UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 21, 2016

Mr. Edward D. Halpin
Senior Vice President and Chief Nuclear Officer
Pacific Gas and Electric Company
Diablo Canyon Power Plant
P.O. Box 56, Mail Code 104/6
Avila Beach, CA 93424

SUBJECT: DIABLO CANYON POWER PLANT, UNITS 1 AND 2 - ISSUANCE OF AMENDMENTS RE: DIGITAL REPLACEMENT OF THE PROCESS PROTECTION SYSTEM PORTION OF THE REACTOR PROTECTION SYSTEM AND ENGINEERED SAFETY FEATURES ACTUATION SYSTEM (CAC NOS. ME7522 AND ME7523)

Dear Mr. Halpin:

The U.S. Nuclear Regulatory Commission (NRC, the Commission) has issued the enclosed Amendment No. 227 to Facility Operating License No. DPR-80 and Amendment No. 229 to Facility Operating License No. DPR-82 for the Diablo Canyon Power Plant, Units 1 and 2 (DCPP), respectively. The amendments consist of changes to the Technical Specifications (TSs) in response to your application dated October 26, 2011, as supplemented by letters dated December 20, 2011; April 2, April 30, June 6, August 2, September 11, November 27, and December 5, 2012; March 7, March 25, April 30, May 9, May 30, and September 17, 2013; April 24 and April 30, 2014; February 2 and June 22, 2015; and January 25, February 11, and August 17, 2016.

The license amendment request would provide a digital replacement of the process protection system (PPS) portion of the reactor trip system and engineered safety features actuation system at DCPP. The amendments replace the Eagle 21 digital PPS with a new digital PPS that is based on the Invensys Operations Management Tricon Programmable Logic Controller and the CS Innovations, LLC (Westinghouse Electric Company) Advanced Logic System. The current Eagle 21 PPS is a digital microprocessor-based system which provides process protection features for the reactor protection system that is comprised of the reactor trip system and engineered safety features actuation system. The PPS replacement consists of a microprocessor-based Tricon Programmable Logic Controller and the field programmable gate array-based Advanced Logic System that will improve the reliability and diversity of the PPS. By letter dated April 30, 2013, the licensee also requested a change to TS 1.1, "Definitions," to revise the definition of "Channel Operational Test (COT)" resulting from the proposed modifications.

Enclosure 3 to this letter contains Proprietary Information. When separated from Enclosure 3, this letter is DECONTROLLED.

The NRC staff has determined that the related safety evaluation contains proprietary information pursuant to Title 10 of the *Code of Federal Regulations* Section 2.390. The proprietary version of the safety evaluation is provided in Enclosure 3. Accordingly, the NRC staff has also prepared a non-proprietary version of the safety evaluation, which is provided in Enclosure 4.

The Notice of Issuance will be included in the Commission's next regular biweekly *Federal Register* notice.

Sincerely,

Balwant K Singal

Balwant K. Singal, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

Enclosures:
1. Amendment No. 227 to DPR-80
2. Amendment No. 229 to DPR-82
3. Safety Evaluation (proprietary)
4. Safety Evaluation (non-proprietary)

cc w/o Enclosure 3: Distribution via Listserv

ENCLOSURE 1

PACIFIC GAS AND ELECTRIC COMPANY

DOCKET NO. 50-275

DIABLO CANYON NUCLEAR POWER PLANT, UNIT 1

AMENDMENT NO. 227 TO FACILITY OPERATING LICENSE NO. DPR-80

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

PACIFIC GAS AND ELECTRIC COMPANY

DOCKET NO. 50-275

DIABLO CANYON NUCLEAR POWER PLANT, UNIT 1

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 227
License No. DPR-80

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment by Pacific Gas and Electric Company (the licensee), dated October 26, 2011, as supplemented by letters dated December 20, 2011; April 2, April 30, June 6, August 2, September 11, November 27, and December 5, 2012; March 7, March 25, April 30, May 9, May 30, and September 17, 2013; April 24 and April 30, 2014; February 2 and June 22, 2015; and January 25, February 11, and August 17, 2016, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and Paragraph 2.C.(2) of Facility Operating License No. DPR-80 is hereby amended to read as follows:

(2) Technical Specifications

The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, as revised through Amendment No. 227, are hereby incorporated in the license. Pacific Gas & Electric Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

3. This license amendment is effective as of its date of issuance and shall be implemented within 120 days from the date of issuance. Implementation of the amendment shall also include revision of the Final Safety Analysis Report Update as described in the licensee's letter dated April 30, 2013.

FOR THE NUCLEAR REGULATORY COMMISSION

RJPascarelli

Robert J. Pascarelli, Chief
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Facility
Operating License No. DPR-80
and Technical Specifications

Date of Issuance: December 21, 2016

ENCLOSURE 2

PACIFIC GAS AND ELECTRIC COMPANY

DOCKET NO. 50-323

DIABLO CANYON NUCLEAR POWER PLANT, UNIT 2

AMENDMENT NO. 229 TO FACILITY OPERATING LICENSE NO. DPR-82

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

PACIFIC GAS AND ELECTRIC COMPANY

DOCKET NO. 50-323

DIABLO CANYON NUCLEAR POWER PLANT, UNIT 2

AMENDMENT TO FACILITY OPERATING LICENSE

Amendment No. 229
License No. DPR-82

1. The Nuclear Regulatory Commission (the Commission) has found that:

   A. The application for amendment by Pacific Gas and Electric Company (the licensee), dated October 26, 2011, as supplemented by letters dated December 20, 2011; April 2, April 30, June 6, August 2, September 11, November 27, and December 5, 2012; March 7, March 25, April 30, May 9, May 30, and September 17, 2013; April 24 and April 30, 2014; February 2 and June 22, 2015; and January 25, February 11, and August 17, 2016, complies with the standards and requirements of the Atomic Energy Act of 1954, as amended (the Act), and the Commission's regulations set forth in 10 CFR Chapter I;

   B. The facility will operate in conformity with the application, the provisions of the Act, and the rules and regulations of the Commission;

   C. There is reasonable assurance (i) that the activities authorized by this amendment can be conducted without endangering the health and safety of the public, and (ii) that such activities will be conducted in compliance with the Commission's regulations;

   D. The issuance of this amendment will not be inimical to the common defense and security or to the health and safety of the public; and

   E. The issuance of this amendment is in accordance with 10 CFR Part 51 of the Commission's regulations and all applicable requirements have been satisfied.

2. Accordingly, the license is amended by changes to the Technical Specifications as indicated in the attachment to this license amendment, and Paragraph 2.C.(2) of Facility Operating License No. DPR-82 is hereby amended to read as follows:

   (2) Technical Specifications (SSER 32, Section 8)* and Environmental Protection Plan

   The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, as revised through Amendment No. 229, are hereby incorporated in the license. Pacific Gas & Electric Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

3. This license amendment is effective as of its date of issuance and shall be implemented within 120 days from the date of issuance. Implementation of the amendment shall also include revision of the Final Safety Analysis Report Update as described in the licensee's letter dated April 30, 2013.

FOR THE NUCLEAR REGULATORY COMMISSION

Robert J. Pascarelli, Chief
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Attachment:
Changes to the Facility
Operating License No. DPR-82
and Technical Specifications

Date of Issuance: December 21, 2016

ATTACHMENT TO LICENSE AMENDMENT NO. 227

TO FACILITY OPERATING LICENSE NO. DPR-80

AND AMENDMENT NO. 229 TO FACILITY OPERATING LICENSE NO. DPR-82

DOCKET NOS. 50-275 AND 50-323

Replace the following pages of the Facility Operating License Nos. DPR-80 and DPR-82, and Appendix A Technical Specifications with the attached revised pages. The revised pages are identified by amendment number and contain marginal lines indicating the areas of change.

Facility Operating License Nos. DPR-80

REMOVE	INSERT
3	3

Facility Operating License Nos. DPR-82

REMOVE	INSERT
3	3

Technical Specifications

REMOVE	INSERT
1.1-2	1.1-2
--	1.1-2a

(4) Pursuant to the Act and 10 CFR Parts 30, 40, and 70, to receive, possess, and use in amounts as required any byproduct, source or special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and

(5) Pursuant to the Act and 10 CFR Parts 30, 40, and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.

C. This License shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

The Pacific Gas and Electric Company is authorized to operate the facility at reactor core power levels not in excess of 3411 megawatts thermal (100% rated power) in accordance with the conditions specified herein.

(2) Technical Specifications

The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, as revised through Amendment No. 227 are hereby incorporated in the license. Pacific Gas & Electric Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

(3) Initial Test Program

The Pacific Gas and Electric Company shall conduct the post-fuel-loading initial test program (set forth in Section 14 of Pacific Gas and Electric Company's Final Safety Analysis Report, as amended), without making any major modifications of this program unless modifications have been identified and have received prior NRC approval. Major modifications are defined as:

a. Elimination of any test identified in Section 14 of PG&E's Final Safety Analysis Report as amended as being essential;

(4) Pursuant to the Act and 10 CFR Parts 30, 40, and 70, to receive, possess, and use in amounts as required any byproduct, source or special nuclear material without restriction to chemical or physical form, for sample analysis or instrument calibration or associated with radioactive apparatus or components; and

(5) Pursuant to the Act and 10 CFR Parts 30, 40, and 70, to possess, but not separate, such byproduct and special nuclear materials as may be produced by the operation of the facility.

C. This License shall be deemed to contain and is subject to the conditions specified in the Commission's regulations set forth in 10 CFR Chapter I and is subject to all applicable provisions of the Act and to the rules, regulations, and orders of the Commission now or hereafter in effect; and is subject to the additional conditions specified or incorporated below:

(1) Maximum Power Level

The Pacific Gas and Electric Company is authorized to operate the facility at reactor core power levels not in excess of 3411 megawatts thermal (100% rated power) in accordance with the conditions specified herein.

(2) Technical Specifications (SSER 32, Section 8)* and Environmental Protection Plan

The Technical Specifications contained in Appendix A and the Environmental Protection Plan contained in Appendix B, as revised through Amendment No. 229, are hereby incorporated in the license. Pacific Gas & Electric Company shall operate the facility in accordance with the Technical Specifications and the Environmental Protection Plan, except where otherwise stated in specific license conditions.

(3) Initial Test Program (SSER 31, Section 4.4.1)

Any changes to the Initial Test Program described in Section 14 of the FSAR made in accordance with the provisions of 10 CFR 50.59 shall be reported in accordance with 50.59(b) within one month of such change.

*The parenthetical notation following the title of many license conditions denotes the section of the Safety Evaluation Report and/or its supplements wherein the license condition is discussed.

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 4

NON-PROPRIETARY SAFETY EVALUATION

RELATED TO AMENDMENT NO. 227 TO FACILITY OPERATING LICENSE NO. DPR-80

AND AMENDMENT NO. 229 TO FACILITY OPERATING LICENSE NO. DPR-82

PACIFIC GAS AND ELECTRIC COMPANY

DIABLO CANYON NUCLEAR POWER PLANT, UNITS 1 AND 2

DOCKET NOS. 50-275 AND 50-323

SAFETY EVALUATION

PACIFIC GAS AND ELECTRIC COMPANY

DIABLO CANYON NUCLEAR POWER PLANT, UNITS 1 AND 2

DOCKET NOS. 50-275 AND 50-323

Table of Contents

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

RELATED TO AMENDMENT NO. 227 TO FACILITY OPERATING LICENSE NO. DPR-80

AND AMENDMENT NO. 229 TO FACILITY OPERATING LICENSE NO. DPR-82

PACIFIC GAS AND ELECTRIC COMPANY

DIABLO CANYON NUCLEAR POWER PLANT, UNITS 1 AND 2

DOCKET NOS. 50-275 AND 50-323

1.0 INTRODUCTION

By letter dated October 26, 2011 (Reference 1), as supplemented by letters dated December 20, 2011 (Reference 2); April 2, 2012 (Reference 3), April 30, 2012 (Reference 4), June 6, 2012 (Reference 5), August 2, 2012 (Reference 6), September 11, 2012 (Reference 7), November 27, 2012 (Reference 8), and December 5, 2012 (Reference 9); March 7, 2013 (Reference 10), March 25, 2013 (Reference 11), April 30, 2013 (Reference 12), May 9, 2013 (Reference 13), May 30, 2013 (Reference 14), and September 17, 2013 (Reference 15); April 24, 2014 (Reference 16), and April 30, 2014 (Reference 17); February 2, 2015 (Reference 18), and June 22, 2015 (Reference 19); and January 25, 2016 (Reference 20), February 11, 2016 (Reference 21), and August 17, 2016 (Reference 22), Pacific Gas and Electric Company (PG&E, the licensee), requested changes to the Technical Specifications (TSs) (Appendix A to Facility Operating License Nos. DPR-80 and DPR-82) for the Diablo Canyon Power Plant, Units 1 and 2 (DCPP, Diablo Canyon), respectively. Portions of the letters dated December 20, 2011; April 2, April 30, June 6, August 2, November 27, and December 5, 2012; March 7, March 25, May 30, and September 17, 2013; April 24, 2014; February 2, 2015; and January 25 and February 11, 2016, contain sensitive unclassified non-safeguards information and, accordingly, have been withheld from public disclosure pursuant to Section 2.390, "Public inspections, exemptions, requests for withholding," of Title 10 of the *Code of Federal Regulations* (10 CFR).

The supplemental letter dated August 17, 2016, provided additional information that clarified the application, did not expand the scope of the application as originally noticed, and did not change the U.S. Nuclear Regulatory Commission (NRC) staff's original proposed no significant hazards consideration determination as published in the *Federal Register* on June 7, 2016 (81 FR 36606).

The license amendment request (LAR) would provide a digital replacement of the process protection system (PPS) portion of the reactor trip system (RTS) and engineered safety features actuation system (ESFAS) at DCPP. The amendments replace the Eagle 21 digital PPS with a new digital PPS that is based on the Invensys Operations Management (IOM) Tricon Programmable Logic Controller (PLC), Version 10 (Tricon V10), and the CS Innovations, LLC (CSI, a Westinghouse Electric Company) Advanced Logic System (ALS). The current Eagle 21 PPS is a digital microprocessor-based system, which provides process protection features for the reactor protection system (RPS) that is composed of RTS and ESFAS. The 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. By letter dated April 30, 2013, the licensee also requested a change to TS 1.1, "Definitions," to revise the definition of "Channel Operational Test (COT)" resulting from the proposed modifications.

The current Eagle 21 PPS was approved by the NRC in license Amendment Nos. 83 (Unit 1) and 84 (Unit 2), by letter dated October 7, 1993 (Reference 23). The DCPP Eagle 21 PPS is being replaced to address obsolescence, diagnostic, maintenance, and reliability issues. The new digital PPS performs functions in support of the RPS comprised of the RTS and ESFAS. The PPS provides signal processing (from the existing input sensors), signal validation, and protection trip logic functions in support of these systems. The replacement system provides on-line self-testing and diagnostic functions to improve the availability of the system and to improve system maintainability. All functions currently performed by the Eagle 21 PPS will be maintained in the replacement digital PPS.

The NRC issued Interim Staff Guidance (ISG) in digital instrumentation and control (I&C) DI&C-ISG-06 (ISG-06), Revision 1, "Task Working Group #6: Licensing Process, Interim Staff Guidance," dated January 19, 2011 (Reference 24). This guidance describes the licensing process to be used for the review of LARs associated with digital I&C system modifications. This LAR is the pilot application for use of ISG-06. The licensee followed the LAR format and contents described in Enclosure E and Section C.3, respectively, of ISG-06. The NRC staff's safety evaluation related to this LAR was prepared in accordance with the guidance of ISG-06. In particular, ISG-06 defines a phased process for submittal of information to support the NRC staff's review.

The DCPP PPS LAR references two topical reports submitted by IOM and CSI. By letter dated January 5, 2011 (Reference 25), IOM submitted Document No. 7286-545-1, Revision 4, "Triconex Topical Report," dated December 20, 2010 (Reference 26), and by letter dated July 29, 2010 (Reference 27), CSI submitted Document 6002-00301, Revision 0, "Advanced Logic System Topical Report," dated July 30, 2010 (Reference 28), and their supporting documents. These platforms were initially referenced as Tier 2 and Tier 3 platforms, respectively, per the guidance of ISG-06. Subsequently, the Tricon V10 platform was approved in the "Triconex Approved Topical Report" by NRC letter dated May 15, 2012 (Reference 29), and the ALS platform was approved in the "Advanced Logic System Topical Report," by NRC letter dated September 9, 2013 (Reference 30). Furthermore, the LAR appropriately addressed all plant-specific action items listed in Section 6.0 of the safety evaluations for the Tricon V10 and ALS topical reports.

The DCPP PPS LAR dated October 26, 2011 (Reference 1), includes a detailed description, safety analysis, technical evaluation, regulatory compliance evaluation, and a significant hazards consideration and environmental consideration for the replacement system. The LAR was accepted for review by the NRC staff on January 13, 2012 (Reference 31). The NRC staff's acceptance review letter identified some aspects of the application that were insufficient and identified issues pertaining to the following design and programmatic features provided in the LAR.

1. Deterministic software
2. Software management plan
3. Software verification and validation (V&V) plan
4. Software configuration management plan
5. Software test plan
6. Equipment qualification testing plans
7. Design analysis reports
8. Setpoint methodology
9. Compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32), IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33), and DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance" (ISG-04), dated March 6, 2009 (Reference 34), are adequately addressed within the LAR and the ALS topical report.

The licensee subsequently addressed each of the issues and provided additional supporting information for the LAR in the September 11, 2012 (Reference 7), response to the NRC staff's request for additional information (RAI) dated August 7, 2012 (Reference 35). The licensee also submitted supplemental documents to support the RAI responses. All Phase 2 documentation was provided per the licensee's commitments. In addition, the NRC staff conducted four audits of the DCPP PPS subsystems at the respective vendor facilities on November 13-16, 2012 (Reference 36), February 11-14, 2013 (Reference 37), June 3-5, 2014 (Reference 38), and June 22-26, 2015 (Reference 39).

By letter dated April 30, 2013 (Reference 12), the licensee resubmitted the updated evaluation of the proposed change previously submitted as the Enclosure to the letter dated October 26, 2011, Significant Hazards Consideration and Environmental Consideration (essentially the same as submitted by letter dated October 26, 2011), and a change to TS 1.1, "Definitions," to revise the definition of "Channel Operational Test (COT)" resulting from the proposed modifications. The rest of the supplements provided additional information in support of the original request.

2.0 REGULATORY EVALUATION

2.1 Regulatory Criteria

Under 10 CFR 50.90, whenever a holder of a license wishes to amend the license, including technical specifications in the license, an application for amendment must be filed, fully describing the changes desired. Under 10 CFR 50.92(a), determinations on whether to grant an applied-for license amendment are to be guided by the considerations that govern the issuance of initial licenses or construction permits to the extent applicable and appropriate. Both the common standards for licenses and construction permits in 10 CFR § 50.40(a), and those specifically for issuance of operating licenses in 10 CFR 50.57(a)(3), provide that there must be 'reasonable assurance' that the activities at issue will not endanger the health and safety of the public.

The U.S. Nuclear Regulatory Commission's (NRC's) NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR [Light-Water Reactor] Edition," Chapter 7, "Instrumentation and Controls," March 2007 (Reference 40), defines the acceptance criteria for this review. Standard Review Plan (SRP) Chapter 7 addresses the requirements for instrumentation and control (I&C) systems in light-water nuclear power plants. The procedures for reviewing a reactor trip system (RTS) and engineered safety feature actuation system (ESFAS), such as the digital process protection system (PPS) of this license amendment request (LAR), are identified in SRP Chapter 7, Table 7-1, Sections 7.2, 7.3, 7.8, and 7.9, and Appendices 7.1-C, "Guidance for Evaluation of Conformance to IEEE STD 603," March 2007 (Reference 41), and 7.1-D, "Guidance for Evaluation of the Application of IEEE STD 7-4.3.2," March 2007 (Reference 42); and SRP Branch Technical Position (BTP) 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips" (Reference 43), BTP 7-11, "Guidance on Application and Qualification of Isolation Devices" (Reference 44), BTP 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints" (Reference 45), BTP 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems" (Reference 46), BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions" (Reference 47), BTP 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems" (Reference 48), BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" (Reference 49), and BTP 7-21, "Guidance on Digital Computer Real-Time Performance" (Reference 50). The NRC staff considered the codes, criteria, and standards included in the SRP guidelines and criteria to evaluate the digital PPS. Standard Review Plan (SRP) Chapter 18, Revision 2, "Human Factors Engineering" (Reference 51), provides guidance for areas of human factors engineering review.

The suitability of a digital platform for use in safety systems depends on the quality of its components; quality of the design process; and system implementation aspects such as real-time performance, independence, and online testing. Because this equipment is being supplied as Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, Appendix B, qualified equipment, the NRC staff evaluated the licensee's submittals in accordance with the provisions of IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Reference 32), and IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33), as well as the guidance contained in SRP Chapter 7 as noted above.

As discussed in Section 3.1 of the "Diablo Canyon Power Plant, Units 1 and 2, Final Safety Analysis Report Update, Revision 22" (FSARU), May 2015 (Reference 52), the DCPP units are, with certain exceptions, licensed to the Atomic Energy Commission's proposed General Design Criteria (GDC) for Nuclear Power Plant Construction Permits, published in July 1967 (32 FR 10213). The DCPP licensing basis includes the following criteria that were promulgated into the Commission's regulations in 1971 (Final Rule, General Design Criteria for Nuclear Power Plants, 36 FR 3256, February 20, 1971, as amended at 36 FR 12733, July 7, 1971): Criterion 3 (Fire Protection), Criterion 17 (Electric Power Systems), Criterion 18 (Inspection and Testing of Electrical Systems), and Criterion 19 (Control Room). The licensing basis also includes Criterion 4 (Environmental and Dynamic Effects Design Bases) as codified in 1987 (Final Rule, Modification of General Design Criterion 4 Requirements for Protection Against Dynamic Effects of Postulated Pipe Ruptures, 52 FR 41294, October 27, 1987). Table 3.1-2 of the DCPP FSARU includes a matrix listing of the 10 CFR 50, Appendix A of the GDC 1971 criterion and the related DCPP licensing basis GDC criterion. This license amendment was evaluated against these DCPP licensing basis GDC criterion to ensure compliance to the DCPP licensing basis is maintained.

Acceptance criteria for the review of the RTS and ESFAS, which include the DCPP PPS, are based on meeting the relevant requirements of the following Commission regulations:

1. 50.55(i) requires that the structures, systems, and components subject to the codes and standards in 10 CFR 50.55a must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

2. 10 CFR 50.55a(h) requires that protection systems of nuclear power reactors must meet the requirements specified in the 50.55a(h). For nuclear power plants with construction permits issued before January 1, 1971 (such as DCPP Unit 1 and Unit 2), protection systems must be consistent with their licensing basis or may meet the requirements IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Reference 32).

3. 10 CFR 50.36(c) requires that technical specifications include items in specified categories. Among the categories are llimiting conditions for operation, which are the lowest functional capability or performance levels of equipment required for safe operation of the facility. When a limiting condition for operation of a

nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the technical specifications until the condition can be met. Also among the categories are surveillance requirements, which are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

4. 10 CFR 50.57(a) states the required findings the Commission must make to issue an operating license.

5. 10 CFR 50.62(c)(1) requires that each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an anticipated transient without scram (ATWS). This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

6. 10 CFR 50.120, “Training and qualification of nuclear power plant personnel,” requires in part that each holder of an operating license shall establish, implement, and maintain a training program that meets the requirements of paragraphs 10 CFR 50.120(b)(2) and (b)(3).

