other special design basis that may be imposed on the system design (example: diversity, interlocks, and regulatory agency criteria). The PPS is a digital instrument and control system and therefore has been designed to meet the criteria of IEEE Standard 7-4.3.2-2003 (Reference 24), and RG 1.152, Revision 3 (Reference 22). The PPS replacement has been designed to meet NRC Digital Instrumentation and Controls Interim Staff Guidance 04, Revision 1 (Reference 23), except for Section 1, “Interdivisional Communications,” Staff Position 10, in which the PPS replacement has been designed to an alternative justification for this position based on the combination of redundancy within the Tricon subsystem and both redundancy and diversity in the ALS subsystem, along with administrative controls.

7.3.2.9.2 IEEE Standard 603-1991 Clause 5, System

IEEE Standard 603-1991, Clause 5.1, Single-Failure Criterion, includes criteria that the safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. The PPS is designed such that no single failure will impact the ability of the equipment to perform the safety function. Single failure for the PPS Tricon subsystem is addressed in Section 2.2.11 of Reference 29 and for the PPS ALS subsystem is addressed in Section 12.1.2 of Reference 30. The failure modes and effects analysis for the PPS Tricon subsystem is contained in Reference 36 and for the PPS ALS subsystem is contained in Reference 35.

IEEE Standard 603-1991, Clause 5.2, Completion of Protective Action, includes criteria that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. The PPS architecture is such that, once initiated, the protective action proceeds to completion. Interrupts are not used and return to normal operation requires deliberate operator action.

IEEE Standard 603-1991, Clause 5.3, Quality, includes criteria that the components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program. The PPS was designed, manufactured, and inspected in accordance with vendor QA programs. The PPS was installed and is tested, operated, and maintained in accordance with the Section 17 Quality Assurance Program and the PPS specific QA requirements in Reference 37.

IEEE Standard 603-1991, Clause 5.4, Equipment Qualification, includes criteria that safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. The equipment testing and analysis for the PPS Tricon subsystem is contained in Section 2 of Reference 29. The equipment testing and analysis for the PPS ALS subsystem is contained in Section 4 of Reference 30 and Reference 33.

IEEE Standard 603-1991, Cause 5.5, System Integrity, includes criteria that safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. The PPS has been designed and tested to confirm the equipment demonstrates system performance adequate to ensure completion of protective actions over the full range of applicable transient and steady-state plant conditions. The functional requirements for the PPS are contained in Reference 34. The PPS consists of four separate and isolated Protection Channels with adequate instrumentation to monitor the required reactor plant parameters and provide signals to the SSPS for use in determining when required protective actions are required.

IEEE Standard 603-1991, Clause 5.6, Independence

IEEE Standard 603-1991, Clause 5.6.1, Independence between Redundant Portions of a Safety System, includes criteria that redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish safety function during and following any design basis event requiring that safety function. The PPS consists of four independent Protection Channels. Each Protection Channel is physically separated and electrically isolated from the other sets. Each PPS Protection Channel is powered from a separate 120 V AC vital bus via a Class 1E uninterruptible power supply.

IEEE Standard 603-1991, Clause 5.6.2, Independence between Safety Systems and Effects of Design Basis Event, includes criteria that safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. The PPS consists of four independent Protection Channels. Each Protection Channel is physically separated and electrically isolated from the other sets. The functional requirements for the PPS considering effects of design basis events are contained in Reference 34. The equipment testing and analysis for the PPS Tricon subsystem is contained in Section 2 of Reference 29. The equipment testing and analysis for the PPS ALS subsystem is contained in Section 4 of Reference 30 and Reference 33. There are no credible missiles that can penetrate the PPS cabinets containing the Tricon and ALS subsystem processing equipment. Protection of the PPS cabinets against external fire events is accomplished through use of fire retardant paint, fire retardant wiring, fire barriers, an area fire suppression system, and through physical separation of the PPS cabinets.

IEEE Standard 603-1991, Clause 5.6.3, Independence between Safety Systems and Other Systems, includes criteria that safety system design shall be such that credible failures in and consequential actions by other systems, as documented in the design basis, shall not prevent the safety systems from meeting the requirements of this standard. Clause 5.6.3.1, Interconnected Equipment, (1) Classification, states equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems, isolation devices used to effect a safety system boundary shall be classified as part of the safety system. The PPS equipment used for both safety and non-safety functions is classified as part of the PPS.

Clause 5.6.3.1, (2) Isolation, includes criteria that no credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system. The PPS consists of four independent Protection Channels to ensure that the PPS protection function can be performed with failure of one Protection Channel. The effect of failure of isolation devices is considered in the system level failure modes and effects analysis for the PPS contained in Reference 39. The PPS Tricon and ALS subsystem processing equipment is protected from high current in the interfacing non-safety systems.

Clause 5.6.3.2 Equipment in Proximity, (1) Separation, includes criteria that equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981. The PPS equipment is physically separated from equipment in other systems by locating the redundant PPS Protection Channels in separate cabinets. The requirement for physical separation is provided in Section 1.2 of Reference 34.

Clause 5.6.3.2, (2) Barriers, includes criteria that physical barriers used to effect a safety system boundary shall meet the requirements of Clauses 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4.7 and 4.8 of the design basis. The PPS isolation devices that provide an electrical barrier meet the requirements of IEEE Standard 603-1991, Clauses 5.3, 5.4 and 5.5 for the applicable conditions specified in IEEE Standard 603-1991 Clause 4.7 and 4.8 of the design basis. The isolation devices meet the functional requirements for the PPS contained in Reference 34.

Clause 5.6.3.3, Effects of a Single Random Failure, includes criteria that where a single random failure in a non-safety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. The PPS consists of four independent Protection Channels that are physically separated and electrically isolated from each other. The functional requirements for the PPS considering effects of design basis events are contained in Reference 34.

Clause 5.7, Capability for Test and Calibration, includes criteria that capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. The PPS is capable of being tested online using the bypass capability of a channel while retaining the capability to perform the PPS safety function.

Simulated signal inputs into a channel can be applied using measuring and test equipment. Indication of channel bypass status is indicated in the control room.

Clause 5.8, Information Displays, Clause 5.8.1, Displays for Manually Controlled Actions, includes criteria that the display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation. Manual initiation of the ESFAS is not required, however manual initiation capability exists as described in Section 7.3.2.1.1.

Clause 5.8.2 System Status Indication, includes criteria that display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The PPS includes display instrumentation that indicates and identifies protective actions of the sense and command features and execute features. A “postage stamp” indicator lamp on the panel illuminates to indicate that a Protection Channel has been activated.

Clause, 5.8.3 Indication of Bypasses, .includes criteria that if the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room. The PPS is designed such that if a Protection Channel has been bypassed for any purpose, a signal is automatically provided to allow this condition to be continuously indicated in the control room.

Clause 5.8.4, Location, includes criteria that informational displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions. The PPS display instrumentation that indicates and identifies protective actions of the sense and command features is located in the control room and is visible from the location of the controls.

Clause 5.9, Control of Access, includes criteria that the design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof. The PPS equipment is located in a controlled area secured by the plant security system in a manner that only allows authorized personnel access. This limits the means to bypass safety system functions, via access controls, to authorized plant personnel.

Clause 5.10, Repair, includes criteria that the safety systems shall be designed to facilitate timely recognition, location, replacement, repair and adjustment of malfunctioning equipment. The PPS is designed with system diagnostics and self-testing features to detect both hardware and software faults and to assist in diagnostic and repair activities. Most failures are detectable within each Protection Channel including the processors, I/O modules, power supplies and the communication features.

The PPS equipment is contained in racks that allow removal and replacement of all cards and modules at power with the system on-line without adverse effect on the PPS safety function.

Clause 5.11, Identification, includes criteria that to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met; safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEEE Std 384-1981 and IEEE Std 420-1982; components for modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification; Identification of safety system equipment shall be distinguishable from identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables); identification of safety system equipment and its divisional assignment shall not require frequent use of reference material, and the associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974. For the PPS, a color coded nameplate on each rack is used to differentiate between different Protection Channels. All non-rack-mounted protective equipment and components are provided with an identification tag or nameplate. Additional details are contained in Section 7.1.2.3.