7. Under the provisions of 10 CFR 50.34, an application for a construction permit must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. The GDC in Appendix A to 10 CFR Part 50 establish minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have been issued by the Commission. The following GDCs were considered during the evaluation of this LAR. Numbers shown in parentheses indicate the associated 1967 GDC as presented in Section 3.1.4 of the DCPP FSARU which remain the licensing basis for DCPP, Units 1 and 2.

    a. GDC 1 (1), “Quality standards and records.”
    b. GDC 2 (2), “Design basis for protection against natural phenomena.”
    c. GDC 4 (40), “Environmental and dynamic effects design basis.”
    d. GDC 14 (9), “Reactor coolant pressure boundary.”
    e. GDC 10 (6), “Reactor design.”
    f. GDC 13 (12), “Instrumentation and control.”
    g. GDC 15 (9), “Reactor coolant pressure boundary.”

h. GDC 16 (10 & 49), "Containment system design."

i. GDC 19 (11), "Control room."

j. GDC 20 (14, 15, 20, 21, and 25), "Protection system functions."

k. GDC 21 (19), "Protection system reliability and testability."

l. GDC 22 (20, 21, 22, and 23), "Protective system independence."

m. GDC 23 (26), "Protection system failure modes."

n. GDC 24 (22), "Separation of protection and control systems."

o. GDC 25 (31), "Protection system requirements for reactivity control malfunctions."

p. GDC 29 (19 and 20), "Protection against anticipated operational occurrences."

q. GDC 33 (44), "Emergency core cooling systems capability."

r. GDC 34 (44), "Emergency core cooling systems capability."

s. GDC 35 (37 and 44), "Emergency core cooling."

t. GDC 38 (49 and 52), "Containment heat removal."

u. GDC 41 (37), "Containment atmosphere cleanup."

v. GDC 44 (44), "Emergency core cooling systems capability."

The following additional NUREGs also provide guidance for performing human factors engineering reviews:

- NUREG-1764, Revision 1, "Guidance for the Review of Changes to Human Actions," September 2007 (Reference 54).

- NUREG-0700, Revision 2, "Human-System Interface Design Review Guidelines," May 2002 (Reference 55). The U.S. Nuclear Regulatory Commission (NRC) staff reviews the human factors engineering (HFE) aspects of nuclear power plants in accordance with the Standard Review Plan (NUREG-0800). Detailed design review procedures are provided in the HFE Program Review Model (NUREG-0711). As part of the review process, the interfaces between plant personnel and plant's systems and components are evaluated for conformance with HFE guidelines. This document, Human-System Interface Design Review Guidelines (NUREG-0700, Revision 2), provides the guidelines necessary to perform this evaluation. The review guidelines address the physical and functional characteristics of human-system interfaces (HSIs). Since these guidelines only address the HFE aspects of design and not other related considerations, such as instrumentation and control and structural design, they are referred to as HFE guidelines. In addition to the review of actual HSIs, the NRC staff can use the NUREG-0700 guidelines to evaluate a design specific HFE guidelines document or style guide. The HFE guidelines are organized into four basic parts, which are divided into sections. Part I contains guidelines for the basic HSI elements: displays, user-interface interaction and management, and controls. These elements are used as building blocks to develop HSI systems to serve specific functions. Part II contains the guidelines for reviewing six such systems: alarm system, group-view display system, soft control system, computer-based procedure system, computerized operator support system, and communication system. Part III provides guidelines for the review of workstations and workplaces. Part IV provides guidelines for the review of HSI support (i.e., maintainability of digital systems).

- NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," November 2012 (Reference 56). This document is used by the NRC staff to review the HFE programs of applicants for construction permits, operating licenses, standard design certifications, combined operating licenses, and license amendments. The purpose of these reviews is to verify that the applicant's HFE program incorporates HFE practices and guidelines accepted by the staff as described within the 12 elements of an HFE program: HFE Program Management, Operating Experience Review, Functional Requirements Analysis and Function Allocation, Task Analysis, Staffing and Qualifications, Treatment of Important Human Actions, Human-System Interface Design, Procedure Development, Training Program Development, Human Factors Verification and Validation, Design Implementation, and Human Performance Monitoring. Each element encompasses five sections: Background, Objective, Applicant Products and Submittals, Review Criteria, and Bibliography.

NRC Information Notice (IN) 97-78, "Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times," dated October 23, 1997 (Reference 57), was also considered.

2.2 Regulatory Guidance

The NRC staff considered the following applicable Regulatory Guides (RGs) in its evaluation of the DCPP digital PPS:

- RG 1.22, Revision 0, "Periodic Testing of Protection System Actuation Functions," February 1972 (Reference 58). This safety guide describes acceptable methods of including the actuation devices in the periodic tests of the protection system during reactor operation.

- RG 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," February 2010 (Reference 59). This guide describes a method that the staff of the NRC considers acceptable for use in complying with the NRC's regulations with respect to a bypassed and inoperable status indication for nuclear power plant safety systems.

- RG 1.53, Revision 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," November 2003 (Reference 60). RG 1.53, Revision 2 endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 61).

- RG 1.62, Revision 1, "Manual Initiation of Protection Action," June 2010 (Reference 62). This guide describes a method that the staff of the NRC considers acceptable for use in complying with the NRC's regulations with respect to the means for manual initiation of protective actions provided (1) by otherwise automatically initiated safety systems or (2) as a method diverse from automatic initiation.

- RG 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems," February 2005 (Reference 63). RG 1.75, Revision 3 endorses IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 64).

- RG 1.89, Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," June 1984 (Reference 65). RG 1.89, Revision 1 endorses IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 66).

- RG 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation," December 1999 (Reference 67). RG 1.105, Revision 3 endorses Part 1 of Instrument Society of America ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation" (Reference 68).

- RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," April 1995 (Reference 69). RG 1.118, Revision 3 endorses IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems" (Reference 70).

- RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011 (Reference 71). RG 1.152, Revision 3 endorses IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations") (Reference 33).

- RG 1.153, Revision 1, "Criteria for Safety Systems," June 1996 (Reference 72). RG 1.153, Revision 1 endorses IEEE Std. 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet dated January 30, 1995 (Reference 32).

- RG 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013 (Reference 73). RG 1.168, Revision 2 endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74), and IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits" (Reference 75).

- RG 1.169, Revision 0, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 76). RG 1.169, Revision 0 endorses IEEE Std. 828-1990, "IEEE Standard for Software Configuration Management Plans" (Reference 77), and IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management" (Reference 78).

- RG 1.170, Revision 0, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013 (Reference 79). RG 1.170, Revision 0 endorses IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation" (Reference 80).

- RG 1.171, Revision 0, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 81). RG 1.171, Revision 0 endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing" (Reference 82).

- RG 1.172, Revision 0, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 83). RG 1.172, Revision 0 endorses IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications" (Reference 84).

- RG 1.173, Revision 0, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 85). RG 1.173, Revision 0 endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Reference 86).

- RG 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," October 2003 (Reference 87). RG 1.180, Revision 1 endorses IEEE Std. 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations" (Reference 88); and portions of U.S. Department of Defense MIL-Std.-461E-1999, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment" (Reference 89); International Electrotechnical Commission IEC 61000-3, "Electromagnetic Compatibility (EMC) - Part 3: Limits," IEC 61000-4, "Electromagnetic Compatibility (EMC) - Part 4: Testing and Measurement Techniques," and IEC 61000-6, "Electromagnetic Compatibility (EMC) - Part 6: Generic Standards" (Reference 90); IEEE Std. C62.41-1991, "IEEE Recommended Practice on Surge Voltages in Low-Voltage AC [Alternating Current] Power Circuits" (Reference 91); and IEEE Std. C62.45-1992, "IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits" (Reference 92).

- RG 1.209, Revision 0, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," May 2007 (Reference 93). RG 1.209, Revision 0 endorses IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," subject to the five enhancements and exceptions (Reference 94).

Industry standards, documents, and reports use the word "requirements" to denote provisions that must be implemented to ensure compliance with the corresponding document. Additionally, these standards, documents, and reports provide guidance or recommendations that need not be adopted by the user to ensure compliance with the corresponding document, and the optional items are not designated as "requirements." The word "requirement" is used throughout the I&C discipline. However, licensee or vendor documentation of conformance to the "requirements" provided in industry standards, documents, and reports referenced in this safety evaluation only constitutes conformance with NRC regulatory requirements insofar as endorsed by the NRC (e.g., an RG). Furthermore, use of the word "requirements" in these documents does not indicate that "requirements" are NRC regulatory requirements.

In addition to the guidelines and criteria in NUREG-0800, the NRC staff used ISG-04 (Reference 34) and ISG-06 (Reference 24).

2.3 Precedents

The NRC has approved two digital applications in safety-related systems at nuclear stations that provide precedence for this licensing application. The main steam and feedwater isolation system control system, which is actuated by the solid state protection system (SSPS) at Wolf Creek Generating Station, was approved by NRC letter dated March 31, 2009 (Reference 95). This application was implemented using field programmable gate array (FPGA)-based Advanced Logic System (ALS) platform, developed by CS Innovations (CSI), currently Westinghouse Electric Company (WEC), which was a first-of-a-kind safety system application for this technology within the nuclear industry. Also, by letter dated January 28, 2010 (Reference 96), the NRC staff approved a digital upgrade of the reactor protection system (RPS) and engineered safeguard protective system at the Oconee Nuclear Station (Oconee), Units 1, 2, and 3. The Oconee application was based on an approved generic safety evaluation report for the TELEPERM XS platform and Duke Energy was required to address a set of plant-specific action items for the Oconee plant-specific application of the TELEPERM XS system to address the differences between its plant-specific application and the generically approved system.

The Pacific Gas and Electric Company (PG&E) PPS replacement LAR is based on an approved generic topical report for the Tricon V10 platform and WEC ALS FPGA platform. PG&E addressed the plant-specific action items listed in the NRC staff's safety evaluations for those platforms and the staff approved these changes accordingly (see Section 3.13, "Plant-Specific Action Items Identified in Platform Topical Report Safety Evaluations," of this safety evaluation).

3.0 TECHNICAL EVALUATION

3.1 System Description

As mentioned before, the replacement digital process protection system (PPS) is based on the Invensys Operations Management (IOM) Tricon Programmable Logic Controller (PLC), Version 10 (Tricon V10), and the Westinghouse Electric Company (WEC, formerly developed by CS Innovations) Advanced Logic System (ALS) platform. The PPS performs the process protection functions for the reactor protection system (RPS). This includes monitoring selected plant parameters and initiation of protective actions as required.

The protective functions initiated by the PPS are broadly classified into the following two categories:

- Tripping of the reactor by the reactor trip system (RTS), and
- Actuation of engineered safety features by the engineered safety features actuation system (ESFAS).

The design basis of the PPS is to actuate the RTS reactor trip and/or the ESFAS safety functions when necessary to:

- Prevent core damage from an anticipated transient,
- Limit core damage from infrequent faults,
- Preserve the integrity of the reactor coolant system (RCS) pressure boundary during limiting fault conditions, and
- Limit site radiological releases to acceptable limits.

3.1.1 Reactor Trip System

The purpose of the RTS is to 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.

The conditions requiring a reactor trip to prevent core damage are as follows:

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

In addition, a manual reactor trip, a reactor trip on manual or automatic safety injection, and a hardware problem-related reactor trip are provided by the RTS.

3.1.1.1 Reactor Trip System Variables

The RTS monitors the following process variables to determine the existence of conditions requiring initiation of a reactor trip:

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 under voltage, bus under frequency, 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

Not all of these process variables are being modified by the PPS upgrade. Those process variables marked with an "*" are not monitored by the PPS and therefore will not be affected by the PPS upgrade. These variables provide direct signal inputs to the solid state protection system (SSPS) with no interface with or reliance on the PPS.

The PPS compares process variables to setpoints and provides signals to the SSPS if established setpoints are exceeded. 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 which could lead to release of radioactive fission products. Coincidence logic functions for the RTS actuation are performed by the SSPS which is not being modified under this license amendment request (LAR).

3.1.1.2 Solid State Protection System Description (Not Within PPS Replacement Scope)

Even though the SSPS is not being modified by the PPS replacement project, the following description is provided to facilitate an understanding of the integral functions the SSPS system performs in conjunction with the PPS to complete reactor trip and ESFAS functions.

The SSPS evaluates the reactor trip and ESFAS actuation signals and performs coincidence logic to initiate RTS and ESFAS functions which are designed to mitigate abnormal operational occurrences and design basis events described in Chapter 15, "Accident Analyses," of the DCPP Final Safety Analysis Report Update (FSARU) (Reference 52). The SSPS is composed of two redundant, essentially identical trains (A and B). These trains are physically and electrically separated from each other.

The SSPS receives inputs from nuclear instrument system, PPS, seismic instrumentation, and field sensor generating initiation signals. Additional redundant inputs enter the SSPS logic directly from the control board switches and pushbuttons. The SSPS logic provides automatic reactor trip signals to the reactor trip switchgear. The SSPS generates actuation signals to the reactor trip 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 to actuate the engineered safety features. Information concerning the PPS status is transmitted to the control board status lamps and annunciators by way of the SSPS control board de-multiplexer. The SSPS provides isolated signals to the computer and the control board by way of de-multiplexers.

3.1.1.3 Reactor Trip Switchgear (Not Within PPS Replacement Scope)

Even though the reactor trip switchgear is not being modified by the PPS replacement project, the following description is provided to facilitate an understanding of the integral functions the reactor trip switchgear performs in conjunction with the PPS to complete the reactor trip function.

When the reactor trip switchgear receives a reactor trip signal from the SSPS, it de-energizes the reactor trip breaker undervoltage coils and energizes shunt trip mechanisms to open the reactor trip breakers. Opening of the reactor trip breakers removes power to the control rod drive mechanisms permitting the control rods to fall by gravity into the reactor core. The insertion of control rods rapidly inserts negative reactivity.

3.1.2 Engineered Safety Features Actuation System

The ESFAS actuates engineered safety features equipment that performs protective actions to mitigate the consequences of postulated accidents. The ESFAS has the capability of sensing plant conditions requiring the initiation of the engineered safety features. The engineered safety features act to limit the consequences of faulted conditions in the plant. The ESFAS automatically provides output signals for the timely actuation of the various ESFAS functions, consistent with the design bases of these systems. The conditions requiring actuation of engineered safety features 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
   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
   d. Loss of offsite alternating current power
   e. Feedwater malfunction (excessive feedwater flow accidents)

3.1.2.1 Engineered Safety Features Actuation System Variables

The PPS develops signals used to initiate engineered safety features. The following process variables are directly used by the ESFAS for the purpose of initiating engineered safety features functions when required based on plant conditions.

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. *Reactor trip breaker position (permissive P-4) (generated outside the PPS)

Not all of these process variables are being modified by the PPS upgrade. The process variables marked with an asterisk "*" are not monitored by the PPS and, therefore, will not be affected by the PPS upgrade. These variables provide direct signal inputs to the SSPS with no interface or reliance on the PPS.

The PPS compares process variables to setpoints and provides ESFAS actuation signals to the SSPS if pre-established setpoints are exceeded. Upon coincidence that multiple directly measured process or calculated variables exceed setpoints, engineered safety features safety functions are actuated to mitigate abnormal operational occurrences and design basis events addressed by Chapter 15, "Accident Analyses," of the DCPP's FSARU. Abnormal operational occurrences are referred to as American Nuclear Society (ANS) Condition I, "operational transients," in FSARU Chapter 15 and are addressed in FSARU Chapter 15.1, "Condition I - Normal Operation and Operational Transients." 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 FSARU Chapters 15.2, 15.3, and 15.4, respectively. Coincidence logic functions for the ESFAS actuation functions are performed by the SSPS which is not being modified under this LAR.

3.1.2.2 ESFAS Functions

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

1. Safety injection actuation
2. Turbine trip
3. Containment spray
4. Containment isolation Phase A
5. Containment isolation Phase B
6. Containment ventilation isolation
7. Main steam isolation
8. Main feedwater isolation
9. Auxiliary feedwater initiation

The low steamline pressure, the low pressurizer pressure, or the high containment pressure protection functions initiate safety injection actuation and a subsequent reactor trip. Safety injection actuation initiates an "S" safety signal, feedwater isolation, containment Phase A isolation, and containment ventilation isolation. Feedwater isolation, containment Phase A isolation, and containment ventilation isolation 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.

3.1.3 Additional Plant Process Protection System Functions

3.1.3.1 Additional Inputs to the PPS

The following are process variable input signals to the PPS which are not associated with either the RTS or the ESFAS functions described above.

- Wide Range RCS Temperature - The wide range RCS temperature signals are used to generate the low temperature overpressure protection function. This function is described below.

- Wide Range RCS Pressure - The wide range RCS pressure signals are used to generate the low temperature overpressure protection function.

- Turbine Impulse Chamber Pressure - The PPS uses turbine impulse chamber pressure to generate an initiation signal used by the SSPS coincidence logic to develop permissive P-13. See Section 3.1.3.5, “Pressurizer Pressure Protection Functions (Function of the ALS Portion of the PPS System),” of this safety evaluation.

The low temperature overpressure protection function provides RCS overpressure protection during startup and shutdown, which consists of two mutually redundant and independent systems. The low temperature overpressure protection functions are performed in the auxiliary safeguards rack and are independent of the SSPS. Each system receives reactor coolant pressure and temperature signals from the PPS. When a low-temperature, high-pressure transient occurs, it opens a pressurizer power-operated relief valve until the pressure returns to within acceptable limits. During normal operation, the low temperature overpressure protection system is off. If the reactor coolant temperature is below the low-temperature setpoint and the enable switch on the main control board is not in the enable position, an alarm is actuated in the main control room. The operator can then enable the circuit before a water-solid condition is reached, and the system is then ready to operate without further operator action.

3.1.3.2 Nuclear Instrument System Protection Function

The nuclear instrument system is independent of the PPS. The nuclear instrument system provides three overlapping protection functions. These include: source range nuclear instrument system protection, intermediate nuclear instrument system protection, and power range nuclear instrument system protection. The PPS is only used in conjunction with the power range nuclear instrument system input to the thermal over temperature and overpower protection functions described in Section 3.1.3.3 below.

3.1.3.3 Thermal Over Temperature and Overpower Protection Function (Function of the Tricon Portion of the PPS)

The thermal over power and over temperature protection functions ensure fuel integrity is maintained by initiating two reactor trip functions: the thermal over power trip (also known as over power ΔT, OPΔT, or OPDT) and the thermal over temperature trip (also known as over temperature ΔT, OTΔT, or OTDT).

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

The thermal over temperature trip function is provided to ensure operation within the departure from nuclear boiling design basis and to ensure operation within the hot-leg boiling limit.

The over temperature ΔT function trips the reactor when 2-out-of-4 over temperature ΔT channels are above the trip setpoint.

Reactor coolant system (RCS) temperature signals used for the OPDT and OTDT functions are processed through the ALS portion of the PPS and then sent to the Tricon portion of the PPS through analog signal (4-20 milliampere (mA)) connections between the two systems. The OPDT and OTDT functions are performed by the Tricon portion of the PPS.

3.1.3.4 T_{ave} Signal Processing (Function of the Tricon Portion of the PPS)

The RCS temperature signals are used to generate the average reactor coolant temperature (T_{ave}) signal. A low T_{ave} signal isolates the main and bypass feedwater regulating valves. A low-low T_{ave} signal actuated permissive P-12. A description of permissive P-12 low-low T_{ave} steam dump block is provided in Section 3.1.3.12, “Protection Functions Associated with Steam Dump Control System,” of this safety evaluation.

3.1.3.5 Pressurizer Pressure Protection Functions (Function of the ALS Portion of the PPS)

The pressurizer pressure channels perform the following protection functions:

1. Provide a high pressurizer pressure reactor trip function to prevent over pressurization of the RCS.

2. Provide a low pressurizer pressure reactor trip function to limit core boiling.

3. Provide a low pressurizer pressure safety injection system actuation for loss-of-coolant accidents and steamline break protection.

4. Provide power-operated relief valve automatic actuation signal to prevent RCS pressurizer overfill without challenging the pressurizer safeties for inadvertent safety injection at power.

5. Generate pressurizer safety injection permissive P-11. See 3.1.3.15, “PPS System Permissive Functions,” of this safety evaluation.

The pressurizer pressure signals are used as an input to the OTΔT and OPΔT setpoints described in Section 3.1.3.3, “Thermal Over Temperature and Overpower Protection Function (Function of the Tricon Portion of the PPS),” of this safety evaluation. In addition, the low temperature overpressure protection uses wide-range RCS pressure measurement channels, which open the pressurizer’s power-operated relief valves when an overpressure condition exists while the reactor is at low temperature. This protection function is performed in the auxiliary safeguards rack and is not within the scope of the PPS replacement project.

The high pressurizer pressure reactor trip 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 reactor trip 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 reactor trip is automatically blocked when low-power permissive P-7 is cleared; however, this permissive function is not performed within the PPS. A description of the P-7 function is provided in Section 3.1.5, "Related Functions Not Performed by PPS," of this safety evaluation.

The low pressurizer pressure safety injection actuation provides protection in the event of a loss-of-coolant accident or steamline break. The low pressurizer pressure safety injection actuation setpoint is lower than the setpoint for low pressurizer pressure reactor trip discussed previously. The pressurizer pressure function actuates safety injection when 2-out-of-4 pressurizer pressure channels are less than the actuation setpoint.

The low pressurizer pressure safety injection actuation is interlocked with pressurizer safety injection permissive P-11. See Section 3.1.3.15, "PPS System Permissive Functions," of this safety evaluation for a description of the permissive P-11 function.

3.1.3.6 Pressurizer Level Protection Function (Function of the Tricon Portion of the PPS)

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 function is performed by protection sets I, II, and III. The high pressurizer water level trip is automatically blocked when low-power permissive P-7 is cleared. The P-7 permissive function is not performed within the PPS; however, it is described in Section 3.1.5, "Related Functions Not Performed by PPS," of this safety evaluation.

3.1.3.7 Reactor Coolant Loop Low Flow Protection Function (Function of the ALS Portion of the PPS)

The primary reactor coolant loop low-flow protection function is designed to protect the core from exceeding departure from nucleate boiling 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 reactor coolant pumps (RCPs), a loss of offsite power, or an RCP bus under frequency. A reactor trip 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 OTΔT trip does not respond fast enough to provide protection for loss-of-coolant flow events.

Each reactor coolant loop has three reactor coolant flow measurement 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. The P-7 and P-8 permissive functions are not performed within the PPS. Further discussion of the P-7 and P-8 permissive functions is provided in Section 3.1.5, "Related Functions Not Performed by PPS," of this safety evaluation.

The P-7 and P-8 permissive functions establish three possible conditions which affect the loss of flow reactor trip function as follows.

1. During low-power operations, when permissive P-7 is cleared, the reactor trip on low-flow function is blocked.
2. In mid-power operation, when power is between the setpoints for permissive functions P-7 and P-8 (only P-7 enabled), a reactor trip 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.
3. During high-power operations, 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.

3.1.3.8 Containment Pressure Protection Functions (Function of the ALS Portion of the PPS)

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 sized loss-of-coolant accidents, steamline breaks, and feedline breaks.

Two containment pressure signals are developed in the ALS portion of PPS and are provided to the solid state protection system (SSPS). These are designated high and high-high in order of increasing containment pressure setpoint.

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

1. Safety injection initiation
2. Reactor trip on a safety injection signal
3. Containment isolation (Phase A actuation)

These containment pressure high protection functions actuate when 2-out-of-3 containment pressure channels exceed the high trip/actuation setpoint. The containment pressure high functions are performed by protection sets II, III, and IV. This coincidence logic is performed by the SSPS and therefore is not impacted by this PPS upgrade LAR.

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)

These containment pressure high-high protection functions actuate 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 safety injection signal to be present concurrently. Manual initiation of containment spray is further discussed in Section 3.1.4, “Manual Initiation Functions,” of this safety evaluation.