Clause, Clause 5.12, Auxiliary Features, includes criteria that auxiliary supporting features shall meet all requirements of the standard. Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety functions, and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. The PPS Tricon subsystem and PPS ALS subsystem are safety-related and do not contain auxiliary features that support performance of the automatic PPS safety function. The communication architecture provides the ability to transmit PPS information to the non-safety related PDN Gateway Computer. The PPS Tricon subsystem utilizes a port aggregator tap device to prevent communication from the PDN Gateway Computer to the Tricon subsystem. The PPS ALS subsystem utilizes a communication channel that is inherently one-way to the PDN Gateway Computer to prevent communication from the PDN Gateway Computer to the ALS subsystem.

The communication architecture also provides the ability to transmit PPS information with the non-safety related MWS for each PPS subsystem used for testing, maintenance, and troubleshooting. The PPS Tricon subsystem utilizes a fiber optic media connection between the Tricon subsystem and the Tricon communications module to provide electrical isolation. The PPS Tricon subsystem prevents communication from the Tricon maintenance workstation to the Tricon subsystem from affecting the safety function by preventing data input while a safety-related instrument-loop-specific out of service switch is determined to be open by the application software. Two-way communication from the Tricon MWS to the Tricon subsystem is only permitted when the safety-related instrument-loop-specific out of service switch is determined to be closed by the application software. The PPS ALS subsystem utilizes a communication channel that is inherently one-way to the ALS MWS. The PPS ALS subsystem also utilizes a test ALS bus communication channel that provides two-way communications between the ALS maintenance software in the ALS MWS and the ALS subsystem. The communication path between the ALS MWS and the ALS subsystem is normally disabled by physically disconnecting the communication link from the Test ALS Bus to the ALS MWS. Two-way communication is only permitted when the communication link is physically connected (enabled) between the TAB and the ALS MWS to allow surveillance testing, maintenance, and trouble-shooting.

Clause 5.13, Multi-Unit Stations, includes criteria that the sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. The PPS does not share any PPS components between the units.

Clause 5.14, Human Factors Considerations, includes criteria that human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988. Human factors are considered in the PPS design. The PPS uses devices located on the control room vertical boards and control console. To support operation, a human system interface located on the control room control console provides PPS system health and status displays via a connection to the PDN Gateway Computer. To support maintenance and engineering, the MWS for each subsystem provides display of PPS functions. The PPS Tricon and ALS system cards and modules display the results of operation and self-diagnostic information.

Clause 5.15, Reliability, includes criteria for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. The PPS is designed to be highly reliable and exceeds the EPRI TR-107330 reliability goal of 99.0 percent reliability analysis as documented for the Tricon subsystem in Reference 38 and for the ALS subsystem in Reference 35.

7.3.2.9.3 Clause 6, Sense and Command Features

Clause 6.1, Automatic Control, includes criteria that means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5. The PPS performs sense and command functions by providing trip and actuation signals to the SSPS for use by the RTS, and ESFAS, which performs the execute functions. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation.

Clause 6.2, Manual Control, Clause 6.2.1, includes criteria that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1. Manual ESFAS capability is provided as described in Section 7.3.2.1.1. Means are provided in the control room for manual initiation at the division level (SSPS Train "A" and Train "B") of the automatically initiated protective actions Manual SI, Manual SLI, Manual Containment Isolation Phase A, and Manual Containment Spray. These means are provided at the SSPS actuation level, downstream of the PPS, and are independent of any PPS hardware or software.

Clause 6.2.2, includes criteria that means shall be provided in the control room to implement manual initiation and control of the protective actions identified in Clause 4.5 that have not been selected for automatic control under Clause 6.1. The displays provided for these actions shall meet the requirements of Clause 5.8.1. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation.

Clause 6.2.3, includes criteria that means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action. The required PPS information and PPS devices is located on the control room vertical boards and control console and are accessible and suitable for the operator to maintain safe conditions after PPS protective actions are initiated.

Clause 6.3, Interaction with Other Systems, Clause 6.3.1 includes criteria that where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis, or equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Clause 6.3.2 includes criteria that provisions shall be included so that the requirements in Clause 6.3.1 can be met in conjunction with the requirements of Clause 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

The PPS diversity and defense-in-depth analysis (References 31 and 32) evaluated the capability of the ESFAS functions to be performed for FSAR Update Section 15 accidents and included evaluation of a common cause software failure in the PPS. PPS diversity and defense-in-depth analysis, determined the built-in diversity provided by the PPS ALS subsystem ensures that all accidents that credit automatic PPS mitigation in the FSAR Update Section 15 accident analyses are mitigated automatically by the PPS. FSAR Update Section 15 accident analyses include consideration of the impact of the accidents on the performance of non-safety systems. For other events such as earthquakes, fire, missiles, flood, and wind, the PPS components are protected from applicable events or sufficient component redundancy is available such that the PPS safety function can be performed. The failure modes and effects analysis for the PPS Tricon subsystem is contained in Reference 36, for the PPS ALS subsystem is contained in Reference 35, and for the PPS system is contained in Reference 39. The failure modes and effects analysis determined the PPS can perform the safety function considering a failure of a PPS Protection Channel. The failure of a PPS Protection Channel is equivalent to the effect of a PPS channel being placed in maintenance bypass.

The PPS is designed to minimize the possibility of occurrence of events that can potentially cause a non-safety system action that results in a condition requiring PPS protective action and concurrently prevents the PPS from providing protection for the event. Transmitter (sensor) inputs required by both the PPS and the control system are provided to the control system via qualified isolation devices (independent of the PPS) located on the transmitter input circuit. The analog signal for use by the control system is not processed by the PPS equipment and thus is not subject to PPS software common cause failure. RTD inputs to PPS channels are an exception. RTD inputs are conditioned (resistance to temperature) by the ALS and output to the Tricon as analog signals for processing by wide range temperature channels, pressurizer vapor temperature channel, and ΔT/Tavg channels. The ΔT/Tavg channels provide analog outputs to the rod speed and direction control system.

Clause 6.4, Derivation of System Inputs, includes criteria that to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. The process variables and derived parameters used for the PPS ESFAS actuation functions identified in FSAR Update Section 7.3.1.1.3 are derived from signals that are direct measures of the variables.

Clause 6.5, Capability for Testing and Calibration, Clause 6.5.1, contains criteria that means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation; and Clause 6.5.2 contains criteria that one of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period, checking the operational availability of sensors by use of the methods described in Clause 6.5.1; or specifying equipment that is stable and retains its calibration during the post-accident time period. The PPS incorporates self-testing diagnostic features as well as range checking on all sensor inputs. A trouble alarm is generated upon detection of an input failure or an out-of-range low or out-of-range high input condition at -5 percent (low) and 105 percent (high) of span. The PPS has the capability for channel checks using indications provided in the control room.

Clause 6.6, Operating Bypasses, includes criteria that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall accomplish one of the following actions, remove the appropriate active operating bypass(es), restore plant conditions so that permissive conditions once again exist, or initiate the appropriate safety function(s). Section 7.3.2.1.5.6 discusses operating bypasses for the ESFAS. Where operating requirements necessitate automatic or manual bypass of a protective function, the design is such that the bypass is removed automatically whenever permissive conditions for the bypass are not satisfied. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protective system and are designed accordingly. The ability to initiate appropriate safety functions is available at all times. Indication is provided in the control room if some part of the protection system has been administratively bypassed or taken out of service.

Clause 6.7, Maintenance Bypass, includes criteria that capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of Clause 5.1 and Clause 6.3. An exception is one-out-of-two portions of the sense and command features are not required to meet Clause 5.1 and Clause 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated) that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability). FSAR Update Section 7.3.2.1.5.6 discusses testing in bypass and presents the normal method for removing channels for maintenance. The PPS is designed to permit an inoperable channel to be placed in a bypass condition for the purpose of troubleshooting or periodic test of a redundant channel. Use of the bypass mode disables the individual channel comparator trip circuitry that forces the associated logic input relays to remain in the non-tripped state until the bypass' is removed. If the PPS channel has been bypassed for any purpose, a signal is provided to allow this condition to be continuously indicated in the control room. The PPS system failure modes and effects analysis contained in Reference 39 assumes an initial condition that a PPS channel is placed in the bypass and determines the overall effect of an evaluated failure on the safety system's capability to perform the required safety functions in this configuration. The PPS system failure modes and effects analysis demonstrates the PPS has sufficient redundancy, independence and other required design fundamentals such that the safety function can be performed even with a channel in the bypass.