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. This is a function of the PPS and is accomplished using manual bypass switches.

3.1.3.9 Steam Generator Level Protection Functions

The steam generator level protection functions prevent loss of reactor heat sink. The following functions are associated with steam generator level.

- Low-Low Steam Generator Level - A reactor trip and auxiliary feedwater actuation, including steam generator blowdown and sample line isolation, are generated on low-low steam generator level. This function actuates when 2-out-of-3 steam generator level channels read below the low-low trip/actuation setpoint in one or more of the four 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 calculated in the PPS using a 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 below 50 percent power determined from reactor coolant ΔT. The TTD is zero when power is at 50 percent or above.

- High-High Steam Generator Level (P-14) - The steam generator high-high level protection function provides a turbine trip and feedwater isolation when 2-out-of-3 steam generator channels in one or more of the four steam generators increase 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. See Section 3.1.3.15, "PPS Permissive Functions," of this safety evaluation for additional discussion of the P-14 permissive signal.

3.1.3.10 Low Steamline Pressure Protection Function

This protection function actuates steamline isolation and safety injection to provide protection for high energy secondary line breaks. The low steamline pressure protection function actuates steamline isolation and safety injection when 2-out-of-3 rate compensated steamline pressure channels on any steamline read pressure below the low-pressure setpoint. These signals are developed in the PPS. Protection sets I and II perform this function for Loops 1 through 4. Protection set III performs this function for Loops 2 and 3 only while protection set IV performs this function for Loops 1 and 4 only. The low steamline pressure protection function may be manually blocked by the P-11 permissive function. See Section 3.1.3.15, "PPS Permissive Functions," of this safety evaluation for a description of the P-11 permissive function. Blocking the low steamline pressure protection function enables the high-negative steamline pressure rate protection function.

3.1.3.11 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. Protection sets I and II perform this function for Loops 1 through 4. Protection set III performs this function for Loops 2 and 3 only while protection set IV performs this function for Loops 1 and 4 only. The high-negative steamline pressure rate steamline isolation function is permitted when the low steamline pressure protection function is manually blocked.

3.1.3.12 Protection Functions Associated with Steam Dump Control System

This protection function blocks steam dump on low-low T_{ave} (P-12) to prevent excessive cool down 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_{ave} below the P-12 setpoint. The P-12 setpoint is set below the no-load T_{ave} 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 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 cool down. 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.

3.1.3.13 Turbine-derived Protection Function

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

1. Reactor trip on turbine trip (developed independently of the PPS). See Section 3.1.3.15, "PPS Permissive Functions," of this safety evaluation for a description of this function.
2. Turbine impulse chamber pressure input to turbine low-power permissive.
3. P-13 (developed in the PPS). See Section 3.1.3.15 of this safety evaluation for a description of the P-13 permissive function.

3.1.3.14 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 containment ventilation isolation signal is initiated. During Modes 1-4, the containment ventilation isolation signal is generated in the SSPS. During refueling Mode 6, when the SSPS may be de-energized, means are provided to generate the containment ventilation isolation signal independently of the normal SSPS power supply.

3.1.3.15 PPS Permissive Functions

<u>P-11 Low Pressurizer Pressure Safety Injection Operational Bypass</u>

The P-11 permissive signal allows the operator to manually block the low pressurizer pressure safety injection actuation and enable high negative steamline pressure rate steamline isolation actuation at low reactor coolant pressures.

The P-11 signal is generated by 2-out-of-3 pressurizer pressure channels reading below the permissive setpoint. The bistable functions for P-11 are performed by the Advanced Logic

System (ALS) subsystem in protection sets I, II, and III. The actuation logic is performed by the SSPS system. Typically, low pressurizer pressure safety injection is manually blocked during cool down and depressurization of the reactor coolant system (RCS). The block may be manually removed for return to normal operation. The manual low pressurizer pressure safety injection block is automatically removed when the pressurizer pressure signals rise above the P-11 setpoint. Clearing of the P-11 signal also opens the safety injection accumulator isolation valves. The setpoint for the P-11 permissive function is not being changed during the PPS replacement modification.

P-12 Low-Low T_{ave} Steam Dump Block

Permissive P-12 is enabled when 2-out-of-4 average reactor coolant temperature (T_{ave}) channels read below the low-low T_{ave} setpoint. The P-12 setpoint is set below the no-load T_{ave} temperature. Permissive P-12 blocks closed all steam dump valves. See Section 3.1.3.12, "Protection Functions Associated with Steam Dump Control System," of this safety evaluation for a more detailed description of the steam dump control system protection functions associated with this permissive. The setpoint for the P-12 permissive function is not being changed during the PPS replacement modification.

P-13 Turbine Low Power Permissive

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 which is a function performed by the SSPS. Permissive P-13 is developed from 2-out-of-2 turbine impulse chamber pressure channels below the P-13 setpoint. The setpoint for the P-13 permissive function is not being changed during the PPS replacement modification.

P-14 High-High Steam Generator Level Turbine Trip – Feedwater Isolation

Permissive P-14 is enabled when 2-out-of-3 steam generator level channels are above the high-high P-14 setpoint in one or more steam generators or when a safety injection signal is initiated. See Section 3.1.3.9, "Steam Generator Level Protection Functions," of this safety evaluation for a more detailed description of the steam generator level protection functions associated with this permissive.

The feedwater isolation is accomplished by closing the main, feedwater control valves, the bypass feedwater control valves, and by tripping the feedwater pumps. The feedwater isolation valve closure function is performed by train A and the feedwater pump trip function is performed by train B. When feedwater control valve and bypass control valve closure on a safety injection signal or high-high steam generator level (P-14) occurs coincident with reactor trip, the valve closure signal is latched-in by a feedback signal. This latched-in function is designed to comply with the criteria of IEEE Std. 603-1991, Section 5.2 (Reference 32), 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.

Feedwater control valve and bypass control valve closure is also initiated by low T_{ave} coincident with reactor trip (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. The setpoint for the P-14 permissive function is not being changed during the PPS replacement modification.

3.1.4 Manual Initiation Functions

Manual Reactor Trip

The function of the existing manual reactor trip is to trip the reactor without using the automatic reactor trip circuitry. The manual reactor trip is accomplished by actuating open a normally closed contact wired-in series between the solid state protection system (SSPS) output logic and the reactor trip switchgear. This interrupts power to the trip breaker and bypass breaker undervoltage coils, resulting in a reactor trip. In addition, a shunt trip relay is wired in parallel for each reactor trip 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 reactor trip in both trains. The manual reactor trip control at the control console is equipped with a momentary reset position for resetting the reactor trip breakers. Resetting the reactor trip breakers is not a safety-related function. The reset switch is required for reactor restart.

Manual Safety Injection

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

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.

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 containment ventilation isolation. Redundant contacts allow either control to initiate these functions in both trains. These controls are electrically downstream of PPS initiations.

Manual Containment Spray

The existing manual containment spray function has special functions designed to reduce the risk of inadvertent containment spray while still meeting single failure criteria.

Manual containment spray actuation requires actuation of two manual switches simultaneously. 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 containment ventilation isolation and containment Isolation Phase B only. An interlocking automatic or manual safety injection actuation signal must be present to manually initiate a containment spray. Redundant contacts allow either pair of controls to initiate these functions in both trains. These controls are electrically downstream and independent of the PPS initiations.

3.1.5 Related Functions Not Performed by PPS

Even though the following functions are not within the scope of the PPS modification being evaluated, these descriptions are provided to facilitate an understanding of the integral relationships existing between these functions and the PPS.

RCP Bus Under Frequency Protection Function (Not Within PPS Replacement Scope)

The reactor coolant pump (RCP) bus under frequency reactor trip is a protective function used to protect the core from exceeding departure from nuclear boiling limits during loss of reactor coolant flow due to a grid under frequency condition. The under frequency trip is interlocked with low power permissive P-7 so the trip signal is blocked when P-7 is cleared. This function is performed independently of the PPS and therefore is not within the scope of this evaluation.

RCP Bus UV Protection Function (Not Within PPS Replacement Scope)

The RCP bus undervoltage (UV) protection function is to protect the core from exceeding departure from nuclear boiling limits during loss of reactor coolant flow by tripping the reactor. The UV trip is interlocked with low power permissive P-7 so the trip signal is blocked when permissive P-7 is cleared. This function is performed independently of the PPS and therefore is not within the scope of this evaluation.

RCP Breaker Position Protection Function (Not Within PPS Replacement Scope)

The RCP breaker position protection function is provided to protect the core from exceeding departure from nuclear boiling limits during loss of reactor coolant flow by tripping the reactor. This function is performed independently of the PPS and therefore is not within the scope of this evaluation.

Seismic Acceleration Reactor Trip Function (Not Within PPS Replacement Scope)

The seismic acceleration trip function provides a reactor trip on seismic accelerometers sensing accelerations exceeding a predetermined setpoint to provide a reactor trip 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 reactor trip is performed. This function is performed independently of the PPS and therefore is not within the scope of this evaluation.

ATWS Mitigating System Actuation Circuitry (Not Within PPS Replacement Scope)

Isolated non-safety-related steam generator narrow-range level and turbine first-stage pressure analog signals are provided to the existing non-safety-related anticipated transient without scram (ATWS) mitigating system actuation circuitry (AMSAC) system. The AMSAC trips the main turbine and initiates auxiliary feedwater flow in the event an 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 auxiliary feedwater pump control circuits. The AMSAC is not safety-related.

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 reactor trip 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 non-safety-related AMSAC input signals are isolated from the safety-related PPS measurement circuits by isolation devices, which are part of the PPS and meet all of the Class 1E requirements for isolators used to prevent control and protection system interaction. The isolators are used to prevent any electrical faults in the AMSAC from affecting the PPS's ability to perform its safety-related functions. The AMSAC output signals are isolated from the actuated devices by output relays. 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 Intel 8086 microprocessor 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 Westinghouse using field programmable gate array (FPGA) architecture and technology and does not use a microprocessor. The

AMSAC input signals are isolated prior to any digital processing by Tricon or ALS PPS components.

Reactor Trip on Turbine Trip Function (Not Within PPS Replacement Scope)

The reactor trip on turbine trip (turbine trip-reactor trip) protects the reactor against loss of heat sink. At power levels above the power range at power permissive (P-9) setpoint, a reactor trip 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. The reactor trip on turbine trip function is blocked when power range at power permissive P-9 is cleared. Turbine trip also generates a non-safety-related generator unit trip.

Low Power Permissive Function (P-7) (Not Within PPS Replacement Scope)

The low power permissive function, also known as permissive P-7, is developed as the logical "OR" of permissive P-10 and permissive P-13. This function blocks the following reactor trip functions when it is cleared at low power levels.

- Low pressurizer pressure,
- High pressurizer level,
- RCP bus under frequency,
- RCP bus under voltage, and
- Low RCS flow

Settings of the bistable comparators used to develop the permissive functions are not affected by the PPS replacement project.

Loss of Flow Permissive Function (P-8) (Not Within PPS Replacement Scope)

The loss of flow permissive function, also known as permissive P-8, serves to change the coincidence logic for the loss of flow reactor trip logic. When disabled and the power level is above the P-7 setpoint, the low flow trip coincidence logic trips the reactor when 2-out-of-4 reactor coolant loops have a low flow signal present. When enabled, the low flow trip coincidence logic trips the reactor when any one of the four reactor coolant loops has a low flow signal present. The loss of flow function is further described in Section 3.1.3.7, "Reactor Coolant Loop Low Flow Protection Function (Function of the ALS Portion of the PPS System)," of this safety evaluation.

Power Range at Power Permissive Function (P-9) (Not Within PPS Replacement Scope)

The power range at power permissive, also known as permissive P-9, is enabled when 2-out-of-4 power range channels are greater than the P-9 setpoint. If power is above the power range at power permissive P-9 setpoint, then the feedwater isolation valve closure (train A) signal, feedwater pump trip (train B) signal, and the turbine trip signal are generated from the output of a retentive memory for the same input signal from steam generator high-high level or safety injection 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. The P-9 setpoint is not affected by the PPS replacement project.

Power Range at Power Permissive (P-10) (Not Within PPS Replacement Scope)

The power range at power permissive, also known as permissive P-10, is enabled when 2-out-of-4 power range channels are greater than the P-10 setpoint.

3.1.6 Process Protection System Hardware Components

The PPS replacement system replaces the Westinghouse Eagle 21 PPS hardware. The new PPS hardware components will be installed into 16 racks in which the current Eagle 21 system resides. System components will be distributed as follows;

• Protection Set A PPS components	Racks 1 through 5	(5)
• Protection Set B PPS components	Racks 6 through 10	(5)
• Protection Set C PPS components	Racks 11 through 13	(3)
• Protection Set D PPS components	Racks 14 through 16	(3)

Each of these protection sets is composed of a Triconex subsystem component and an ALS subsystem component. Each of the PPS functions described in Section 3.1, "System Description," of this safety evaluation is assigned to one of these two PPS subsystems. The allocation of functions to these subsystems was performed based on the following criteria.

- If there were existing diverse and independent automatic functions available to mitigate the effects of a postulated common-cause failure concurrent with FSARU Chapter 15 events, then the function was assigned to the software-based Triconex subsystem.

- If the diversity and defense-in-depth (D3) analysis results did not identify a diverse and independent automatic function and instead determined additional diversity measures were necessary to preclude manual mitigating action, then the function was assigned to the ALS subsystem which contains design features to establish built-in diversity.

The basis for this allocation was the D3 analysis of the PPS, provided in the PG&E "Diablo Canyon Power Plant, Topical Report: Process Protection System Replacement, Diversity & Defense-in-Depth Assessment," Revision 1, August 2010 (Reference 97). The resulting allocation of PPS functions is summarized as follows:

Triconex Subsystem Functions

- Pressurizer high level reactor trip
- Over temperature delta temperature (OTDT) reactor trip
- OPDT reactor trip
- Steam generator low level reactor trip and auxiliary feedwater initiation
- Steam generator high level turbine trip, feedwater isolation, and main feedwater pump trip
- Steam line pressure high negative pressure rate main steam line isolation
- Low steam line pressure main steam line isolation
- Low steam line pressure safety injection
- Turbine impulse pressure permissive

ALS Functions

- Low pressurizer pressure safety injection
- High pressurizer pressure reactor trip
- Low pressurizer pressure reactor trip
- Pressurizer pressure input to OTDT reactor trip function
- High containment pressure safety injection
- High containment pressure Phase A and Phase B containment isolation
- Reactor coolant system low flow reactor trip

3.1.6.1 Tricon Components

Within each protection set, the Tricon subsystem has three layers of redundancy, which is called Triple Mode Redundancy (TMR) from input terminal to output terminal. The TMR configuration is shown in Figure 3.1.6.1-1 of this safety evaluation section.[1] 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 during system operation, without interruption of monitoring, control, or 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

[1] This is Figure 4-7 of the LAR (Reference 12).

dual-redundant mode. The system has the capability of returning to the triple-redundant TMR mode of operation when the affected module is subsequently replaced.

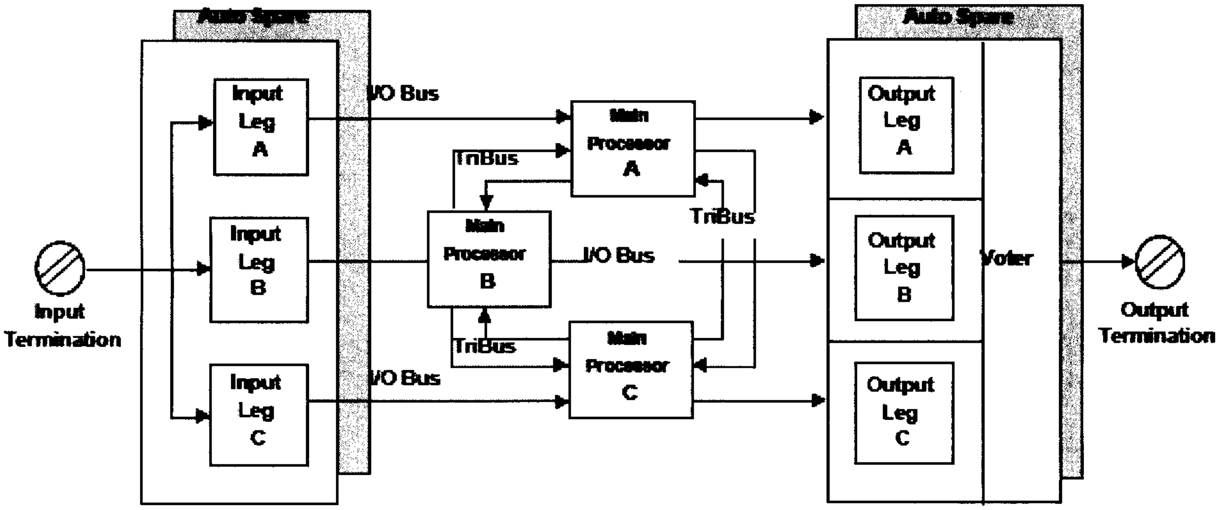


Figure 3.1.6.1-1. Tricon Triple Modular Redundant Architecture

The hardware components of each Tricon subsystem are a main chassis, expansion chassis termination panels, power supply modules, main processor modules, and input/output modules. Each PPS Tricon subsystem within a protection set contains a main chassis, a primary remote extender module (RXM) chassis and an expansion chassis called a remote RXM chassis. Various Tricon modules are installed into these chassis to accomplish the systems input/output, processor, and communications functions.

3.1.6.1.1 Tricon Main Chassis

The main chassis for each subsystem contains a processor module and a communications module. A number of input/output modules are also installed into the main chassis to support the required safety and non-safety signal inputs and outputs. The Tricon Communications Module supports communications with external systems including the Tricon maintenance work station and the process plant computer.

The main chassis has a keyswitch to set the system operating mode. The keyswitch is a four-position, three-ganged switch that allows the three processor modules to monitor the position of the keyswitch independently. The voted position of the keyswitch is available as a read-only system variable that can be monitored by the Test System Application Program (TSAP). This variable can call the function blocks to provide the keyswitch position or the gate enable and gate disable function blocks, which are used as part of the Tricon online maintenance and test features for adjusting selected tunable parameters and modifying setpoints when the keyswitch is in the RUN position, as described in the licensee's letter dated April 30, 2012 (Reference 3). The keyswitch modes are defined as follows;

- 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 computer running the TriStation software, including application program downloads.
- STOP - Stops application program execution.
- REMOTE - Allows writes to application program variables by a TriStation computer or by MODBUS masters and external hosts.

The Tricon keyswitch will be in the RUN position when the Tricon is performing safety-related functions and is not bypassed or manually tripped. When the keyswitch is in PROGRAM or REMOTE, changes to setpoints can be made from the Tricon maintenance work station. The keyswitch must be in the PROGRAM position to accept commands from TriStation 1131 to allow modifying the application program executing on the main processors. However, the PPS protection set is considered inoperable whenever the keyswitch is not in the RUN mode. In addition, if the Tricon keyswitch is not in the RUN position, an alarm is initiated on the control room main annunciator system and the Tricon is considered inoperable.

For the DCPP PPS, the STOP function is disabled in the application software configuration to prevent inadvertent application program halt. By letter dated April 30, 2014 (Reference 17), PG&E explained the reason for disabling the STOP function. PG&E requested this because Invensys recommends disabling the STOP function to prevent inadvertently stopping the program while performing software maintenance functions; this requirement is described in the Triconex Application Guide, Appendix B of the Tricon V10 Topical Report (Reference 26). In its letter dated April 30, 2014, PG&E noted that if necessary to halt operation of the Tricon chassis, the keyswitch can be placed in PROGRAM and the main processor can be halted using the TriStation 1131 program in the Tricon maintenance work station.

During the second Invensys regulatory audit performed June 3-5, 2014 (Reference 38), the NRC staff reviewed the keyswitch design and confirmed its operation. Strict administrative control over the use of the Tricon keyswitches is necessary to ensure operability of the PPS is maintained during system maintenance and surveillance activities. Refer to Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation for associated site inspection follow-up item.

3.1.6.1.2 Tricon Expansion Chassis

An expansion chassis is connected to the main chassis via three separate RS-485 data links, one for each of the three input/output legs. Each main chassis is connected to an expansion chassis containing a primary RXM. Three separate RS-485 data links are required for the three communications busses between the primary RXM and the remote RXM.

The primary RXM supports communications with a second remote expansion chassis used for the handling of non-safety-related signals to external systems. This second remote RXM expansion chassis contains a secondary RXM module to facilitate communications with the primary RXM. The remote RXM chassis is non-safety-related. Figure 3.1.6.1-2 illustrates the chassis and module configurations used for a single protection set of the DCPP PPS.

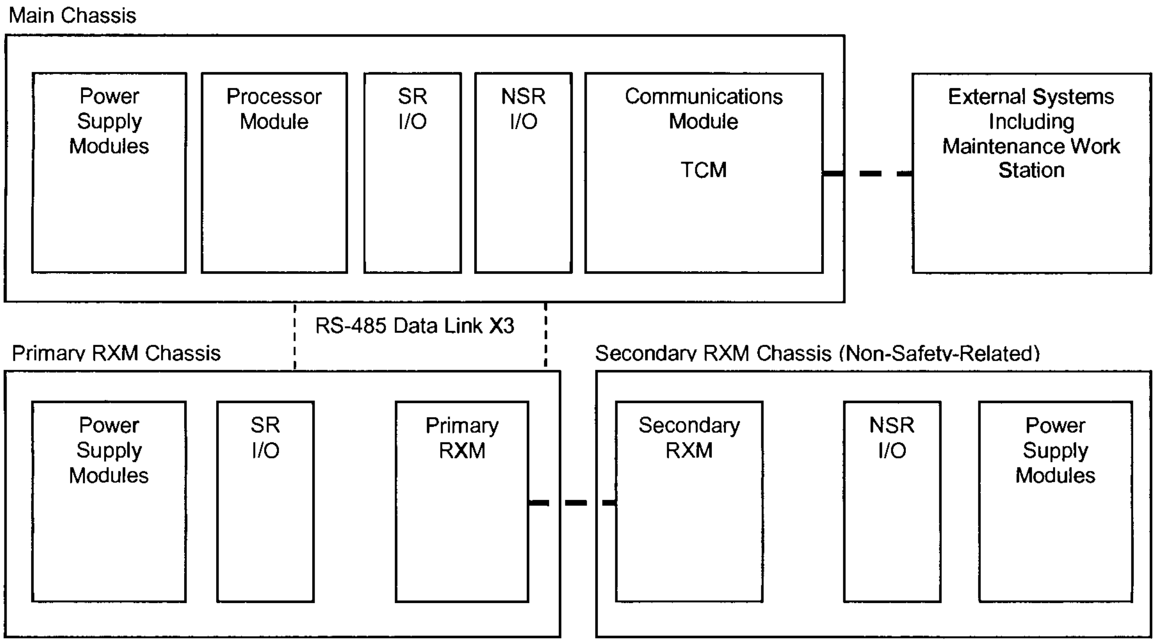


Figure 3.1.6.1-2. Tricon Subsystem Architecture

The Tricon backplanes in the system main and remote RXM extension chassis are designed with dual independent power rails. Both power rails feed each of the three legs on each input/output 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 inserted into the chassis. Each power rail is fed from one of the two power supply modules installed in the chassis. Under normal circumstances, each of the three legs on each input/output 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.

Each Tricon subsystem has dual redundant batteries located on the main chassis backplane. If a power failure occurs within the protection set, then these batteries maintain data and programs on the associated main processor modules for a period of 6 months. The system generates an alarm when the battery power is too low to support the system.

3.1.6.1.3 External Termination Assembly

The external termination assemblies 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 external termination assembly includes an interface cable connecting the termination panel to the Tricon chassis backplane.