Clause 6.8, Setpoints, includes criteria that the allowance for uncertainties between the process analytical limit and the device setpoint shall be determined using a documented methodology, and that where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features. The calculations for the PPS setpoints are contained in Reference 40 and include allowance for uncertainties between the process analytical limit and the device setpoint. The PPS does not utilize multiple setpoints for any parameter in any one direction.

7.3.2.9.4 Clause 7, Execute Features

Clause 7.1, Automatic Control, includes criteria that capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4.4 of the design basis. The PPS performs sense and command functions by providing trip and actuation signals to the SSPS for use by the ESFAS. PPS protection outputs provide ON/OFF (partial trip) signals to the two trains of the SSPS whenever measured parameters indicate that safety limits are being approached (a pre-established setpoint is exceeded). The SSPS actuates ESFAS component(s) when the requisite number of PPS channels have tripped (designed coincidence logic is satisfied). The execute features for the ESFAS are performed by the SSPS. The ESFAS functions proceed to completion because the output signals from the SSPS are electrically latched and seal-in on command. These signals also require a manual operator action to unlatch them. In addition, the SI signal has a timer that prevents manual reset by the operator for 30 seconds following SI actuation to ensure the SI proceeds to completion.

Clause 7.2, Manual Control, includes criteria that If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of Clause 5.1 and Clause 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis. The PPS is designed to provide automatic initiation for all FSAR Update Section 15 accidents and events that credit automatic PPS mitigation. Manual ESFAS capability is provided as described in Section 7.3.2.1.1. Means are provided in the control room for manual initiation at the division level (SSPS Train "A" and Train "B") of the automatically initiated protective actions Manual RT. These means are provided at the SSPS actuation level, downstream of the PPS, and are independent of any PPS hardware or software. The required PPS information and PPS devices is located on the control room vertical boards and control console.

Clause 7.3, Completion of Protective Action, includes criteria that the design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function. All PPS execute features are performed by the SSPS. The PPS monitors plant parameters and sends partial trip/actuation signals to the SSPS when predetermined setpoints are exceeded. The SSPS provides sealed-in ESFAS actuation signals when the coincidence logic for a particular trip/actuation function is satisfied. The SSPS does not require manual intervention or acknowledgement of actuation commands to complete a protective function. The SSPS ESFAS actuation signal requires manual action to reset following completion of the protective action and only after the PPS initiating signals have reset.

Clause 7.4, Operating Bypasses, includes requirements that whenever the applicable conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions; remove the appropriate active operating bypass(es), restore plant conditions so that permissive conditions once again exist, or initiate the appropriate safety function(s). The operating bypasses associated with the PPS are performed by the SSPS and are not performed by the PPS. The operating bypasses are automatically removed when plant conditions change to an operating mode in which protective actions are required to be operable so that a design basis event can be mitigated.

Clause 7.5, Maintenance Bypass, includes criteria that the capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability. FSAR Update Section 7.3.2.1.5.6 discusses testing in bypass and presents the normal method for removing channels for maintenance. Alternatively, for various PPS ESFAS functions, the Technical Specifications allow an inoperable channel and one additional channel to be surveillance tested with one channel in bypass and one channel in trip for up to 12 hours, or both the inoperable and the additional channel to be surveillance tested in bypass for up to 12 hours. During the period the PPS ESFAS functions are in the bypass configurations allowed by the Technical Specifications, the PPS is still capable to accomplish its safety function if a valid ESFAS signal occurs.