3.1.6.1.4 Power Supply

Electrical power for the PPS is supplied by vital uninterruptible alternating current (AC) power from four electrically independent and physically separated 120 Volts alternating current (VAC) distribution panels. Each of these distribution panels is supplied from a separate, dedicated inverter. Each inverter can be fed from a 125 Volts direct current (VDC) vital system or from a 480 VAC vital system. The 125 VDC system is designed with three vital batteries, with each battery having a dedicated charger supplied from a 480 VAC vital bus.

The following table identifies the normal power sources to each PPS protection set:

Protection Set	Vital 120 VAC Bus Unit One (Unit Two)	480 VAC Bus (Normal)	125 VDC Bus
I	PY-11	1F(2F)	SD11(21)
II	PY-12	1G(2G)	SD12(22)
III	PY-13	1H(2H)	SD12(22)
IV	PY-14	1H(2H)	SD13(23)

Table 3.1.6.1.4-1. PPS Power Distribution

Each 480 VAC vital bus is designed to be supplied from the main generator, from the two independent offsite sources or from the onsite diesel generators. Vital inverter loads are normally supplied by the associated 480 VAC bus. When 480 VAC becomes unavailable, the inverter becomes supplied by its associated 125 VDC bus.

Triconex Power Supply Modules

The Triconex PPS subsystem uses two Triconex power supply modules in each chassis. The power supply modules are supplied by redundant uninterruptible 120 VAC safety-related instrument power supply described above. Power supplies in non-safety-related PPS chassis are supplied by Class 1E vital 120 VAC power as well; however, these power supplies are isolated from the safety-related primary power source by qualified circuit breakers.

The power supply modules possess built-in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator light-emitting diodes on the front face of each power module provide module status. The power supply modules also contain the system alarm contacts. The alarm function operates independently for each power module. 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
- Fault of an input/output module in a main or expansion chassis
- System trouble such as a processor or input/output module fault is detected in the main chassis
- Trouble is detected within the module or if its primary power is lost

Each of the three legs on each input/output module and each main processor module normally draws power from both of the associated chassis power supplies through dual power rails and the dual power regulators. If one of the power supplies or its supporting power line fails, the other power supply is designed to increase its power output to support the requirements of the modules in the chassis.

Analog Input Loop Power Supplies

The Tricon subsystem in each protection set is provided with its own pair of safety-related adjustable, redundant loop power supplies, which are capable of powering all 4-20 mA instrument input loops associated with the subsystem. Separate input/output power supplies will be provided and qualified by the licensee during detailed design for the Triconex and ALS subsystems.

Note: The power distribution design portion of the PPS described here was not complete at the time of this safety evaluation. The NRC staff was, however, able to perform a review of the preliminary design in progress during the June 22-26, 2015, Westinghouse audit. The NRC staff confirmed compliance with the PPS functional requirements of the system. Refer to the audit report dated September 2, 2015 (Reference 39), for additional details of this activity.

Triconex Discrete Input/Output Power Supplies

De-energize to trip discrete Triconex outputs to the solid state protection system (SSPS) and auxiliary relays use a 120 VAC 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 VDC power supplies. Other discrete Triconex outputs are powered by the external system.

Triconex discrete inputs are powered by redundant 24 VDC power supplies, except trip output loopback signals, which are powered by the 120 VAC discrete output.

Non-Safety-Related Utility Power

A non-safety-related 120 VAC utility power source is used to supply the following non-safety-related components of the DCPP PPS.

- Port aggregators
- Network switches
- Media converters
- Maintenance work station computers
- Maintenance work station video display units
- Keyboard-video-mouse (KVM) switches
- Utility receptacles

3.1.6.1.5 Tricon Safety Function Processors

The Tricon subsystem within each protection set of the PPS uses three safety-related model main processor modules to control the three separate legs of the system, shown in Figure 3.1.6.1-1. 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 protection set, and each contains two 32-bit processors. One of the 32-bit processors is a dedicated, leg-specific input/output and communication (IOCCOM) microprocessor which processes all communication with the subsystem input/output modules and communication modules. The second 32-bit primary processor manages execution of the control program and all system diagnostics at the main processor module level.

These two processors operate asynchronously, sharing information by means of dual-ported memory dedicated exclusively to this exchange of information. The operating system, run-time library, and fault analysis code for the main processor is fully contained in flash memory on each module. The three main processors within a single protection set communicate with one another through the proprietary, high-speed, voting, bidirectional serial channel. Each main processor has an input/output channel for communicating with one of the three legs of each input/output module. Each main processor has an independent clock circuit and selection mechanism enabling all three main processors to synchronize their operations each scan to allow voting of data and exchange of diagnostic information.

3.1.6.1.6 Tricon Input/Output Modules

As shown in Figure 3.1.6.1-1, Tricon 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 such that same signal input from a single sensor is provided to all three input legs. 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 performed independently. The input/output modules provide three complete signal paths in each leg for all boards used in the PPS replacement, with the exception of the enhanced relay output module 3636T. The enhanced relay output module is simplex (one signal processing path per channel), thus providing data isolation and independence so a component failure in one leg does not affect the signal processing in the other two legs. The enhanced relay output module provides discrete outputs to non-safety-related systems such as the main annunciator system, hence loss of the single leg does not affect a safety function and TMR capability is not required.

Input data are sampled, conditioned, and sent to the main processors. Each main processor communicates via an individual input/output bus with one of the three microprocessors on each input/output module. In each main processor, the input/output bus microprocessor reads the data and provides it to the main processor through a dual-port random access memory (DPRAM) interface. For analog inputs, the three values of each point are compared, and the middle ("median") value is selected. All input modules include self-diagnostic functions designed to detect single failures within the module.

After the main processors complete the control algorithm, data are sent to the output modules. Outputs from the main processors are provided to the input/output bus microprocessors through DPRAM. The use of DPRAM allows separation of the control and communications functions of the main processor. The input/output bus microprocessors transfer the data to the three microprocessors on the output modules. The output modules set the output hardware appropriately on each of the three sections and perform voting to determine the appropriate state and/or verify correct operation.

Discrete outputs use a 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.

3.1.6.1.7 Tricon Communications

The Tricon can communicate with safety and non-safety systems via the Tricon Communication Module (TCM) and the RXMs.

The Tricon Communication Module

The TCM handles all network communications. The TCM includes two fiber optic port connectors which support peer-to-peer, time synchronization, and open networking to external systems. The TCM contains four serial ports allowing the Tricon V10 to communicate with Modbus master and slaves. Each serial port is uniquely addressed and supports the Modbus protocol.

The TCMs have three separate communication busses and three separate communication bus interfaces, one for each of the three main processors within a single PPS protection set. The three communication bus interfaces are merged into a single microprocessor. That microprocessor votes on the communications messages received from the three main processors and transfers only one of them to an attached device or external system. Messages received from the attached device are triplicated and provided to the three 3008N main processor modules. The TCM interfaces with the main processor via the IOCCOM, using the communication bus.

The TCM was qualified by Invensys for the Tricon V10 as the functional and electrical isolator. This provides assurance that safety functions performed by the Tricon would not be impacted by any failure of external devices, in this case the Tricon maintenance work station.

The TCM is capable of supporting bidirectional safety-related communication for communication with safety-related devices. However, the DCPP PPS application does not invoke these features. This type of communication uses peer-to-peer for communication between safety divisions, and safety application protocol for communication within a safety division. The safety application protocol is not used either because a safety-related video display unit is not used in the DCPP PPS.

The TCM supports bidirectional communication for communication with non-safety-related devices, through the NetOptics Model PA-CU port aggregator network tap devices. Specifically, the TCMs are used in the DCPP PPS to facilitate the following communications:

- Two-way communication between the Tricon subsystem and the associated Tricon maintenance work station within each protection set. Two communication links are established for each protection set through a pair of NetOptics Model PA-CU port aggregator tap devices.

- One-way communication between the Tricon subsystem and the process plant computer system. In particular, the NetOptics Model PA-CU port aggregator taps establish one-way communication pathways to the process plant computer system through a gateway switch.

A detailed description of the port aggregator tap is provided in Section 3.1.7.3, "Port Tap Aggregator," of this safety evaluation.

The TCM output media from the Tricon is fiber optic to provide electrical isolation. Media converters are used to convert the fiber optic media to 100 Base-T copper Ethernet to establish communications paths to the Tricon maintenance work station and process plan computer gateway computer via the port aggregator taps. Furthermore, the communication paths use cyclic redundancy checks, handshaking, and other protocol-based functions to ensure data communication integrity.

As stated in the "Triconex Approved Topical Report," September 2013 (Reference 29), Invensys Operations Management (IOM) performed testing that demonstrated the TCM would protect the safety core from network storms and other communication failures.

Tricon RXM Modules

The Tricon RXM modules are used to increase the number of input/output modules in the Tricon V10 PLC system. The DCPP PPS also uses the RXM to provide a communications interface between the safety-related and non-safety-related portions of the system.

The RXMs are single-mode fiber optic modules used in the PPS to isolate non-safety-related non-1E input, and output signals from the safety-related 1E portion of the Tricon subsystem within a single protection set. This isolation capability is used to provide one-way non-safety-related signal outputs to external systems.

Each RXM connection consists of three sets of identical modules, serving as repeaters/ extenders of the Tricon input/output bus. These modules provide ground loop isolation between the safety-related and non-safety-related portions of the Tricon subsystem. Furthermore, non-safety-related RXM chassis and modules are only considered within each protection set.

For each protection set of the DCPP PPS, the Tricon subsystem includes two RXM modules. The RXM consists of a safety-related primary RXM and a non-safety-related remote RXM. The main Tricon chassis is connected to a "primary" RXM via triplicated input/output expansion bus. The RXM serves as repeaters/extenders of the Tricon input/output bus. The primary RXM is connected to the main chassis with the triplicated input/output bus cable. The primary RXM is connected to a "remote" RXM chassis using multi-mode fiber optic cables. Figure 3.1.6.1-3 illustrates the connection pathways established by the RXMs. The three RXM modules in the primary RXM chassis are connected to corresponding RXM modules housed in the remote RXM chassis. Each pair of RXM modules is connected with two fiber optic cables.

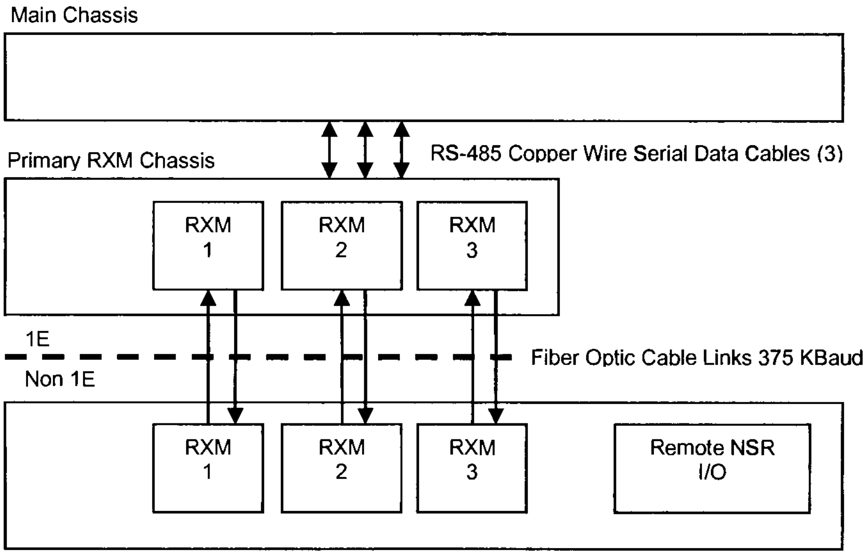


Figure 3.1.6.1-3. RXM Communications Pathway

The interfacing cabling is unidirectional and point-to-point for each channel of the RXM communication link. 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 because the RXM modules are connected with fiber optic cables.

The use of RXM communications in this manner was described in the Triconex Approved Topical Report and was evaluated by the NRC in the associated safety evaluation dated April 12, 2012 (Reference 29). The safety evaluation concluded the RXM elements provide adequate protection to the safety side input/output bus and to the overall safety function.

The non-safety RXM does not have any safety-related input/output assigned to it.

3.1.6.2 ALS Components

The diverse Advanced Logic System (ALS) portion of the PPS replacement platform uses field programmable gate array (FPGA) hardware logic technology. The built-in diversity features of the ALS subsystem are designed to ensure the PPS replacement system will perform all required safety functions automatically in the presence of a postulated common-cause failure without an adverse impact on the operator's ability to diagnose the event or perform manual actuation activities. These activities were previously credited for accident mitigation during a postulated common-cause failure of the Eagle 21 PPS.

The general architecture for an ALS subsystem is illustrated in Figure 3.1.6.2-1.[2] For the DCPP application, each PPS protection set contains one ALS subsystem. Each ALS subsystem is comprised of two ALS chassis, and the following peripheral equipment:

- Core logic board,
- Power supplies,
- Input and output boards,
- Control panels,
- Chassis,
- Assembly panels, and
- ALS Service Unit (ASU).

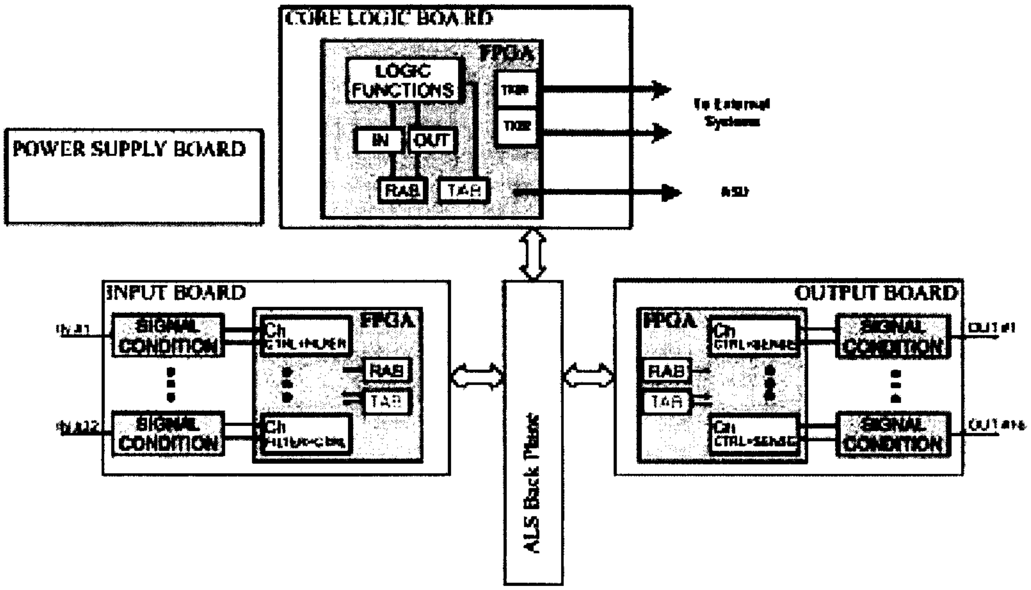


Figure 3.1.6.2-1 Generic ALS FPGA Architecture

The assembly panels incorporate field terminal blocks, fuse holders, and switches. The ALS chassis is an industry standard 19-inch chassis. The ALS chassis contains the ALS core logic board and input/output boards.

[2] This is Figure 4-8 of the LAR (Reference 12).

3.1.6.2.1 ALS Core Logic Board (ALS-102)

The ALS-102 core logic board contains the application-specific logic circuits which define and control the operation of the PPS subsystem. The ALS-102 is based on a generic ALS board configured with application logic for the DCPP PPS ALS subsystem. The ALS-102 performs the following functions:

1. Controls all sequencing within the ALS subsystem;
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.

A portion of the FPGA logic in the ALS-102 is customized for the PPS replacement application based on the DCPP Conceptual Design Document (Reference 1), Interface Requirements Specification (IRS) (Reference 98), and Controller Transfer Function Requirements Specification (Reference 99). These documents specify the overall functionality requirements of the PPS replacement. From this design input, the application-specific ALS-102 FPGA Requirements Specification is developed and from this specification, the detailed application-specific logic specification for the ALS-102 is created.

3.1.6.2.2 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 24 Volt (V) or 48 V digital contact sensing, 4-20 mA analog inputs, 0-10 V analog inputs, resistance temperature detector inputs, or thermocouple inputs.

The ALS input boards provide self-test capability to continuously verify vital components within the channel are operational. Isolation between the channels and the ALS logic is maintained by galvanic isolators. The input channels are protected against electrostatic discharge and surge voltages.

The input boards provide front panel light-emitting diode indicators which show the status of a particular input signal.

3.1.6.2.3 ALS Output Modules

The ALS output boards provide signals to control field devices such as actuators, indicators, and relays. 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. Isolation between the channels and the ALS logic is maintained by galvanic isolators. The output channels are protected against electrostatic discharge and surge voltages. Depending on the board type, the output boards can have individually isolated channels, or they can be located on a common isolation domain.

The output boards provide front panel light-emitting diode indicators to show the status of a specific output signals. Digital output channels in the PPS replacement are configured in the output board non-volatile random access memory to drive the output to a predefined state in case of board failure or lack of communication with the ALS core logic board. These predefined states are Open, Closed, or As Is.

3.1.6.2.4 ALS Communications

The ALS platform provides digital communications methods for intra-channel safety signals, unidirectional transmit-only to external devices, bidirectional communication for use with a maintenance work station (maintenance work station), and unidirectional receive or transmit for exchanges between instrument channels or to additional non-safety equipment. Regarding the DCPP PPS, there are no communication paths between redundant safety divisions or protection sets in the ALS portion of the PPS replacement.

The ALS system provides two separate and independent serial communication data bus structures for intra-channel safety communication and bidirectional communication with the maintenance work station. These communication buses use a master/slave communication protocol, with the bus master initiating all communication to the slaves on the bus.

- RAB: Reliable ALS Bus.

  The ALS boards communicate using the Reliable ALS Busses (RABs). The RABs are exclusively used for all data transfers between ALS boards during normal system operation. This communication is discussed in detail in the Advanced Logic System Topical Report (Reference 30), which describes configuration and operation of the RAB, and thus no additional description is provided in this safety evaluation.

- TAB: Test ALS Bus.

  The TAB is used to transfer monitoring, diagnostic, test, and calibration information to the ASU. For the DCPP PPS replacement system, the TAB communication channel is used to enable TAB functions between the ASU maintenance software in the ALS maintenance work station and the ALS system. The TAB is a master/slave protocol. In the DCPP PPS, the ALS system is the slave and the maintenance work station is the TAB master. The TAB uses a simple differential Electronic Industries Association EIA-485 point-to-point communications.

> This EIA-485 communication path is normally disabled, with two-way communications only permitted when the TAB data link is physically connected and the TAB Enable Digital Input is activated. Connection of the TAB is alarmed in the control room. The TAB uses a standard cyclic redundant checks protection to ensure the integrity of the communication isolation. Section 3.7, "Communications," of this safety evaluation provides details of the TAB communication.

In addition to these communication buses, the ALS-102 control logic board in the ALS system provides two unidirectional communication channels (TxB1 and TxB2), which can be used for sending run time information to a remote data logger or computer. The data are sent through one-way EIA-422 link making it impossible for the non-Class-1E equipment to send any commands or data back to the ALS system. Specifically, the receiving capability of the TxBs has been physically disabled by hardware as described in PPS ALS-ASU Communication Protocol (Reference 100) and PG&E's letter dated June 22, 2015 (Reference 19).

For the DCPP PPS replacement system, the TxB channels are configured as follows:

- <u>TxB1</u>:

  This one-way RS-422 communications channel on the ALS-102 transmits application-specific input and output states and values continuously to the non-safety process plant computer system via the 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 communication channel from each ALS chassis to the gateway computer is an isolated serial one-way with no handshaking.

- <u>TxB2</u>:

  This one-way RS-422 communications channel on the ALS-102 transmits the ALS core logic board application-specific input and output states and values continuously to the non-safety-related ALS maintenance work station which performs the function of the ASU. The TxB2 communication channel is serial one-way with no handshaking.

Additional information about configuration of the TxB channels is provided in Section 3.7, "Communications," of this safety evaluation.

3.1.6.2.5 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 core logic boards, input boards and output boards. Each board within these two paths contains two sets of cores which independently perform the same functions.

Core diversity is implemented for each of the FPGAs on all of the ALS boards to establish a first level of diversity. An additional level of design diversity is incorporated into the PPS ALS subsystem, which receives sensor signal inputs and makes trip or actuation determinations.

The diverse "A" and "B" execution path outputs are combined in hard-wired logic to ensure the protective action is taken if directed by either path. A single failed path cannot prevent a protective action. A more detailed description and evaluation of the ALS system diversity features is provided in Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation.

3.1.6.2.6 ALS Power Supplies

Each ALS PPS subsystem chassis is powered via the backplane assembly from an external dual-redundant power supply system. The power supply system in each ALS safety system cabinet is comprised of two independent 48 Volts direct current (VDC) power supplies. Each of these power supplies is mounted in the same cabinet as the associated ALS chassis and is capable of providing 150 percent of the cabinet load. The cabinet load consists of all ALS platform components and peripheral devices.

The individual 48 VDC chassis power supplies are supplied by PG&E. They 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 VDC from the redundant cabinet power supplies is fed to the ALS chassis, where they are diode auctioneered to provide a single local 48 VDC supply. Each ALS board contains direct current (DC)/DC converters to generate stable local board power. All ALS boards are fused, filtered, and over-voltage protected on the incoming cabinet 48 VDC supply voltage. The fuse ensures 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. An alternating current (AC) line filter within the ALS cabinet reduces incoming noise and suppresses conducted emissions and conducted susceptibility.

Power supply failures (loss of output voltage) are designed to actuate alarms on the main annunciator system. The ALS-A and ALS-B subchannels within a single protection set are supplied by the same pair of 48 VDC power supplies in the associated cabinet.

3.1.7 Other Subsystems

Figure 3.7-1 (Figure 4-13 of Enclosure 1 to the licensee's letter dated October 26, 2011; Reference 1) illustrates other subsystems included in the DCPP PPS replacement project. This figure includes the processors and equipment to provide additional functional and communication capabilities as follows:

1. Maintenance work station(s)
2. Port tap aggregators
3. KVM switch and common keyboard, monitor, and mouse
4. Gateway computer(s)
5. Media converters

3.1.7.1 Maintenance Work Station

Each protection set in the PPS replacement is provided with two dedicated and separated non-safety-related maintenance work stations for the purpose of maintenance and calibration. One maintenance work station is connected to and communicates with the ALS system, and the other maintenance work station is connected to the Tricon system, in the associated protection set. The two maintenance work stations cannot communicate with each other. Also the maintenance work stations in a protection set cannot communicate with the maintenance work station in redundant protection sets nor can it communicate with safety-related equipment outside its associated protection set.

The maintenance work stations are configured to be read-only, except during testing and calibration, when two-way communication between the maintenance work station and its associated safety-related system is required to perform the test or calibration function. The maintenance work station is able to read, but not write, process instrumentation information for local display at the maintenance work station during normal operation.

Using the maintenance work station, 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. Section 3.7 describes communication between the Tricon and ALS system with their respective maintenance work stations.

The maintenance work station will be located inside a locked cabinet inside a vital area inside the protected area, minimizing the possibility of the inadvertent actions.

Tricon Subsystem Maintenance Work Station Operation

Section 4.2.13.4, "Tricon-Based PPS Equipment Communications with Tricon MWS and PDN Gateway Switch," of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the software installed in the maintenance work station. Specifically, this maintenance work station includes the software applications necessary to: (1) communicate maintenance actions and diagnostic functions, (2) modify software application, and (3) relay status information, alarms, data, and responses from the Tricon system. The licensee's letter dated June 22, 2015 (Reference 19), lists the application programs installed in this maintenance work station.