7.3.2.9.5 Clause 8, Power Source

Clause 8.1, Electrical Power Sources, provides criteria that those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1980. The PPS portion of the protection system is designed to conform to IEEE-308-1980 (Reference 17). The PPS utilizes Class 1E power sources. Each PPS Protection Channel is powered from a separate 120 V AC vital bus via a Class 1E uninterruptible power supply. The Class 1E power sources are described in Section 8.1.1.4.

Clause 8.2, Non-Electrical Power Sources, includes criteria that non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. The PPS does not rely on non-electrical power sources for performance of its safety related functions.

Clause 8.3, Maintenance Bypass, includes criteria that the capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability. Each PPS Protection Channel is powered from a separate 120 V AC vital bus. If an external power source for a safety-related Protection Channel fails, the remaining safety-related Protection Channel will ensure that the safety system remains capable of performing the assigned safety function. Additional power source redundancy to assure reliability is provided within the Protection Channel. The Tricon subsystem chassis contains two redundant chassis power supplies that are qualified Class 1E power modules that are supplied from separate external power sources. Each ALS subsystem chassis contains two redundant chassis power supplies that are qualified Class 1E power supplies that are supplied from separate external power supplies. Each chassis power supply is capable of supplying full chassis load in the event of failure (or bypass) of the other power supply.

Insert 4, Section 7.3.3

Reference 17 IEEE Standard 308-1980, Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations, The Institute of Electrical and Electronics Engineers, Inc.

Insert 5, Section 7.3.3

Reference 23 NRC Digital Instrumentation and Controls Interim Staff Guidance, Digital I&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms - Communications Issues (HICRc), Revision 1," March 6, 2009.

Insert 6, Section 7.3.3

Reference 27 EPRI TR-107330, Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, 1997.

Reference 28 J. W. Hefler, Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Conceptual Design Document, Revision 4, 2011, Altran Solutions.

Reference 29 Triconex Topical Report, Invensys Operations Management Document 7286-545-1-A, Revision 4, May 15, 2012.

Reference 30 Advanced Logic System Topical Report, CS Innovations Document 6002-00301, Revision 4, February, 2013.

Reference 31 S. B Patterson, Diablo Canyon Power Plant Process Protection System Replacement Diversity & Defense-in-Depth Assessment, Revision 1, August, 2010, PG&E Proprietary Report.

Reference 32 Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, "Process Protection System Replacement

Diversity & Defense-In-Depth Assessment (TAC Nos. ME4094 and ME4095), US NRC, April 19, 2011.

Reference 33 ALS EQ Results, 6002-00200, CS Innovations proprietary.

Reference 34 Functional Requirement Specification, Process Protection System Replacement, MONTH YEAR.

Reference 35 Diablo Canyon ALS Reliability Analysis and Failure Mode and Effects Analysis, CS Innovations Document 6116-00029, Revision 1, April 2012.

Reference 36 Failure Modes and Effects Analysis, Invensys Operations Management Document 993754-1-811.

Reference 37 Process Protection System (PPS) Replacement System Quality Assurance Plan (SyQAP), Revision 1, March 2013.

Reference 38 Reliability Analysis, Invensys Operations Management Document 993754-1-819.

Reference 39 Process Protection System (PPS) Replacement System Level Failure Modes and Effects Analysis, Revision 0, 201x.

Reference 40 C. R. Tuley, et. al., Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant, WCAP-17706-P, Revision 0, January 2013, and Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System, WCAP 17696-P, Revision 0, January 2013.

Reference 41 Final Safety Evaluation For Invensys Operations Management "Triconex Topical Report", NRC Office of Nuclear Reactor Regulation, April 12, 2012.

Reference 42 Process Protection System Replacement Diablo Canyon Power Plant Regulatory Guide 1.152 Conformance Report, Invensys Operations Management Document 993754-1-913-P, Revision 0, September 2011.

Reference 43 Process Protection System Replacement Diablo Canyon Power Plant DI&C-ISG-04 Conformance Report, Invensys Operations Management Document No. 993754-1-912-P, Revision 0, September 2011.

Reference 44 Diablo Canyon PPS ISG04 Matrix, CS Innovations Document 6116-00054, Revision 0, November 2012.

Reference 45 License Amendments No. x (Unit 1) and y (Unit 2), TITLE, dated DATE.