ALS Subsystem Maintenance Work Station Operation

Section 4.2.13.5, "FPGA-Based ALS PPS Equipment Communication with ALS MWS and PDN Gateway Computer," of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the software installed in the maintenance work station. The ALS maintenance work station uses the ALS Service Unit (ASU) described in the Advanced Logic System Topical Report (Reference 30). The ASU provides graphical user interfaces for displaying ALS system status on the maintenance work station and for providing user-controlled access to the ALS controllers for performing maintenance operations such as calibration. Specifically, the ASU will be used for: (1) system diagnostics, (2) post-trip analysis, (3) monitoring real-time operation, and (4) assistance in performing user initiated test, calibration, and maintenance operations. The licensee's letter dated June 22, 2015 (Reference 19), lists the application programs installed in this maintenance work station.

The ALS subsystem of the DCPP PPS replacement does not use a keyswitch to enable and disable external Test ALS Bus (TAB) communications as described in the Advanced Logic System Topical Report. The TAB communication requires physical connection of the TAB link and the TAB Enable Digital Input is activated. Activation of the TAB access will be alarmed in the control room. Pacific Gas and Electric Company (PG&E) will control connection of the TAB data link through plant administrative procedures, as described in the licensee's letter dated June 22, 2015 (Reference 19).

Malfunctions of the ASU parameter display function cannot adversely affect the ALS system operation because communications between the ALS and the ALS maintenance work station via TxB2 are strictly one-way.

3.1.7.2 KVM Switch and Common Keyboard, Monitor, and Mouse

Each redundant protection set pair of maintenance work stations (one for the Tricon and one for the ALS safety system) will share a common keyboard, video monitor, and mouse through a device known as a KVM switch.

Section 4.2.14 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the KVM switch. In addition, the Interface Requirements Specification (Reference 98) specifies the operation required for the KVM switch as described in the licensee's letter dated June 22, 2015 (Reference 19).

3.1.7.3 Port Tap Aggregator

The PPS replacement design incorporates the NetOptics Model 96443, Model PA-CU port aggregator network tap to permit two-way communications between the Tricon Communication Module (TCM) and the maintenance work station, while permitting the process plant computer gateway computer read-only access to the TCM and the maintenance work station. The NetOptics port aggregator network tap was previously approved by NRC staff's January 28, 2010, safety evaluation for LAR, "Oconee Nuclear Station, Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade" (Reference 96). The NRC performed a circuit analysis of this device as part of its evaluation and identified the internal data signal flow paths using the device schematics. For data signals to flow from the TCM (bidirectional communications bus) toward the receiving instrument—in this case, the plant computer system—electrical signals must pass through a buffer amplifier integrated circuit component. The buffer amplifier was analyzed for the potential of electrical signals to flow in the opposite direction of intent even under failure or overload conditions. The results of this analysis showed the amplifiers were not capable of passing electrical signals in the reverse direction under any condition; therefore, data cannot flow from port 1 (plant computer system) to port A (TCM).

To confirm these analysis conclusions, the NRC's Office of Research contracted a lab to conduct data tests on an actual port tap device. During these tests, several attempts were made to force data signals to flow in the reverse direction. Although several of these tests resulted in a loss or failure of the communications to the non-safety systems, none was able to cause data to flow in the reverse direction (from the non-safety system to the safety system) and none was able to affect or compromise the ability of the safety system to perform its safety functions.

3.1.7.4 Gateway Computer(s)

The DCPP gateway computer and gateway switch are part of an existing system that was installed by a previous project and therefore were not part of the scope of changes requested for approval in the LAR.

The Tricon system and ALS system communicate with the process plant computer gateway computer one-way. Specifically, the Tricon communications are performed through the NetOptics port tap aggregator port 1. This port prevents inbound communications from the gateway computer to the Tricon system because it is configured as a transmit-only port for external devices. The ALS system communicates with the gateway computer through the ALS-102 transmit bus TxB1.

3.2 Hardware Development Process

Hardware components of the DCPP PPS are comprised of Tricon and ALS platform components as well as licensee-provided components such as system power supplies, cabinets, and interconnecting wiring. All platform components were previously evaluated by the NRC as part of the safety evaluations of the Tricon and ALS platform topical reports. For the Tricon subsystem components, hardware development processes were evaluated in Section 3.2 of the safety evaluation for the Triconex Approved Topical Report (Reference 29). For ALS subsystem components, hardware development processes were evaluated in Section 3.2 of the safety evaluation for the Advanced Logic System Topical Report (Reference 30). Additionally, process changes were made to the Tricon development processes and these changes are evaluated in Section 3.8, "Tricon V10 Platform Reference Design Changes," of this safety evaluation. Plant application-specific requirements for each of these platforms were provided in the associated platform topical report safety evaluations and have been addressed in Section 3.13, "Plant-Specific Action Items Identified in Platform Topical Report Safety Evaluations," of this safety evaluation.

The quality control programs for both vendors and the licensee used to develop PPS hardware have been evaluated by the NRC staff and have been determined to be acceptable. See Section 3.9.2.3, "IEEE 603-1991, Clause 5.3, Quality," of this safety evaluation for quality evaluation information. The staff determined that the information provided by the licensee adequately describes the PPS hardware development processes as defined in the PPS replacement Interface Requirements Specification (Reference 98). The staff also confirmed use of ALS and Tricon platform hardware components previously evaluated by the NRC and determined to be acceptable for use in nuclear power plant safety applications.

3.3 Software/Core Logic Architecture

Tricon Software Architecture

Software architecture for the Tricon subsystem is designed to support the Tricon Triple Modular Redundant (TMR) functionality to allow continued system operation in the presence of any single point of failure within the system. All system and application software is replicated for each set of three redundant Tricon hardware modules used in the system.

The Tricon V10 software architecture is composed of the following three main elements:

1. The executive for the application processor,
2. The executive for the communications processor, and
3. The executive element for the various input/output modules.

Details of the TMR architecture are described in the Triconex Approved Topical Report (Reference 29). TMR architecture allows the Tricon V10 to detect and correct individual faults online. When a fault does occur, the Tricon initiates an alarm, removes the affected portion of the faulted module from operation, and continues to perform all safety functions normally in a dual-redundant mode. The system returns to the fully triple-redundant mode of operation when the affected module is restored without interruption of monitoring, control, or protection capabilities. The platform safety evaluation determined that the Tricon V10 platform meets the criteria regarding deterministic performance of SRP Chapter 7, "Instrument and Controls – Overview of Review Process" (Reference 40), SRP Section 6.1 of Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603" (Reference 41), SRP BTP 7-21, "Guidance of Digital Computer Real – Time Performance" (Reference 50), and Electric Power Research Institute (EPRI) technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996, Section 4.4.1.3 (Reference 101).

The Tricon application software used for the DCPP PPS is developed using the TriStation 1131 development tool and is downloaded into each of the subsystems' redundant processor modules. The PPS Tricon application is written using function block diagrams. The NRC staff reviewed several of these function block diagrams provided in the "Software Design Description (SDD)," 993754-11-810-P, Revision 0, dated February 25, 2013 (Reference 102), to gain an understanding of how specific safety functions were being allocated to software modules of the PPS. All system safety function requirements are traceable to the software design description via the "Project Traceability Matrix," 993754-1-804-P, Revision 1, dated October 17, 2012 (Reference 103). The function block diagrams are translated into structured text that is subsequently translated into an emulated and then native mode assembly language. This is then assembled and linked with native mode code libraries to generate a program.

Compiled application programs are then downloaded to the Tricon processor modules through a communication module. During the download process, the individual communication blocks are protected from corruption via a cyclic redundancy check. The program segments, which may span communication blocks, have an overall 32-bit cyclic redundancy check. The 32-bit cyclic redundancy check for each program is stored both in the TriStation and in the Tricon and can be compared to ensure proper program transfer by the user.

Once downloaded into the Tricon hardware, the application program implements the required protection, monitoring, and control functions defined by the design basis documents for the DCPP digital PPS.

ALS Core Logic Architecture

The ALS subsystem of the DCPP PPS uses technology that does not use software while the system is in operation. Instead, the ALS system uses software to generate a hardware layout that is implemented in a field programmable gate array (FPGA) circuit board. Because of this, the operational ALS subsystem architecture is hardware and not software-based. An evaluation of the tools used for the generation, implementation, and maintenance of these FPGA boards is provided in Section 3.10.1.1.2, "IEEE 7-4.3.2-2003, Clause 5.3.2, Software Tools," of this safety evaluation.

An FPGA is a very large-scale, high-speed integrated circuit that provides user programmable logic through the configuration and interconnection of elemental circuit building blocks within the device. The "field programmable" portion of FPGA refers to the ability of an end-user to program the device after it has left the device manufacturer's foundry. The "gate array" portion of FPGA refers to the collection (an "array") of elemental digital building blocks ("gates") within the device.

The ALS platform uses natural language in its requirement specifications. The ALS platform then uses a text-based high-level language to specify the functionality of its FPGA-based digital circuits. The ALS platform FPGA designers use the hardware descriptive language as the high-level language to specify functionality. The hardware descriptive language uses standard text-based expressions to govern the structural and behavioral aspects of the desired digital circuit. In this way, hardware descriptive language can be considered a method that refines the natural language requirements into specifications of a more precise set of formatted requirements.

Hardware descriptive language allows for FPGA circuit modules to be developed independently and validated through simulation. After individual modular FPGA circuits have been validated, integration and hardware descriptive language simulation and validation of new individual circuit modules with previously integrated ones is performed.

A synthesis of the FPGA-based circuit implementation from the high-level description is then performed. A software-based development tool, which is referred to as a "synthesizer," determines the required FPGA elemental digital building blocks and their interconnections from the hardware descriptive language statements using synthesizer directives. The FPGA-based circuit is then simulated and validated for proper operation.

After acceptable performance of the synthesis output has been determined, the synthesized circuits undergo a "place and route" operation. The "place and route" operation uses an FPGA device manufacturer specific software-based development tool. During the "place and route" operation, each proposed logic element is assigned to an actual elemental digital building block within the targeted FPGA device. The place and route operation also determines the specific physical interconnections required between the elemental digital building blocks. The described circuit is then simulated and validated before programming it into the FPGA device. This simulation is referred to as "gate-level simulation."

The ALS platform uses a non-volatile "flash" method to program its FPGA device. The "flash" method allows the device to be reprogrammed; however, non-volatile FPGAs do not lose their internal configuration when electrical power is removed.

A more detailed description of the ALS FPGA architecture is provided in Section 3.2 of the safety evaluation for the Advanced Logic System Topical Report (Reference 30).

The NRC staff determined that the information provided by the licensee includes an adequate explanation of the software and core logic architecture established for the DCPP PPS. Based on previous approval of the Tricon and ALS platform architectures and the staff's understanding of how these systems have been developed and integrated into the PPS, the NRC staff concludes the DCPP PPS architecture provides adequate framework for the performance of plant safety functions and to support reliable operation of the PPS.

3.4 Software/Core Logic Development Process

The processes used for the development of Tricon PPS application software and ALS application logic implementation were evaluated by the NRC staff in accordance with the review guidance of NUREG-0800 (SRP) Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," March 2007 (Reference 46). The following subsections provide the details and results of this evaluation.

3.4.1 Software/Core Logic Planning Documentation

This section evaluates the software planning documents associated with the DCPP PPS replacement system's development. As is indicated by the revision levels and dates of issue for the plans reviewed under this section of the BTP 7-14, Section B.2.1, "Software Life Cycle Process Planning," identifies the software planning documents that could be prepared to support the software lifecycle. Section B.2.1 identifies 12 documents, most of which are evaluated in the following subsections. The following documents were not included in the evaluation because ISG-06 (Reference 24) does not recommend they be submitted for review. Furthermore, the software activities described in these plans are not part of the licensing process. Consequently, the NRC staff did not evaluate these plans.

- Software integration plan
- Software maintenance plan
- Software training plan
- Software operations plan

Branch Technical Position (BTP) 7-14, Section B.3.1, "Acceptance Criteria for Planning," describes acceptance criteria for the software development activities and documentation. In addition, IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33), provides specific requirements concerning software development activities. See Section 3.10, "Conformance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," of this safety evaluation for details concerning the licensee's conformance with this standard.

Note during the course of the DCPP PPS project, Westinghouse Electric Company (WEC) closed its operations in Scottsdale, Arizona (CS Innovations or CSI), and consequently many planning documents and process procedures transitioned from CSI to WEC. WEC evaluated changes to planning documents and processes. WEC found that no adverse effect was introduced. The WEC topical report 6116-00500, "Independent Verification and Validation Summary Report," Revision 1, October 2015 (Reference 104), provides a summary of WEC's evaluation.

3.4.1.1 Software/Core Logic Management Plan

Standard Review Plan (SRP) BTP 7-14, Section B.3.1.1, "Acceptance Criteria for Software Management Plan (SMP)" (Reference 46), provides acceptance criteria for software management plans. This section states that Regulatory Guide (RG) 1.173, Revision 0, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 85), endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Reference 86). Further, IEEE Std. 1074-1995, Clause A.1.2.7, "Plan Project Management," of the standard contains an acceptable approach to software project management.

The overall PPS replacement project is managed by PG&E. Invensys was responsible for the development of a Tricon-based portion of the PPS replacement system, and WEC was responsible for the development of an ALS-based portion of the PPS replacement system. Section 4.5.1 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the software management plans for PG&E, Invensys Operations Management, and WEC established for the PPS replacement project.

PG&E

Section 4.5.1.1 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes PG&E's approach for software management. In this section, PG&E states that it did not develop software for the PPS replacement system. Instead, PG&E contracted Invensys and WEC to design, develop, manufacture, and test the DCPP PPS to replace the existing Eagle 21 system. After completion of the PPS replacement project, and the PPS is installed and operating (operations and maintenance phase), PG&E will control software development and modifications to the Tricon and ALS platforms in accordance with its PPS "Management Plan," 6116-00000, September 2015 (Reference 105), and DCPP Procedures CF2, "Computer Hardware, Software and Database Control" (Reference 106), CF2.1D2, "Software Configuration Management for Plant Operations and Operations Support" (Reference 107), and CF2.1D9, "Software Quality Assurance for Software Development" (Reference 108). These documents state that software modifications to the PPS will be performed by the vendors for ALS and Tricon platforms, CS Innovations and Invensys, respectively.

In Attachment 3 of the LAR dated October 26, 2011, PG&E submitted Revision 1 of the PPS replacement "Concept, Requirements, and Licensing Phase 1 Project Plan" (Reference 109), which describes the proposed system, project organization and responsibilities, project deliverables, and development and licensing activities associated with the PPS replacement project. Section 2 of the Concept, Requirements, and Licensing Phase 1 Project Plan describes the organization and roles and responsibilities for PG&E personnel. This section identifies the project organization members to be: PG&E project manager, engineering of choice design change package, PG&E project engineering team, and vendors. The relationship among these members is shown in Figure 2-1, "PPS Replacement Project Organization," of the Concept, Requirements, and Licensing Phase 1 Project Plan. This figure shows the design change package team and Altran Solutions project team under engineering of choice design change package and PG&E project engineering, respectively. By letter dated May 9, 2013 (Reference 13), PG&E clarified that the role and responsibilities of the engineering of choice design change package team was to prepare the design package for the PPS replacement project. Also, in the letter dated May 9, 2013, PG&E explained the role of the Altran project team. In particular, for the PPS replacement project, Altran as a subcontractor providing engineering support to the PG&E project team. Altran's work was governed by the Altran Engineering Procedures Manual. Further, Altran's documents submitted to PG&E were prepared in accordance with Altran procedures. All Altran documents were verified in accordance with Altran procedures. In addition, PG&E accepted Altran documents, which was noted in the Altran Verification Report for these documents.

Section 3 of the Concept, Requirements and Licensing Phase 1 Project Plan describes the development process for the PPS replacement project. For the PPS replacement project, PG&E was responsible for the following phases in the system development process: project initiation and planning phase, conceptual design phase, installation and checkout phase, operation phase, and maintenance phase. During the design, development, and testing phase, PG&E provided oversight of vendors' activities. The oversight activities were described in PG&E's Quality Assurance Plan for the DCPP PPS replacement provided in Attachment 1 of the licensee's letter dated August 2, 2012 (Reference 6). These activities included technical audits, cyber security audits, and software quality assurance audits. In its letter dated May 9, 2013 (Reference 13), PG&E clarified the roles and responsibilities for PG&E personnel to provide oversight activities. It also clarified the responsibilities for the PG&E project manager, who has overall responsibility for system development, including management of the PPS replacement project and share responsibilities for meeting the software quality objectives and for implementing the software quality management throughout the project (Reference 109). In addition, PG&E, the system vendors, and the NRC staff held conference calls at least once a month to discuss open items and project management activities and status.

As stated in its letter dated January 25, 2016, as part of the oversight activities, PG&E performed assessments, audits, and source inspections during development and testing of the equipment (Reference 20). Assessments of Invensys and WEC/ALS qualification for this project, as well as their quality assurance programs, were performed; results from these assessments were recorded in PG&E audit File Nos. 121520008 and 121520007, respectively. In addition, during the design and development of the PPS replacement system, PG&E reviewed documents prepared by the vendor, performed inspections of the systems, and reviewed and witnessed the testing during the factory acceptance testing (FAT) of the systems.

To support the PPS replacement project, PG&E developed and implemented the following plans:

- System Quality Assurance Plan (SyQAP) (Reference 110)
- System Verification Plan (SyVVP) (Reference 111)
- Requirements Traceability Matrix (Reference 188)
- System verification and validation (V&V) report
- Site acceptance test procedure and test execution
- Installation plan

These documents provide a methodology for documenting quality assurance elements and software development for the replacement PPS software. Also, the PG&E documents define the activities and project deliverables for each phase of the system lifecycle. Further, they describe the software V&V, quality assurance, software testing, and software safety requirements for the PPS replacement system. These plans comply with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.1 (Reference 33), and BTP 7-14 (Reference 46). These plans are described in the subsequent sections of this safety evaluation.

The licensee identifies and reports non-conformances and implements corrective action in accordance with its "Problem Identification and Resolution." If an event needs to be reported to the NRC (as required by 10 CFR Part 21), PG&E will follow the guidance in its administrative procedure XI1.ID2, "Regulatory Reporting Requirements and Reporting Process." During software development of the PPS replacement system, the vendors' anomaly reporting procedures were used. As stated in its letter dated January 25, 2016 (Reference 20), PG&E evaluated reported deviations or anomalies during software development, approved corrective actions, and coordinated the disposition of discrepancies in the course of V&V.

Tricon

The Invensys NTX-SER-09-21, Revision 1, "Nuclear Systems Integration Program Manual," dated July 9, 2010 (Reference 112), describes the overarching approach for Invensys to develop the Tricon platform. In addition, Invensys created a Project Procedures Manual (PPM), Quality Procedures Manual, Manufacturing Department Manual, and Project Instructions, which are the implementing procedures under the Nuclear Systems Integration Program Manual. The Quality Procedures Manual and Manufacturing Department Manual were reviewed during the evaluation of the Tricon generic platform in the Triconex Approved Topical Report (Reference 29). The PPM defines the process and administrative controls to follow when working on a nuclear safety-related system. Invensys submitted NTX-SER-09-21, "Summary of the Invensys Project Procedures Manual for Safety-Related Work," dated August 31, 2009 (Reference 113). Also, Invensys created specific Project Instructions for the PPS replacement project to address project-specific procedures and administrative controls. The NRC staff reviewed the PPM and Project Instructions during the first regulatory audit of Invensys on

November 13-16, 2012 (Reference 36), and confirmed the PPM was properly implemented in the Invensys software plans for the PPS replacement project.

The Invensys "Project Management Plan (PMP)," Revision 3, 993754-1-905-P, dated December 18, 2012 (Reference 114), describes the management activities and lifecycle activities followed by Invensys during the DCPP PPS replacement project. The PPM conforms to the requirements in BTP 7-14 (Reference 46). The PMP defines the project organization and roles, responsibilities, and skills for Invensys personnel for the PPS replacement project. In particular, the Invensys project manager for the PPS replacement project is the single point of contact for external interactions with PG&E. Invensys Nuclear Delivery is responsible for the quality and safety of the delivered PPS, Nuclear IV&V is responsible for ensuring that Nuclear Delivery has adequately met the safety system requirements, and Nuclear Quality Assurance is responsible for ensuring that Nuclear Delivery and Nuclear IV&V are adhering to applicable procedures and processes for nuclear safety-related system development. A formal software safety organization was not established, because the Nuclear IV&V organization fulfilled that role for the PPS replacement project. Nuclear Delivery interfaces with Nuclear IV&V staff and Nuclear Quality Assurance as needed. For the PPS replacement project, Invensys subcontracted services for performing supplemental electromagnetic interference/ radio-frequency interference testing. This plan describes the interaction with subcontracting engineering company that performed this testing.

The PMP describes the managerial process, including project risks and mitigation strategies, as well as the monitoring mechanisms used to manage and control Tricon system development process. For example, Invensys performed design verification and software safety reviews. These reviews required participation of Nuclear Delivery, Nuclear IV&V, Nuclear Quality Assurance, and PG&E. The reviews were documented in the document review comment sheets, as required by PPM 2.0. During the June 3-5, 2014, regulatory audit (Reference 38), the NRC staff reviewed examples of these reviews to observe how configuration management of project documents was implemented.

Appendix A of the PMP lists documents created for the PPS replacement project. In particular, Invensys developed the following documents to support software management and development of the PPS replacement project:

- Software Development Plan (Reference 115)
- Software Configuration Management Plan (Reference 116)
- Software Integration Plan (Reference 117)
- Software Verification and Validation Plan (Reference 118)
- Software Safety Plan (Reference 119)

In addition, Invensys prepared the "Project Traceability Matrix (PTM)," 993754-1-804-P, dated October 17, 2012 (Reference 103), to trace all requirements for each protection set. Section 1.2 of the PMP describes the schedule to deliver project documents to support PG&E licensing process.

Invensys has established non-conforming procedures to address anomalies, non-conformances, and process deficiencies as required by Nuclear Systems Integration Program Manual Sections 7 and 8. The Invensys "Software Development Plan," 993754-1-906-P, dated December 18, 2012 (Reference 115), discusses problem reporting and procedures for corrective action. In addition, the Invensys "Project Quality Plan (PQP)," 993754-1-900-P, dated March 2, 2012 (Reference 120), and "Software Configuration Management Plan (SCMP)," 993754-1-909-P, dated December 18, 2012 (Reference 116), provide reference to procedures to follow when deviations are identified and how deviations are corrected. In particular, Invensys staff reported program errors, problems, and deviations on a system integration deficiency report (SIDR) in accordance with PPM 10.0, which was reviewed during the June 3-5, 2014, regulatory audit (Reference 38). Invensys requires the Project Review Committee to review and approve the disposition of SIDRs. For software plan reviews, Invensys staff used document review comment sheets to record comments or modifications in accordance with PPM 2.0, which was reviewed during the regulatory audit.

ALS

WEC was responsible for defining and implementing the process used to manage and develop the ALS platform for the PPS replacement project.

The WEC DCPP PPS "Management Plan," 6116-00000, September 2015 (Reference 105), describes the process used to manage the ALS platform development project and the overall project lifecycle. The Management Plan follows the intent of IEEE Std. 1074-1995 (Reference 86) and IEEE Std. 1058-1998, "IEEE Standard for Software Project Management Plans" (Reference 121). The Management Plan follows the quality assurance processes and procedures defined in DCPP PPS "Quality Assurance Plan," 6116-00001, May 2014 (Reference 122).

The Management Plan describes the project organization for the design and development of the ALS subsystem of the DCPP PPS replacement. This document describes the project organization, interfaces, and roles and responsibilities for the WEC staff involved in the project. Westinghouse personnel were assigned the following roles: (1) IV&V manager, who oversees and manages IV&V activities; (2) project manager, responsible for managing the DCPP project and is also responsible for the commercial process interface with PG&E; (3) WEC product manager, who is responsible for the overall management of WEC activities; and (4) quality assurance manager, responsible for product quality and implementation of quality assurance plan. Both the IV&V team and the quality assurance team have independent organizational reporting structures from the design and implementation team.

Westinghouse required all staff participating in the PPS replacement project to complete the quality assurance indoctrination training and all training required for their job function, as indicated in the specific training plan for this project. The NRC staff reviewed WEC training records during the regulatory audit on June 22-26, 2015 (Reference 39).

The Management Plan defined the project deliverables, schedule and budget, process model, and project management methodologies used during the project to track progress, record corrective actions, configuration management, and project metrics. For this project, Westinghouse used the Enterprise Document Management System as the official repository for all approved documents and plans, DOORS® for requirements tracing, and OnTime™ ticket for deficiencies and corrective actions.

The Management Plan identifies the reviews and audits conducted during the system development. For example, Westinghouse performed design reviews during the development stage. The NRC staff reviewed the design reviews performed during the June 22-26, 2015, regulatory audit (Reference 39).

The WEC staff used the same tools used for the development of the generic ALS platform, which is described in "Advanced Logic System Design Tools," 6002-00030, May 2015 (Reference 123).

Westinghouse used a risk assessment worksheet to identify project risks and issues, as well as mitigation strategies. This worksheet is maintained and reviewed periodically by the project leadership team. The NRC staff reviewed a risk assessment worksheet during the regulatory audit on June 22-26, 2015.

The Management Plan describes how Westinghouse identifies and records non-conformities and problem resolution. Non-conformities were recorded, addressed, and tracked via the OnTime™ defect tracking tool in accordance with Westinghouse 9006-01501, "Defect Management Work Instruction." Corrective actions are resolved following the procedure specified in WEC 16.2, "Westinghouse Corrective Actions Process." The Management Plan also described how problems are resolved during the different system's lifecycle phase. During the course of the DCPP PPS project, Westinghouse migrated from its Corrective Action Program to the Corrective Action, Prevention and Learning (Reference 104). The Issue Review Committee manages issue resolution identified in the Corrective Action, Prevention and Learning. Issues are recorded and tracked to resolution. Audit findings and results are also documented in accordance with WEC 16.2. During the June 22-26, 2015, regulatory audit (Reference 39), the NRC staff reviewed several OnTime™ tickets and confirmed the process was properly implemented.

The Management Plan identified and briefly described supporting system plans (e.g., configuration management plan) developed for the DCPP PPS replacement project. Evaluations of these plans are provided in the following sections of this safety evaluation.

Software Management Plan Safety Conclusion

In summary, the NRC staff determined that the software management plan established the organization and authority structure for the application software development, the procedures to be used, and the relationships between major activities. The staff concludes that the management structure provided for adequate project oversight, control, reporting, review, and assessment and, therefore, the software management plan satisfies IEEE Std. 1074-1995, in terms of software project management. In particular, this standard includes Clause A.1.2.7, which requires the management plan to describe planning for support, problem reporting risk management, and retirement. The staff concludes that the software management plan adequately addresses the planning aspect of BTP 7-14, Section B.3.1.1 which describes acceptance criteria for the software management activities and documentation of the software development project and is, therefore, acceptable.

The NRC staff has reviewed the results of the oversight activities performed by the licensee and determined the vendor oversight functions are providing an effective means of assuring the development of high-quality safety-related software in accordance with the licensee's Appendix B, quality assurance plan. Individual management and technical responsibilities are delineated in the software configuration management plan, software quality assurance plan, and V&V plans. As a result of interviews conducted with personnel responsible for performing various V&V and software quality assurance plan activities, the NRC staff concluded the assigned personnel have the experience and have received the necessary training needed to perform those assigned duties.

3.4.1.2 Software/Core Logic Development Plan

Standard Review Plan (SRP) Branch Technical Positon (BTP) 7-14, Section B.3.1.2, "Software Development Plan (SDP)" (Reference 46), describes acceptance criteria for software development plans. Regulatory Guide (RG) 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (Reference 85), endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Reference 86), as providing an acceptable approach to software development processes for meeting the regulatory requirements and guidance as they apply to development processes for safety system software and that Clause 5.3.1, IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33), contains additional guidance on software development.

The PG&E PPS replacement "Concept, Requirements, and Licensing Phase 1 Project Plan," Revision 1, dated October 26, 2011 (Reference 109), and PPS replacement "System Quality Assurance Plan (SyQAP)," Revision 0, dated October 26, 2011 (Reference 124), describe software development activities, software reviews, and problem reporting and corrective actions for the PPS replacement project. PG&E did not develop software for the PPS replacement project, so a PG&E software development plan was not submitted. However, PG&E prepared these documents to provide guidance for the vendors to establish requirements, conventions, rules, and standards to follow when developing their software for the PPS replacement system. In particular, the PG&E project plan states that a traditional waterfall model is chosen as the software lifecycle model for the PPS project development process. The waterfall model, as discussed in IEEE Std. 7-4.3.2-1993, Annex E (Reference 33), assumes that each phase of the lifecycle is completed in sequential order from requirements definition to the retirement phase. The PG&E project plan identifies the following project phases for PG&E: project initiation phase, conceptual design phase, test phase, installation and checkout phase, operation phase, and maintenance phase. The other project phases were performed by each supplier in accordance with their 10 CFR 50 Appendix B programs, and are described below. Note that PG&E will not perform software modifications following FAT. Such modifications, if necessary, will be performed by the 10 CFR 50 Appendix B suppliers. Section 3.1 of the PG&E project plan provides a brief description of each phase of the development process, including responsibilities for each sub-vendor.

The PPS replacement SyQAP defines the general development process required by PG&E to the sub-vendors, including tasks and outputs for each phase in the development process. The NRC staff's evaluation of this plan is provided in Section 3.4.1.3, "Software/Core Logic Quality Assurance Plan," of this safety evaluation.

As described in its letter dated January 25, 2016 (Reference 20), during the software development processes, PG&E performed management and oversight activities for development activities performed by Invensys and Westinghouse/ALS. These activities were defined in the PG&E SyQAP, Revision 1, dated May 9, 2013 (Reference 110).

Tricon

An evaluation of the development process for the generic Tricon V10 platform was performed by the NRC as part of the Tricon platform topical report review. This evaluation is documented in the safety evaluation for the Triconex Approved Topical Report (Reference 29).

The Invensys "Project Management Plan (PMP)," 993754-1-905-P, dated December 18, 2012 (Reference 114), describes the organization, responsibilities, and management activities for the PPS replacement project to ensure adherence to the Invensys quality and process requirements for the development of nuclear safety-related software and hardware. The Invensys organization for this project is described in Section 3.4.1.1, "Software/Core Logic Management Plan," of this safety evaluation.

For the DCPP PPS replacement project, Invensys developed the following software to be installed in the operating PPS safety-related system hardware.

- Test System Application Program (TSAP) software, and

- Embedded software including operating system software, communication software, and firmware used in the Tricon portions of the PPS.

The Invensys PMP describes the development processes and the lifecycle activities to develop the Tricon software for the PPS replacement project. The lifecycle activities resulted from the modified waterfall model for the software development lifecycle process described in the "Nuclear Systems Integration Program Manual," dated July 9, 2010 (Reference 112), as implemented by the project procedures manuals (PPMs) and in conformance to IEEE Std. 1074 (Reference 86).

The Invensys "Software Development Plan (SDP)," 993754-1-906-P, dated December 18, 2012 (Reference 115), provides a detailed description of the software development process. In particular, this plan defines the software lifecycle and technical guidance for Invensys personnel to develop the Tricon software for the PPS replacement project. In addition, Invensys prepared project instructions to complement the instructions in the Nuclear Systems Integration Program Manual and PPMs in order to provide administrative controls and software quality plan for development of the system application program software for the PPS replacement project.

The Invensys SDP and project instructions describe the software lifecycle phases applicable to this project. Specifically, these documents identify the following lifecycle phases: acquisition phase, planning phase, requirements phase, design phase, implementation phase, test phase, and delivery phase. These documents also provide a description of the inputs, tasks, processes, and outputs associated with each lifecycle phase. Note that the installation/acceptance testing phase, operation phase, maintenance phase, and retirement phase are not within the scope of the DCPP PPS replacement project for Invensys and, therefore, were not included in the software development lifecycle process because these activities are the licensee's responsibility.

At the completion of each software lifecycle phase, Invensys requires the Project Review Committee to access the risks and identify recommendations for the next phase. The SDP identifies the Invensys personnel required to participate in the Project Review Committee. The SDP describes how modifications identified during these reviews are disposed before exiting the phase and continuing to the next one.

In addition, at the conclusion of each phase, the Nuclear IV&V team would prepare a V&V phase summary report and a safety analysis. The Invensys PPS replacement "Software Verification and Validation Plan (SVVP)," 993754-1-802-P, dated December 18, 2012 (Reference 118), describes the requirements for the IV&V process applied to the TSAP software developed for the PPS replacement project, running on the safety-related Tricon V10 platform hardware. The SVVP is described in more detail in Section 3.4.1.6 of this safety evaluation.

During the development of the application software, Invensys performed software walkthroughs to evaluate the code. Discrepancies and comments identified during this process were documented in software walkthrough reports. During the June 3-5, 2014, regulatory audit (Reference 38), the NRC staff reviewed the Invensys System Integration Deficiency Report (SIDR), where test anomalies were documented during verification testing. After the development of the software application was complete, the design team prepared a software development checklist to accompany the software application. The software development checklist was then used to manage the configuration of the application program upon initiation of the IV&V process and during PG&E review. During the regulatory audit, the NRC staff reviewed examples of software development checklists for the TSAP.

The Invensys "Software Configuration Management Plan (SCMP)," 993754-1-909-P, dated December 18, 2012 (Reference 116), describes the method for control of the application software. The SCMP is described in more detail in Section 3.4.1.7 of this safety evaluation.

The design team used the TriStation 1131 development tool to develop the Tricon V10 protection set application software. In addition, the design team used stand-alone computers, not connected to Invensys network, and with appropriate security controls to restrict access to only design team members. The Nuclear IV&V team used the TriStation emulator for verification of the application code.

When anomalies, non-conformances, and process deficiencies were encountered during the design, implementation, and test phases, Invensys resolved them in accordance with the Nuclear Systems Integration Program Manual, Sections 7.0 and 8.0, as implemented by PPM 10.0. The SCMP describes in detail the process for identification and control of anomalies. If resolution of the anomaly requires the preparation of an anomaly report (i.e., SIDR), the SIDR would accompany the software development checklist for the new version of the application program. During the June 3-5, 2014, regulatory audit, the NRC staff reviewed examples of SIDRs created to identify errors or problems encountered during testing.

After the software application was completed, verified, and validated, Invensys prepared a master disk, which included all files associated with the application software for the PPS replacement project.

The Invensys "Software Safety Plan (SSP)," 993754-1-911-P, dated October 13, 2011 (Reference 119), describes the activities implemented to ensure the project and system safety objectives were met. In addition, the Invensys PMP (Reference 114) describes major risks for the PPS replacement project and how they were managed to mitigate the identified risk factors.

Use of the Invensys SDP in conjunction with other software development plans, such as the Software Quality Assurance Plan (SQAP), SVVP, and SCMP, etc., which together with the SDP, addresses the SRP BTP 7-14 evaluation criterion for software development.

ALS

An evaluation of the development process for the generic ALS platform was performed by the NRC as part of the ALS platform topical report review. This evaluation is documented in the safety evaluation for the Advanced Logic System Topical Report (Reference 30).

Westinghouse did not prepare a software development plan for the DCPP PPS replacement project. Instead, Westinghouse described its design process in its "Management Plan," 6116-00000, September 2015 (Reference 105), and referenced NA 4.51, "Field Programmable Gate Array (FPGA) Development Procedure," as the software development plan; NA 4.51 was reviewed during the June 22-26, 2015, regulatory audit (Reference 39).

The PPS Management Plan describes the project organization and roles and responsibilities for Westinghouse personnel assigned to this project. Specifically, Westinghouse established a project team consisting of the different disciplines necessary to design, develop, and test the system. For example, the FPGA lead is responsible for the FPGA design and implementation. Westinghouse also identified the roles and responsibilities for the activities performed during the each project phase. The Management Plan defines the roles and responsibilities for the members of the project. This plan also defines the roles and responsibilities for the activities performed during each phase of the project lifecycle.

The Management Plan described the system lifecycle process, including inputs, tasks, processes, outputs, and exit criteria associated with each lifecycle phase. This plan identifies the following lifecycle phases: opportunity, planning, development, manufacturing, system test, installation, maintenance, and retirement. Note installation, operation, maintenance, and retirement phases are not within Westinghouse's scope for the DCPP PPS replacement project, and therefore were not included in the software development lifecycle process; these activities are PG&E's responsibility.

During the project lifecycle, Westinghouse performed design reviews in accordance with a WEC design review procedure. The design reviews are described in the "ALS Quality Assurance Plan," 6002-00001-P, dated October 25, 2012 (Reference 125), and the Management Plan. WEC performed a preliminary design review to evaluate the adequacy of the design review process, an intermediate design review at the completion of the development stage, and a final design review at the completion of the test phase. During the June 22-26, 2015, regulatory audit, the NRC staff reviewed the WEC design review procedure as well as the intermediate design review report.

Westinghouse used the PG&E "Functional Requirements Specification," Revision 7, dated October 25, 2012 (Reference 126), and "Interface Requirements Specification," Revision 7, dated October 23, 2012 (Reference 98), to develop the Diablo Canyon PPS ALS "System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127). This document was then used to create the design requirements of the ALS portion of the DCPP PPS replacement. The System Design Specification defines requirements and attributes applicable to the ALS subsystem design and the associated implementing processes. The system design specification was used to create the FPGA software requirements specification and software design description. WEC prepared "Diablo Canyon PPS Updated Scoping Tables and CD/ER Forms for Submittal to PG&E," to identify requirements not applicable to WEC. The NRC staff reviewed this document during the June 22-26, 2015, regulatory audit. This document was used in the preparation of the System Design Specification.

NA 4.51 defines the responsibilities, inputs, reviews, error reporting, tools, and development process followed for the design and development of its ALS system. Westinghouse uses an FPGA review checklist for review of FPGA requirements and its implementation during the FPGA development. Westinghouse also uses a non-volatile memory configuration specification to record system configuration and setpoints. During the June 22-26, 2015, regulatory audit, the

NRC staff reviewed examples of WEC's design reviews and records for the FPGA and non-volatile memory checklists.

Westinghouse used the OnTime™ defect tracking tool to record and track anomalies and non-conformance. Specifically, Westinghouse followed the instruction in its "Defect Management Work Instructions" for identification and resolution of such problems. The PPS Management Plan describes the approach to identify and resolve problems during the different lifecycle process stages. During design, problems were resolved by the project staff. After the development stage was complete, problems would be entered in the Westinghouse Corrective Action, Prevention and Learning (CAPAL). Westinghouse tracked software quality metrics throughout OnTime™ tickets, in accordance with its "Defect Management Work Instruction." During the June 22-26, 2015, regulatory audit, the NRC staff selected modifications proposed in several OnTime™ tickets to trace them until the resolution was implemented, approval was granted, and the ticket was closed. The NRC staff reviewed several CAPALs, including resolutions for those issues identified.

Westinghouse followed its quality assurance processes and procedures, defined in its "Quality Assurance Plan," 6116-00001, May 2014 (Reference 122), to assure quality in the design and test development of the ALS for the DCPP PPS replacement.

The WEC DCPP PPS "Management Plan," 6116-0000, September 2015 (Reference 105), includes the configuration management plan for the DCPP PPS replacement project. The Management Plan describes the planned method for change control of configuration items throughout the project lifecycle. The configuration management plan is described in more details in Section 3.4.1.7, "Software/Core Logic Configuration Management Plan," of this safety evaluation.

Westinghouse used the same tools used for the development of the ALS platform. These tools are described in the "Advanced Logic System Design Tools," 6002-00030, May 2015 (Reference 123).

SDP Safety Conclusion

The development of the Tricon and ALS subsystems of the DCPP PPS replacement project follow the lifecycle planning guidance of IEEE Std. 1074-1995 (Reference 86), as endorsed by RG 1.173 (Reference 85). The inputs/tasks, processes, and outputs/results activities for each of these phases include processes for V&V, software configuration, management, software quality assurance, software safety, and non-conformance resolution. The NRC staff has established reasonable assurance the software development processes used for the DCPP PPS replacement promotes high functional reliability and design quality of safety-related software suitable for its intended use.

3.4.1.3 Software/Core Logic Quality Assurance Plan

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.1.3, "Software Quality Assurance Plan (SQAP)" (Reference 46), provides guidance for evaluating a software quality assurance plan. The software quality assurance plan shall conform to the requirements of 10 CFR Part 50, Appendix B, and the applicant's overall quality assurance program. The regulations under 10 CFR Part 50, Appendix B state that the applicant shall be responsible for the establishment and execution of the quality assurance program. The applicant may delegate the work of establishing and executing the quality assurance program, or any part thereof, but shall retain responsibility for the quality assurance program. The software quality assurance plan would typically identify which quality assurance procedures are applicable to specific software processes, identify particular methods chosen to implement quality assurance procedural requirements, and augment and supplement the quality assurance program as needed for software.

Institute for Electrical and Electronics Engineers (IEEE) Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.1 (Reference 33), which is endorsed by RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011 (Reference 71), also provides guidance on software quality assurance. Also see the Invensys 993754-1-913-P, Revision 0, "Regulatory Guide 1.152 Conformance Report," dated September 6, 2011 (Reference 128).

IEEE Std. 7-4.3.2-2003, Clause 5.3.1, states, "Computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance plan consistent with the requirements of IEEE/Electronic Industries Association (EIA) Std. 12207.0-1996," and that "Guidance for developing software quality assurance plans can be found in IEEE Std. 730-1998."

<u>PG&E Quality Assurance Plan</u>

Section 4.5.3.1 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), identifies the DCPP "System Quality Assurance Plan (SyQAP)," dated May 9, 2013 (Reference 110), for the PPS replacement project as the quality assurance plan used by the licensee to meet the regulatory requirements stated above.

The SyQAP defines the organizational responsibilities for the various activities relating to software and logic quality assurance. It defines the methods used to ensure required software functions are performed correctly. The stated objectives of the SyQAP are to:

- Define the software quality assurance activities to be performed during the lifecycle of the software;
- Describe the responsibilities and authorities for accomplishing the planned software quality assurance activities;

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

Software and logic to be used in the PPS requires safety-related quality controls to meet software integrity level 4, as defined in IEEE 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74). PPS software and program logic will be provided by the two suppliers: Invensys and Westinghouse. Each of these vendors has an approved 10 CFR 50 Appendix B quality assurance program. Upon system turnover to the licensee, the SyQAP will provide the quality assurance requirements for nuclear safety-related software, programmable logic, and data. The processes defined in the SyQAP are used in conjunction with the ALS and Tricon software quality assurance plans, which are separately evaluated below. The licensee is responsible for acceptance, installation, and post-installation testing of software and logic changes, as well as continued operations and maintenance of the modified system in accordance with applicable technical specifications. In cases where quality assurance activities are required beyond the scope of the supplier, these activities will be performed by the licensee under the SyQAP quality assurance processes.

The SyQAP defines the overall organization for the PPS project. This includes the organizational structures relevant to software quality for each of the two suppliers, the contractors, and of the licensee. The SyQAP also delineates roles and responsibilities for the various quality-related tasks performed throughout the development lifecycles of the PPS subsystems (ALS portion and the Tricon portion of the PPS). The suppliers' lead verification engineers perform the role of software or logic application quality assurance manager as well as the project safety officer for each subsystem of the PPS.

The SyQAP defines supplier tasks related to assurance of software or application logic quality for each of the following phases of development:

- Project initiation and planning
- Conceptual design
- Requirements
- Design
- Implementation
- Integration
- Test

These phases do not directly align with the phases used in the ALS or Tricon development lifecycles; however, the SyQAP provides a table which correlates the DCPP-defined lifecycle activities to those used by each supplier. The SyQAP defines licensee tasks related to assurance of software quality for each of the following phases of development:

- Installation and checkout
- Operation
- Maintenance

The SyQAP defines the roles and responsibilities for each of the following individuals and teams responsible for performing software quality assurance activities:

- PG&E project manager
- Engineer of choice design change package team
- PG&E project engineering team
- 10 CFR 50 Appendix B suppliers
- Supervisor project quality assurance
- Project manager
- Project lead engineer
- Design team
- Testing and integration team
- Lead verification engineer (software quality assurance manager)
- Verification and validation staff
- Project quality assurance engineer or equivalent

The PG&E project manager has ultimate responsibility, authority, and accountability for all aspects of the project. The SyQAP also identifies documentation requirements for plant software. Quality documentation components include:

- Conceptual design document
- Functional requirements specification
- Interface requirements specification

- System verification and validation plan
- Site acceptance test plan
- Requirements traceability matrix
- System verification and validation final
- 10 CFR 50 Appendix B supplier documents
- System requirements specification
- Software V&V plan
- Software configuration management plan
- Baseline review report
- Requirements traceability matrix
- Software design description
- Software V&V reports
- Software safety plan
- Software requirements specification
- Software requirements review report
- User documentation

Additionally, the following supplier test documents are required:

- Software test plan(s)
- Security test plan(s)
- Software V&V final report

Tricon Quality Assurance Plans

An evaluation of the development process for the Tricon V10 platform was performed by the NRC as part of the review of the Triconex Approved Topical Report (Reference 29). This evaluation, which is documented in Section 3.2 of the Tricon platform topical report safety evaluation, includes reviews of the quality assurance manual and procedures used by Invensys to implement its quality assurance program.

During the Tricon V10 safety evaluation, the NRC staff reviewed the Tricon software qualification report and the associated documentation, and determined the Invensys quality assurance and engineering procedures were of sufficient quality to provide reasonable assurance the platform development process met the provisions for software planning documents as defined in BTP 7-14 (Reference 46). The NRC staff identified changes made to the software development processes, and determined that these changes did not result in any reduction to previous commitments made by Invensys.

Invensys also developed a project-specific “Software Quality Assurance Plan (SQAP),” 993754-1-801-P, dated March 14, 2012, for the DCPP PPS replacement (Reference 129). Four types of software are within the scope of this SQAP. They are:

- Test System Application Program (TSAP) software
- Embedded software including operating system software, communication software, and firmware used in the Tricon portions of the PPS
- Software development tools (including the TriStation 1131 software application) used during the Tricon software development process
- Software V&V tools

Of these software types, only the TSAP and embedded software are to be installed on the operating PPS safety-related system hardware. The TriStation 1131 software is intended to be loaded onto the maintenance work stations which are non-safety-related and do not perform any PPS safety functions. See the software tools evaluation in Section 3.10.1.1.2, “IEEE 7-4.3.2-2003, Clause 5.3.2, Software Tools,” of this safety evaluation for further information on Tricon software V&V and development tools.

Software development tasks performed by Invensys are defined in the project schedule; however, the quality assurance processes are applied to each of these development tasks as defined in the software quality assurance plan and the Tricon quality procedures manual. Quality assurance tasks defined by the SQAP cover the following areas of project development:

- Training
- Reviews and audits of project activities to verify compliance with project plans and procedures
- Inspections, tests, and reviews performed under the SVVP

Responsibilities for performance of quality assurance tasks are not assigned within the SQAP but are instead defined within the “Project Management Plan (PMP),” 993754-1-905-P, dated December 18, 2012 (Reference 114).

ALS Quality Assurance Plans

An evaluation of the development process for the ALS platform was performed by the NRC as part of the review of the Advanced Logic System Topical Report (Reference 30). This evaluation, which is documented in Section 3.2 of the ALS platform topical report safety evaluation, includes reviews of the “ALS Quality Assurance Plan,” 6002-00001-P, dated October 25, 2012 (Reference 125), and procedures used by Westinghouse to implement its quality assurance program.

Westinghouse developed a project-specific DCPP PPS "Quality Assurance Plan," 6116-00001, dated May 2014 (Reference 122). This plan was developed under the umbrella of the CSI quality assurance manual which is compliant with 10 CFR 50 Appendix B. The DCPP PPS Quality Assurance Plan was developed in accordance with the criteria of IEEE Std. 730-1998, "IEEE Standard for Software Quality Assurance Plans" (Reference 130). Its stated purpose is to define the techniques, procedures, and methodologies used by Westinghouse to assure quality in the design and test development of the ALS portion of the safety-related (Class 1E) PPS. The scope of the DCPP PPS Quality Assurance Plan includes the non-generic elements of the PPS project development lifecycle, including hardware and software.

Compliance to the Westinghouse quality management system is achieved through implementation of Westinghouse policies and procedures. The DCPP PPS Quality Assurance Plan includes tables in Appendix A which list project quality procedures used during system development. These tables define limits of applicability for these procedures. This was necessary due to a transition between Scottsdale, Arizona, operations to Westinghouse Monroeville, Pennsylvania, operations which occurred during the development of the DCPP PPS.

The quality assurance activities listed in the DCPP PPS Quality Assurance Plan include reviews of the following:

- Software requirements
- Preliminary design
- Critical design review
- Software V&V plan
- Software configuration management plan

The DCPP PPS Quality Assurance Plan includes requirements for performance of in-process functional and physical audit activities of the ALS application development and related processes. Requirements for planning and scheduling of audit activities based upon completion of critical phases of the project lifecycle are provided in the Quality Assurance Plan.

Software tools are used during the field programmable gate array (FPGA) development process; therefore, the NRC staff considers these tools to be a key component to the assurance of quality in the ALS development process. The PG&E SyQAP, Revision 1 (Reference 110), also states the tools, techniques, and methods used for software development are considered to be system quality assurance activities. Even though the ALS does not include a software development process, the software-based tools are used for the system development and are included as tools used to support quality assurance activities. See the software tools evaluation in Section 3.10.1.1.2, "IEEE 7-4.3.2-2003, Clause 5.3.2, Software Tools," of this safety evaluation for further information on ALS software V&V and development tools.

In regard to quality assurance requirements for software tools, the ALS Quality Assurance Plan refers to document 6002-00030, Advanced Logic System Design Tools, dated May 2015 (Reference 123). This document describes the tools used for application development and how they are used in the design process. It defines configuration management requirements for these tools and provides individual assessments of the tools used for ALS system development. Assessments are made for FPGA design tools, IV&V simulation tools, schematic capture and printed circuit board layout tools, analog circuit simulations, concurrent versioning system version control system, change management tools, and ALS test tools. The NRC staff reviewed these assessments and determined all software-based tools used to support system development activities are identified and are included within the ALS configuration management program. These assessments adequately identify the expected usage for each tool and define appropriate limitations and controls to be applied during tool usage activities. The assessments also identify relevant tool operating experience as well as justification for tool selections. The NRC staff concludes the processes being used for ALS tool selection and use provide an adequate level of quality assurance when used as defined and are therefore acceptable for use in the development of nuclear safety-related applications.

Software Quality Assurance Plan Safety Conclusion

The software quality assurance plans, as implemented by the licensee and vendor quality programs, are compliant with the requirements of IEEE Std. 730-1998 and, therefore, provide reasonable assurance that high-quality software capable of performing safety functions is produced for the DCPP PPS application.

3.4.1.4 Software/Core Logic Integration Plan

The acceptance criteria for a software integration plan are contained in SRP BTP 7-14, Section B.3.1.4, "Software Integration Plan (SIntP)" (Reference 46). This section states that RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 85), endorses IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (Reference 86), and that within the standard, Clause A.1.2.8, "Plan Integration," contains an acceptable approach relating to planning for integration. Clause A.1.2.8 states that software requirements and the software design description should be analyzed to determine the order for combining software components into an overall system, and that the integration methods should be documented. The integration plan should be coordinated with the test plan. The integration plan should also include the tools, techniques, and methodologies needed to perform the integrations. The planning shall include developing schedules, estimating resources, identifying special resources, staffing, and establishing exit or acceptance criteria.

NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," dated June 11, 1993, Section 3.1.7, "Software Integration Plan," and Section 4.1.7, "Software

Integration Plan" (Reference 131), provides additional guidance on software integration plans. Section 3.1.7 states that software integration should consist of three parts: (1) integrating the various software modules together to form a single program, (2) integrating the result of this with the hardware and instrumentation, and (3) testing the resulting integrated product.

PG&E

Section 4.5.4 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), states that software integration plans provided by the vendors Invensys and Westinghouse provide the information necessary to meet the regulatory requirements stated above. The licensee did, however, submit a document entitled "Interface Requirements Specification," dated October 23, 2012 (Reference 98), which specifies the interface design details for integrating the PPS with other connected systems as well as integrating the individual parts of the PPS with each other.

Tricon

The integration plan governing the development of the Tricon portion of the PPS is provided by the "Software Integration Plan (SIntP)," 993754-1-910-P, dated October 14, 2011 (Reference 117). The Tricon SIntP describes the strategy used for integrating the Tricon V10 protection set software functions into a Test System Application Program (TSAP). It also describes the processes used for integrating the TSAP with the Tricon V10 hardware. There are three major steps to the Tricon integration process:

1. Integrating various software programs into a single TriStation 1131 project file.

2. Integrating the TriStation 1131 project file with the Tricon V10 hardware.

3. Testing the integrated Tricon V10 product.

During the first integration of software programs step, pre-approved TriStation 1131 function blocks are assembled to implement the protection functions to be performed by the system. These functions are defined by the system software design description document. Once these function blocks are assembled into completed function block diagrams, individual TriStation 1131 programs are combined into a project master TSAP project file. When a TSAP is issued, it is sent to the software independent verification and validation (IV&V) team for formal review and verification testing prior to installation of the software onto a V10 hardware platform.

During the second integration step, the TSAP software is loaded into the Tricon V10 hardware in the vendors' assembly area. It is in this area where the system integration, construction, assembly, inspection, and testing activities are conducted. Once the Tricon equipment is staged and powered, control of the equipment is turned over to the IV&V group for performance of system validation testing activities.

In the final testing step of the integration process, the IV&V team performs testing activities defined by the hardware validation test and factory test procedures. During this test phase, the IV&V staff conducts tests and maintains configuration control over the equipment under test as well as test tools and documentation.

The ALS portion of the PPS is not considered to be within the scope of the Tricon SIntP and is not integrated with Tricon equipment nor tested during the Tricon test phase.

ALS

Section 4.5.4 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), identifies the CS Innovations (CSI) field programmable gate array (FPGA) development procedure as well as the ALS electronics development procedure as the ALS documents that meet the guidance for system integration in BTP 7-14, Section B.3.1.4 (Reference 46), and RG 1.173 (Reference 85).

The FPGA development process involves several levels of integration. The activities associated with performing integration are defined within the ALS FPGA development procedure. This procedure covers all aspects and phases of the development lifecycle. The integration activities are:

- Board integration – This activity integrates completed and tested modules into a finished FPGA design.
- System integration – This activity integrates completed ALS FPGA designs into a connected system based on two or more ALS boards. System integration allows testing and simulation of multiple FPGA designs.
- Board verification – This is a test of completed ALS boards with installed FPGA designs to verify the requirements of the system component.
- System verification – This is an overall integrated system test to verify system requirements on the completed and fully integrated ALS system.
- Synthesis.
- Place and route.

Software Integration Plan Safety Conclusion

The software integration plans, as implemented by the licensee and vendor programs, are compliant with the requirements of IEEE Std. 1074-1995 (Reference 86) and, therefore, provide reasonable assurance that an acceptable method of software integration was used.

3.4.1.5 Software/Core Logic Safety Plan

The acceptance criteria for a software safety plan are contained in the SRP BTP 7-14, Section B.3.1.9, "Software Safety Plan," and Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities" (Reference 46). These sections state that the software safety plan should provide a general description of the software safety effort, and the intended interactions between the software safety organization and the general system safety organization. It further states that NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Section 3.1.5, "Software Safety Plan," and Section 4.1.5, "Software Safety Plan" (Reference 131), contain guidance on software safety plans. Further guidance on safety analysis activities can be found in NUREG/CR-6101 and Regulatory Guide (RG) 1.173, Section C.3, "Software Safety Analyses" (Reference 85), contains guidance on safety analysis activities.

PG&E's PPS replacement "Concept, Requirements, and Licensing Phase 1 Project Plan," (Reference 109), and the "System Quality Assurance Plan (SyQAP)" (Reference 124), provided in the licensee's letter dated October 26, 2011 (Reference 1), describe software development activities, software reviews, problem reporting, and corrective actions for the PPS replacement project. PG&E did not develop software for the PPS replacement project, so a PG&E software safety plan was not submitted. Furthermore, PG&E will not perform software modifications to the systems. Such modifications, if necessary, will be performed by the 10 CFR 50 Appendix B suppliers. Section 3.1 of the PG&E project plan provides a brief description of each phase of the development process, including responsibilities for each sub-vendor.

<u>Tricon</u>

The Invensys "Software Safety Plan (SSP)," 993754-1-911-P, dated October 13, 2011 (Reference 119), defines the plan to identify, document, and resolve software safety concerns regarding the development of the Test System Application Program (TSAP) for the DCPP PPS. Note the Tricon firmware is not part of the scope because the qualification and safety aspects were evaluated during the review of the Triconex Approved Topical Report (Reference 29).

The Invensys "Project Management Plan (PMP)," 993754-1-905-P, dated December 18, 2012 (Reference 114), defines the project organization and roles and responsibilities for Invensys personnel involved in the PPS replacement project. This information is described in Section 3.4.1.1 of this safety evaluation. The Invensys SSP defines the relationship between the Invensys organizations involved in the PPS replacement project. The SSP also defines the organization responsibilities and staff qualifications necessary to perform the activities described in the SSP. For software safety activities, Invensys identifies the software safety officer, who is responsible for the overall software safety program, and the Nuclear IV&V engineer, responsible for performing the software safety activities.

The software safety activities were performed during the requirement, design, implementation, and testing phases of the TSAP development lifecycle. The SSP defined the specific tasks performed during the TSAP development lifecycle. In particular, the Nuclear IV&V engineer performed a safety analysis during each phase, and maintained the traceability of the software safety requirements in the project traceability matrix. These reviews included evaluation of software documentation (e.g., software requirements specification and software design specification), as well as code reviews. During the June 3-5, 2014, regulatory audit (Reference 38), the NRC staff reviewed Invensys software safety processes including the SSP and the procedures used during PPS software safety analysis activities with representatives of the Invensys quality assurance and IV&V organizations to assess the effectiveness of these programs in achieving this objective.

The safety analysis activities included a comprehensive evaluation of the software safety. Invensys prepared a "Safety Analysis," 993754-1-915-P, dated December 9, 2014 (Reference 132), to document the methodology and results of the safety analysis. In particular, this evaluation determined whether new software hazards were introduced or if existing hazards were controlled. During this evaluation, if the Nuclear IV&V engineer identified a software safety concern, this concern would be included in the verification test procedures and/or validation test plan. Furthermore, when a safety issue was identified, it was resolved informally between the Nuclear Delivery engineer and the IV&V engineer. If the safety issue could not be resolved, it was escalated to the project manager and software safety officer for technical resolution. Assessment, resolution, and mitigation measures were documented in accordance with the "Nuclear Systems Integration Program Manual," dated July 9, 2010 (Reference 112). If mitigation measures included modifications to the software requirements and/or software design, Invensys performed a change impact analysis to assess the change required in the TSAP. The Invensys SSP describes the procedure used to perform the change impact analysis. During the regulatory audit, the NRC staff observed software safety analysis activities performed were proportionate with the requirements for software integrity level 4 software, as defined in the software V&V plan.

In addition to the safety analyses performed during each phase of the software lifecycle, the IV&V report for each phase included a summary of the software safety effort. In addition, the final V&V report included an assessment of the overall software safety effort. This information is described in Section 3.4.2.2.1, "Tricon IV&V Summary Report Evaluation," of this safety evaluation.

Invensys recorded software safety data to determine the effectiveness of the software effort. The data gathered was included in each phase of the software lifecycle.

ALS

The WEC Diablo Canyon PPS "Software Safety Plan," 6116-10020, January 2015 (Reference 133), describes the approach and methodology used to identify, evaluate, and mitigate potential hazards through the development of the ALS-based system for the PPS replacement project.

The Software Safety Plan identifies the organization and personnel responsible for software safety. Specifically, this plan shows the product manager responsible for the safety software activities performed for this project. This plan also identifies the WEC team assigned to the different software safety activities. The design team is responsible for software safety during the requirement and design phases. The IV&V team is responsible for the software safety analysis, hazard analysis, and risk analysis performed through the project lifecycle of the PPS replacement system. The quality team audits implementation of the Software Safety Plan.

The Software Safety Plan describes the software safety activities performed during the system lifecycle, as well as techniques to be used to perform such analysis. WEC documented the results of safety analysis in its IV&V summary reports. These reports provide recommendations to address any deficiency or problem. Section 3.4.2.2.2, "ALS IV&V Summary Report Evaluation," of this safety evaluation summarizes the results of the software safety activities.

The WEC Project Management Plan and V&V Plan define the process to report, document, and resolve anomalies and errors. This information is described in Section 3.4.1.1, "Software/Core Logic Management Plan," of this safety evaluation.

Software Safety Plan Safety Conclusion

The Software Safety Plan provides a list of software safety activities. For each of these activities, a software safety evaluation is conducted and the results documented in the appropriate phase V&V summary report. The NRC staff performed an assessment of the performance of these activities and determined that planning for software safety is appropriate for the DCPP PPS replacement and is, therefore, acceptable. Furthermore, the NRC staff concludes the software safety plan, as executed, provides adequate assurance that the various software safety activities will resolve safety issues presented during the design and development of the safety application software.

3.4.1.6 Software/Core Logic Verification & Validation Plan

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.1.10, "Software Verification and Validation Plan (SVVP)" (Reference 46), provides guidance to evaluate a software verification and validation (V&V) plan. Regulatory Guide (RG) 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013 (Reference 73), endorses IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74), as providing methods acceptable for meeting the applicable regulatory requirements listed in Section 2.0 of this safety evaluation. BTP 7-14, Section B.3.1.10.1, "Management Characteristics of the SVVP," states that management characteristics of the SVVP should exhibit purpose, organization, oversight, responsibilities, and risks.

The PG&E DCPP PPS replacement project "System Verification and Validation Plan (SyVVP)," dated February 19, 2013 (Reference 111), meets the guidance of BTP 7-14 Section B.3.1.3, "Software Quality Assurance Plan (SQAP)," and RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (Reference 85), and defines the activities to be followed in the V&V for the PPS replacement project by PG&E, IOM, and WEC.

The verification and validation (V&V) activities for the PPS replacement project were governed by the suppliers' respective quality assurance programs. The V&V activities for Invensys are described in the Invensys PPS replacement DCPP "Software Verification and Validation Plan (SVVP)," 993754-1-802-P, dated December 18, 2012 (Reference 118). The V&V activities for ALS are described in Westinghouse's "ALS V&V Plan," 6002-00003-P, January 2013 (Reference 134), DCPP "Management Plan," 6116-00000, September 2015 (Reference 105), "Diablo Canyon PPS VV Plan," 6116-00003, November 2014 (Reference 135), and DCPP "Test Plan," 6116-00005, October 2014 (Reference 136). These plans were reviewed and accepted by PG&E to ensure the V&V effort is complete. These documents met the guidance of BTP 7-14, Section B 3.1.3, and NRC RG 1.173. These plans established the requirements for the V&V process to be applied to the software developed for the PPS replacement project.

The SyVVP establish the goals, processes, and responsibilities required to implement effective system level V&V for the PPS replacement project at DCPP. Specifically, the SyVVP describes activities performed by the responsible parties: PG&E, Altran, Invensys, and Westinghouse. Further, the PG&E DCPP PPS replacement "Concept, Requirements, and Licensing Phase 1 Project Plan" (Reference 109), Section 5, describes the V&V activities performed during lifecycle activities for the PPS replacement project for which PG&E was responsible.

As previously described in the Software Development Plan (Section 3.4.1.2, "Software/Core Logic Development Plan," of this safety evaluation), PG&E performed the following lifecycle phases: project initiation phase, conceptual design phase, installation and checkout phase, operation phase, and maintenance phase. The SyVVP does not cover V&V tasks for PG&E operation phase and maintenance phase.

During the concept phase, PG&E identified system requirements, then Altran prepared design documents. As described in the licensee's letter dated May 9, 2013 (Reference 13), verification and acceptance of the concept phase documents was performed in accordance with PG&E procedure CF7.ID4, "Processing of Documents Received from Suppliers." As stated in its letter dated January 25, 2016 (Reference 20), PG&E quality verification personnel assessed the technical adequacy of design phase documentation that was developed by PG&E and Altran Solutions personnel. The output of PG&E's concept phase (i.e., interface requirements specification and functional requirements specification) was used by IOM and WEC in accordance with their approved procedures to develop, implement, and test their respective systems.

In its letter dated January 25, 2016 (Reference 20), the licensee stated that during testing of the PPS replacement system, PG&E participated in the factory acceptance testing (FAT) by reviewing the FAT plan documents, witnessing the FAT for one protection set, reviewing the FAT test reports, and verifying that non-conformances were entered in the corrective action system.

The SyVVP describes the V&V activities to be performed by PG&E, Westinghouse, and Invensys during the installation and checkout phase. PG&E will perform the site acceptance test and design verification test. The site acceptance test will test the integrated PPS replacement system using the transmission of live 4-20 milliampere analog reactor coolant system temperatures from the ALS to the Tricon V10. During the site acceptance test, PG&E will verify that installed software corresponded to the software or logic subjected to V&V, and validate that all site-dependent parameters or conditions to verify supplied values are correct. The licensee will perform the design verification test on the PPS once it is fully installed. The design verification test will be performed in accordance with PG&E plant procedure CF3.1D9, "Design Change (Package) Development." PG&E will be responsible for acceptance of the results of the site acceptance test and design verification test.

The licensee prepared a requirements traceability matrix (RTM) to document the V&V of specified requirements. This RTM includes requirements that were not included in the V&V scope of Invensys and WEC. An inspection follow-up activity is included in Section 3.14.3, "Licensee Site Inspection Follow-up Items," of this safety evaluation to confirm implementation of licensee-scope requirements prior to system startup.

The SyVVP, Section 6, identifies the requirements for V&V reporting. PG&E requires that both Invensys and WEC prepare task reports, V&V activity summary reports, and the final V&V report. Invensys and WEC prepared V&V reports in accordance with their procedures, and then they prepared a final V&V report, "Tricon V10.5.2, V&V Test Report," Revision 1.1, dated January 14, 2011, summarizing these reports (Reference 137).

In addition, the SyVVP, Section 6, requires that anomalies detected are identified, documented, and resolved during the V&V activities. PG&E requires that anomaly reporting after the system is delivered to the site is performed in accordance with its "Problems Identification and Resolution." During FAT, PG&E confirmed that anomalies and non-conformances were captured in the vendors' corrective action systems (Reference 20).

The NRC staff also evaluated the DCPP PPS V&V task summary reports. The results of these evaluations are described in Section 3.4.2.2, "V&V Analysis and Reports," of this safety evaluation.

Tricon

Invensys PPS replacement "Software Verification and Validation Plan (SVVP)," 993754-1-802-P, dated December 18, 2012 (Reference 118), specifies activities to be performed during the application software management and development processes intended to demonstrate high levels of quality and confidence in the software being developed. The licensee provided a document of conformance to IEEE Std. 1012-1998 (Reference 74), in Appendix D of SVVP 993754-1-802-P.

The Invensys SVVP describes the requirements for the V&V process to be applied to the Test System Application Program (TSAP) software developed for the PPS replacement project, running on the safety-related Tricon V10 platform hardware. This SVVP also describes the Tricon V10 system hardware interface with Advanced Logic System (ALS) (but not the ALS functions themselves) and maintenance work station. These ALS inputs to the Tricon V10 were simulated during the factory acceptance testing (FAT), as discussed in the Invensys DCPP "Validation Test Plan (VTP)," 993754-1-813-P, dated December 18, 2012 (Reference 138). The Invensys quality assurance manual, policy and procedures manual, quality procedure manual, and engineering department manual procedures provide the basis for the V&V of the TSAP.

For system integration and validation, Invensys prepared the "Software Verification Test Plan (SVTP)," 993754-1-868-P, dated April 3, 2014 (Reference 139), "Software Verification Test Specification," 993754-1-869 (not required to be submitted), "Validation Test Plan (VTP)," 993754-1-813-P (Reference 138), and "Validation Test Specification (VTS)," 993754-812-P, dated April 4, 2014 (Reference 140). These plans and specifications provide detailed descriptions of the tests, testing approach, features to be tested, requirements, acceptance criteria, and procedures.

The Invensys PPS "Project Management Plan (PMP)," 993754-1-905-P, dated December 18, 2012 (Reference 114), describes Invensys project organization for the PPS replacement project. In addition, the Invensys SVVP (Reference 118), describes the organizational structure and interfaces of the PPS replacement project associated with V&V activities. This plan states the V&V organization for the PPS replacement project involves: Nuclear Delivery, the Nuclear IV&V team, and Nuclear Quality Assurance. Each of these organizations play a specific role in the Tricon V10 application project lifecycle. Invensys engineering is responsible for designing and maintaining the Tricon V10 platform, and Nuclear Delivery is responsible for working with nuclear customers on safety-related Tricon V10 system integration projects. Invensys engineering is not directly involved in system integration, but Nuclear Delivery may consult with engineering on technical issues related to the Tricon V10 platform. In addition, the PMP describes organizational boundaries between Invensys and the other external entities involved in the PPS replacement project: PG&E, Altran, Westinghouse, and Invensys suppliers. The combination of the PMP and SVVP demonstrate compliance of the Invensys organization with RG 1.168 (Reference 73).

Nuclear IV&V is responsible for ensuring that Nuclear Delivery has adequately met the safety system requirements as defined in contract documents, design input documents, regulatory requirements, and Invensys procedures. Figure 3 of the Invensys' PPS PMP, dated December 18, 2012 (Reference 114), shows that Nuclear IV&V is independent of Nuclear Delivery. This ensures that Nuclear IV&V is not adversely impacted by schedule pressure and financial/budget constraints. Nuclear Quality Assurance is responsible for ensuring that Nuclear Delivery and Nuclear IV&V are adhering to applicable procedures and processes for nuclear safety-related system development.

The Invensys SVVP requires the use of V&V metrics to evaluate software development process and products. By letter dated May 9, 2013 (Reference 13), Invensys explained the V&V metrics to be used during the development of the Tricon portion of the PPS replacement system. In particular, Invensys tracked the number of defects and non-conformances during the lifecycle process to determine software quality and measure effectiveness of the V&V activities to produce a system with no technical defects. Invensys reported the software metrics in its V&V summary reports.

The Invensys SVVP identifies requirements for anomaly reporting and resolution for the PPS replacement project. Invensys followed the process described in Project Procedures Manual (PPM) 10.0 to identify and control non-conforming items for nuclear applications. In particular, Invensys used its System Integration Deficiency Report (SIDR) to document non-conformances and corrective actions during testing. During the June 3-5, 2014, regulatory audit (Reference 38), the NRC staff reviewed examples of SIDRs created to identify errors or problems encountered during test. In addition, the V&V summary reports describe anomalies reported on SIDR for each lifecycle phase.

Invensys personnel also prepared a test log to record all testing activities, deficiencies, and testing personnel. The Invensys Project Review Committee was responsible for review and approval of dispositions for SIDRs and review of the test log. In addition, Invensys used the document review comment sheet to track and resolve comments during documents review.

The Invensys SVVP identifies the nuclear independent verification and validation (IV&V) manager as the person responsible for evaluating risks associated with V&V tasks, and also for assigning appropriate resources for their resolution. Invensys's PMP describes the major risk factors for this project, as well as the monitoring and control mechanisms to mitigate the identified risk factors. The V&V activity summary report for each phase summarizes the risks encountered in the associated phase. Section 3.4.2.2.1, "Tricon IV&V Summary Report Evaluation," of this safety evaluation describes and evaluates Invensys IV&V summary reports.

The Invensys SVVP describes the tools, techniques, and methods used for V&V activities throughout the PPS replacement project. Invensys does not strictly follow IEEE Std. 1012 (Reference 74) guidelines for V&V; however, the NRC staff reviewed the SVVP and during audit, the staff observed that verification techniques used by Invensys included design document review and code walkthrough to verify the correctness of code modifications and functionality enhancements. Validation activities include functional tests, including regression testing, of the integrated system in accordance with written test procedures.

The Invensys "Validation Test Plan (VTP)," 993754-1-813-P (Reference 138), describes the tools, techniques, and methods used for system integration and validation. In addition, Invensys prepared a project traceability matrix, which was updated through the system lifecycle to trace requirements defined in the DCPP's system specifications. Note during the requirements and design phase, the Nuclear Delivery group was responsible for the project traceability matrix, and during implementation and test phase, the Nuclear IV&V was responsible.

Invensys prepared a V&V activity report for each lifecycle phase. Section 6 of the SVVP describes the content of these reports. Section 3.4.2.2.1, "Tricon IV&V Summary Report Evaluation," of this safety evaluation discusses the V&V activity summary reports.

ALS

An evaluation of the development process for the ALS platform was performed by the NRC as part of the review of the ALS platform topical report 6002-00031-P-A, "ALS Diversity Analysis," January 2013 (Reference 141). This evaluation includes a review of the "ALS V&V Plan," 6002-00003-P, January 2013 (Reference 134), used by Westinghouse to perform V&V activities. Westinghouse prepared "Diablo Canyon PPS VV Plan," 6116-00003, November 2014 (Reference 135), to define supplemental V&V information specific to the DCPP PPS replacement project.

The Diablo Canyon PPS VV Plan defines the activities and methodologies to perform V&V tasks for the development of the application software. In addition, the plan provides references to Westinghouse procedures that have superseded procedures described in the "ALS V&V Plan," 6002-00003-P.

The DCPP PPS "Management Plan," 6116-00000, September 2015 (Reference 105), defines the organization and roles and responsibilities for the DCPP PPS replacement project. This information is summarized in Section 3.4.1.1, "Software/Core Logic Management Plan," of this safety evaluation. The independent verification and validation (IV&V) organization reports to a different management than the development team. However, in "Diablo Canyon PPS VV Plan," 6116-00003, November 2014 (Reference 135), Westinghouse explained that the organization model for this project is modified per the description from IEEE Std. 1012-1998. During the June 22-26, 2015, regulatory audit (Reference 39), Westinghouse explained how it met the requirements in RG 1.168 for independence of the V&V group.

The Diablo Canyon PPS VV Plan describes the test tools used to perform testing during the design and IV&V activities. IV&V testing activities were performed at the component level and then during system integration. For the component level, Westinghouse used its "ALS Platform FPGA VV Test Plan," 6002-00018, February 2013 (Reference 142). For the system integration, Westinghouse followed its "Test Plan," 6116-00005, October 2014 (Reference 136). A description of system testing is provided in Section 3.4.1.8, "Software/Core Logic Test Plan," of this safety evaluation.

The lifecycle process for the DCPP PPS replacement project is defined in the DCPP PPS "Management Plan," described in Section 3.4.1.1, "Software/Core Logic Management Plan," of this safety evaluation. The Diablo Canyon PPS VV Plan describes the tasks performed in each phase, as well as documents prepared. The VV Plan also describes the managerial and technical reviews of activities, documentation, and test evaluation. In addition, Westinghouse used DOORS® to track system requirements and perform its traceability analysis.

Westinghouse tracked anomaly metrics for its evaluation. The IV&V summary report summarizes the anomalies observed during each phase. The "ALS V&V Plan," 6002-00003-P, January 2013 (Reference 134), describes how anomalies were tracked, reported, and resolved. Section 3.4.1.2, "Software/Core Logic Development Plan," of this safety evaluation discusses Westinghouse's process to report anomalies.

SVVP Safety Conclusion

The V&V groups for Invensys and Westinghouse were technically, managerially, and financially independent from the software design organizations. The V&V groups performed the various software lifecycle activities listed in the software V&V plans, which provides V&V task descriptions, inputs, and outputs for each lifecycle process. V&V reports were prepared for each software lifecycle phase capturing analysis, risks, and issues. The software V&V plans adequately address the V&V planning guidance in BTP 7-14, IEEE Std. 1012-1998, and IEEE Std. 7-4.3.2-2003, Clauses 5.3.1.1, 5.3.3, and 5.3.4, and, therefore, the NRC staff determines that the software V&V plans are acceptable.

3.4.1.7 Software/Core Logic Configuration Management Plan

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.1.11, "Software Configuration Management Plan (SCMP)" (Reference 46), provides guidance to evaluate the software configuration management plan, and states that IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," Clause 7.2 (Reference 86), provides an acceptable approach to software configuration management. IEEE Std. 1074-1995, Clause 7.2.1 states that software configuration management identifies the items in a software development project and provides both for control of the identified items and for reporting the status of such items to management to maintain visibility and accountability throughout the software lifecycle. Examples of items to be controlled include, but are not limited to, code, documentation, plans, and specifications. BTP 7-14, Section B.3.1.11.1, "Management Characteristics of the SCMP," asks for the definition of the responsibilities and authority of the software configuration management organization.

PG&E, Westinghouse, and Invensys were responsible for the software management of the PPS replacement project.

PG&E

PG&E's DCPP Procedure CF2, "Computer Hardware, Software and Database Control" (Reference 106), establishes overall policies and general requirements related to the quality and security of computer hardware, software, and database control processes for the plant. PG&E's DCPP Procedure CF2.1D2, "Software Configuration Management for Plant Operations and Operations Support" (Reference 107), identifies requirements for preparing the software configuration management plan and software quality assurance plan and maintaining configuration control of computer systems and applications. Using this information, PG&E prepared PG&E the PPS replacement "Software Configuration Management Plan (SCMP)," SCM 36-01, Revision 1, dated March 18, 2013 (Reference 143), to describe the PG&E software configuration management activities associated with the PPS replacement project after shipment and installation of the system. As described in the licensee's letter dated May 9, 2013 (Reference 13), this plan states that changes or upgrades to the Tricon application program would be performed by Invensys, and changes or upgrades to the code in the ALS platform would be performed by Westinghouse. Note that PG&E will have limited capability to change the non-volatile random-access memory configuration for a specific ALS input/output board to support board replacement (such as to replace a failed board) by loading non-volatile random-access memory images that are under CS Innovations (CSI) configuration control and that have been previously verified and validated at the system level by CSI. Configuring the non-volatile random-access memory in order to replace an ALS input/output board will be performed by PG&E under an approved plant maintenance procedure.

Diablo Canyon Procedure CF2.1D2 describes the overall DCPP organization and responsibilities for configuration management. The roles and responsibilities identified for PPS replacement project are described in Section 2 of the PG&E SCMP. In particular, the PG&E SCMP identifies the applicant sponsor as the person responsible for the system, the system coordinator who will be responsible for the technical aspects and maintenance of the system and its associated peripheral and software, as well as control of software documentation, and the system team, who comprises of support staff necessary to ensure the PPS operates properly. The system coordinator is responsible of maintaining configuration control. In the case a modification is required, the applicant sponsor will evaluate and identify maintenance activities and or modifications that may require hardware or software changes and then work with the system coordinator and the system team to address activities required for this request (i.e., modify ALS non-volatile random-access memory configuration).

The PG&E SCMP, Section 3.1, describes the configuration items covered under configuration management, such as commercial off-the-shelf hardware, software, firmware, etc. For the PPS replacement project, PG&E established the baseline for the Triconex operating system, application software, and database, and the field programmable gate array (FPGA) configuration and database for the ALS system at the time the equipment is shipped and placed in operation. After this, changes can be made through a formal request change. As mentioned before, PG&E does not have the capability to modify the FPGA in the ALS system and the Tricon functional software. These activities will be performed by Westinghouse or Invensys in accordance with their 10 CFR 50 Appendix B procedures.

In case that problems are identified, PG&E will report them in accordance with PG&E "Problem Identification and Resolution" and will be tracked using safety application protocol notifications. The Problem Identification and Resolution procedure provides guidance for identifying, evaluating, and resolving problems. Depending on the problem reported, the resolutions would vary, and in case those corrective actions do not resolve the problem, a new notification would be initiated for long-term actions. DCPP managers are responsible for closing notifications. If an event needs to be reported to the NRC (as required by 10 CFR Part 21), PG&E will follow the guidance in its administrative procedure XI1.ID2, "Regulatory Reporting Requirements and Reporting Process." During software development of the PPS replacement system, the vendors' anomaly reporting procedures were used. PG&E evaluated reported deviations or anomalies which occurred during software development and testing, as described in its letter dated January 25, 2016 (Reference 20).

Tricon

The Invensys "Software Configuration Management Plan (SCMP)," 993754-1-909-P, dated December 18, 2012 (Reference 116), describes software configuration management activities for the Triconex portion of the DCPP PPS replacement project. This plan defines software configuration management activities performed, Invensys personnel responsible for doing software configuration management activities, the schedule for such activities, and resources required. In addition, Invensys staff uses the following procedures:

- Engineering Department Manual (EDM) 20.00, "Configuration Management," dated October 28, 2009 (Reference 144), addresses the configuration management measures for Triconex products from the design stages until release of the product.
- EDM 24.00, Software Configuration and Change Control," dated April 8, 2005 (Reference 145), addresses software configuration and control.
- Project Procedures Manual (PPM) 4.0, "Project Document Control and Data Control," describes the process for preparing and controlling project documents.
- PPM 2.0, "Design Control," describes the design controls for documentation associated with application projects.

EDM 20.00 and EDM 24.00 were reviewed during the evaluation of the Triconex platform under the Triconex Approved Topical Report (Reference 29). PPM 4.0 and 2.0 were reviewed during the November 13-16, 2012, regulatory audit (Reference 36).

Invensys applies configuration management to each protection set firmware, libraries and modules, software engineering tools, and software documentation. Further, the version of the firmware provided with each protection set is identified on the hardware modules. Other software to be controlled includes the operating system software of the computers running the TriStation 1131, the signal simulation software used for testing, and software nuclear IV&V tools.

Section 2 of the Invensys SCMP describes that the Invensys Nuclear Delivery group is responsible for software configuration management activities. Specifically, the developer of the Test System Application Program (TSAP) (i.e., application engineer) is responsible for software configuration management. During the November 13-16, 2012, regulatory audit, the NRC staff discussed the process described in Project Instruction 7.0 for TSAP configuration management, and found that they were acceptable. After the TSAP is completed, the project engineer reviewed the TSAP and associated documentation. Review of the TSAP was recorded in the software development checklist. Review of documentation and comments/modifications were recorded in the design review checklist, design review comment sheet, and a document review release in accordance with PPM 3.0, "Drawing Preparation & Control." The project manager was responsible for approving modifications. All software development checklists and document review releases were recorded in their respective logs.

ALS

The Westinghouse "ALS Configuration Management Plan," 6002-00002-P, Revision 11, March 2015 (Reference 146), describes configuration management activities for developing the ALS platform and project-specific applications, in this case for the DCPP PPS replacement project. Evaluation of this plan was performed by the NRC as part of the review of the ALS platform Advanced Logic System Topical Report (Reference 30). Note the ALS Configuration Management Plan was modified to align with WEC quality assurance procedures after the closure of CS Innovations (CSI).

The ALS Configuration Management Plan for the DCPP PPS replacement project is included within the DCPP PPS "Management Plan," 6116-00000, September 2015 (Reference 105). The Management Plan describes the method for identifying change control of configuration items throughout the project lifecycle. In addition, this plan states that the project manager is responsible for issuing baselines in accordance with the project milestones identified in the plan. The ALS Configuration Management Plan and the Management Plan govern the configuration management for the DCPP PPS replacement project.

The Management Plan identifies and describes the organization responsible for configuration management activities. CSI and Westinghouse used the "Diablo Canyon PPS Configuration Status Accounting (CSA)" to track configuration items for the DCPP PPS project. Westinghouse later replaced the CSA with the DCPP PPS "Configuration Management Report," 6116-00400, Revision 7, October 2015 (Reference 147), the DCPP PPS "Configuration Management Baseline Report," 6116-00401, October 2015 (Reference 148), and the Document Index. The PPS Configuration Management Report includes lower level configuration items and the PPS Configuration Management Baseline Report summarizes the project baseline configuration items. The Document Index is a Microsoft Access database used to control configuration items, baselines, and releases related to the DCPP PPS project.

Westinghouse uses its Enterprise Document Management System as the official repository for all DCPP-approved documents and configuration items.

SCMP Safety Conclusion

The NRC staff determined the software configuration management processes and activities performed meet the requirements of IEEE Std. 828-1998, "IEEE Standard for Software Configuration Management Plans" (Reference 77), and ANSI/IEEE Standard 1042-1987, "IEEE Guide to Software Configuration Management" (Reference 78), and are therefore acceptable. In particular, the NRC concludes that both vendors established a process to control software items through a librarian, and it also provides a process to control code or documentation changes through a configuration control board. The software configuration management plans adequately address the guidance in BTP 7-14 (Reference 46), which describes the acceptance criteria for software configuration management and the methods and tools to identify and control the system and programming throughout the software development process and use.

3.4.1.8 Software/Core Logic Test Plan

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.1.12, "Software Test Plan (STP)" (Reference 46), provides guidance to evaluate a software test plan. IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation" (Reference 80)," as endorsed by RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, July 2013 (Reference 79), provides an acceptable method for providing test documentation. IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing" (Reference 82), as endorsed by RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (Reference 81), provides an acceptable method for satisfying software unit test requirements. BTP 7-14, Section B.3.1.12.4, "Review Guidance for the STP," states the software test plan (STP) should cover all testing done to the software, including unit testing, integration testing, factory acceptance testing (FAT), site acceptance testing, and installation testing.

Section 4.5.8 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the software test plan for the PPS replacement system. As described in Sections 3.4.1.1, "Software/Core Logic Management Plan," and 3.4.1.2, "Software/Core Logic Development Plan," of this safety evaluation, PG&E did not develop software for the PPS replacement project; therefore, PG&E did not submit a software test plan. Nonetheless, by letter dated October 26, 2011, the licensee prepared the PPS replacement "Concept, Requirements, and Licensing Phase 1 Project Plan," Revision 1 (Reference 109), to describe all software activities and the project plan for the PPS replacement system by providing high-level details for this project. In particular, this plan provides guidance for the vendors to develop their software test plan.

During the software development and testing, PG&E performed management and oversight of the activities performed by Invensys and Westinghouse/ALS. These activities are defined in PG&E Quality Assurance Plan for the DCPP PPS replacement, dated May 9, 2013 (Reference 110).

Tricon

An evaluation of the software testing for the generic Tricon V10 platform (i.e., Tricon firmware) was performed by the NRC as part of the Tricon platform topical report review. This evaluation is documented in the safety evaluation for the Triconex Approved Topical Report (Reference 29).

Section 4.5.8 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), indicates that for the PPS replacement project, Invensys prepared its "Validation Test Plan

(VTP)," 993754-1-813-P, Revision 2, dated December 18, 2012 (Reference 138), to describe the scope, approach, and resources of validation testing activities of the Tricon V10 portion of the PPS replacement project. Verification testing is not described in this plan; instead, Invensys prepared its "Software Verification Test Plan (SVTP)," 993754-1-868-P, Revision 1, dated April 3, 2014 (Reference 139), to address verification testing, which included both software component and software integration testing activities of the Tricon PPS replacement protection sets (I, II, III, or IV) test system application programs.

Invensys "Project Management Plan (PMP)," 993754-1-905-P, dated December 18, 2012 (Reference 114), and "Software Verification and Validation Plan (SVVP)," 993754-1-802-P, dated December 18, 2012 (Reference 118), describe the organization, roles, and responsibilities to perform software verification and validation testing. In addition, the VTP describes the team responsible for system integration testing from Nuclear Delivery team, Quality Assurance team, and Independent Verification and Validation (IV&V) team.

The Invensys SVTP describes the features to be tested, and also those items not covered. The SVTP was used to test the software components and functions described in the SDD to implement the PPS design. An evaluation of the Invensys Software Verification Test Specification is provided in Section 3.4.2.4, "Testing Activities," of this safety evaluation.

The Invensys VTP describes the activities required to perform system integration, including hardware validation tests, pre-FAT, and FAT. This plan also describes the team responsible to perform these tests, as well as the test tools and environment needed to conduct the system test. The VTP covered hardware of all four Tricon V10 protection sets and their related TSAP in order to test application function, system interfaces, and system performance. In this plan, Invensys describes the use of the maintenance work station (maintenance work station), media converters, and the NetOptics port aggregator tap to test interface between the Tricon and its maintenance work station.

The Invensys VTP describes the test tools, measurement and test equipment, test techniques, and methodologies used for performing including hardware validation tests, pre-FAT, and FAT. Results from validation tests are recorded in the validation test summary report. An evaluation of the Invensys "Validation Test Specification (VTS)," 993754-1-812-P, Revision 1 (Reference 140), is provided in Section 3.4.2.4, "Testing Activities," of this safety evaluation.

<u>ALS</u>

An evaluation of the code testing for the generic ALS platform was performed by the NRC as part of the ALS platform topical report review. This evaluation is documented in the safety evaluation for the Advanced Logic System Topical Report (Reference 30). Specifically, for the ALS platform, Westinghouse prepared "ALS Test Plan," 6002-00005, Revision 4, dated March 1, 2013 (Reference 149), to describe the scope, approach, resources, and scheduling of testing activities; identifies the items being tested, the features to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risk associated with the plan for the generic ALS platform. This plan covered board level testing and board hardware circuit testing for the ALS platform.

For the PPS replacement project, Westinghouse prepared the DCPP PPS "Test Plan," 6116-00005, Revision 4, October 2014 (Reference 136), to describe test planning, test specification, and test documentation for the ALS portion of the PPS replacement system. Specifically, this test plan describes test activities of the ALS components and sub-assemblies for the PPS replacements. Also, the Test Plan describes testing activities for verification and validation (V&V), system integration, and FAT.

The Test Plan defines the scope for testing activities performed by the design team and the IV&V team. Furthermore, the Test Plan identifies test design and test case specifications applicable to the DCPP PPS project, as well as the tools used by each team. The DCPP PPS "Management Plan," 6116-00000, Revision 8, September 2015 (Reference 105), defines the roles and responsibilities for the design and IV&V teams. An evaluation of the DCPP PPS "System Test Design Specification," 6116-70030, Revision 5, June 2015 (Reference 150), and the PPS Test Case Specification are provided in Section 3.4.2.4, "Testing Activities," of this safety evaluation.

The IV&V team performed V&V activities described in the "Diablo Canyon PPS V&V Plan," 6116-00003, Revision 3, November 2014 (Reference 135). The Test Plan provided additional information regarding component, integration, and system testing of the DCPP PPS. When anomalies were found, the IV&V team used the OnTime™ process to report them.

The DCPP PPS Test Plan defined the criteria and requirements to suspend and resume testing if this was necessary. As part of the V&V activities, Westinghouse performed simulation testing on the ALS-102. To support this test, Westinghouse prepared "Diablo Canyon PPS VV Simulation Environment Specification," 6116-10216, Revision 2, September 2015 (Reference 151). This document describes in detail the simulation environment to perform V&V of the field programmable gate array in ALS-102. This document describes the features tested, test approach, criteria to pass/fail, and test design specification (including the requirements and test cases).

The Test Plan defines the documents that summarize DCPP PPS test activities. This plan also identifies the test tools used by the design team and the IV&V team.

STP Safety Conclusion

The NRC staff reviewed the test plans for the Tricon and ALS systems and determined that the plans were sufficiently comprehensive to demonstrate the DCPP PPS replacement system will meet its required functionality and there is reasonable assurance that the system will perform its safety functions. The NRC staff concludes that the test plans adequately address the guidance in BTP 7-14, Section B.3.1.12. An evaluation of ALS and Tricon Test Plan implementation is provided in Section 3.4.2.4, "Testing Activities," of this safety evaluation.

3.4.2 Software Implementation Documentation

This section summarizes the evaluation of PPS application software and logic implementation documentation. This documentation corresponds with the software lifecycle process implementation information described in Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.2.2, "Software Life Cycle Process Implementation," and Section B.3.2, "Acceptance Criteria for Implementation."

3.4.2.1 Review of Safety Analyses

The acceptance criteria for software safety analysis activities are contained in SRP BTP 7-14, Section B.3.2.1, "Acceptance Criteria for Safety Analysis Activities" (Reference 46). This section states that the documentation should show that the system safety requirements have been adequately addressed for each activity group; that no new hazards have been introduced; that the software requirements, design elements, and code elements that can affect safety have been identified; and that all other software requirements, design, and code elements will not adversely affect safety. Further guidance on safety analysis activities can be found in NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," dated June 11, 1993 (Reference 131), and RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997, Section C.3, "Software Safety Analyses" (Reference 85).

3.4.2.1.1 Tricon System

Invensys prepared its "Safety Analysis," Revision 9, 993754-1-915-P, dated December 9, 2014 (Reference 132), to document the methodology and results of its safety analysis. Invensys created its Safety Analysis during the requirements phase and it was updated during the subsequent phases. The Safety Analysis consists of the Interface Analysis, Criticality Analysis, Hazard Analysis, and Risk Analysis.

During the requirements phase, Invensys performed a Preliminary Hazard Analysis (PHA) to identify possible hazards to the PPS, evaluate each of the hazards and describe their expected impact in the protection set software functionality.

Invensys used the fault tree method for the PHA. The NRC staff reviewed the PHA and confirmed correlation to the activities prescribed in the "Software Safety Plan" (SSP), Revision 1, 993754-1-911-P, dated October 13, 2011 (Reference 119). The NRC staff confirmed for each hazard, the source, initiating mechanism, and consequences were identified.

The PHA identified 47 events that could lead to hazards, but only five of them were used for the safety analyses (the others were analyzed in separate areas, such as the failure modes and effects analysis or FMEA). In the "V&V Requirements Phase Summary Report," Revision 1, 993754-1-860-P, dated October 30, 2012 (Reference 152), Invensys noted its risk assessments and mitigation plans were examined. The V&V report identifies mitigations for these hazards, if they were not resolved during the requirements phase.

3.4.2.1.1.1 Interface Analysis

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

The interfaces of the Tricon with external systems were via hard-wired input/output or the Tricon Communication Module interface. In addition, the interface analysis verified the interfaces among the design elements in each PPS protection set have been properly designed and do not introduce a safety hazard.

Invensys performed interface analyses during the requirements, design phases and implementation phase. These analyses were performed for set I and then for sets II, III, and IV.

During the requirements phase, Invensys evaluated the requirements for the software interfaces for protection sets I-IV. In the design phase, Invensys evaluated the interfaces among the different components did not introduce a safety hazard.

The interface analyses concluded the interface requirements and design were verified and validated for correctness, consistency, completeness, accuracy, and testability. In addition, Invensys concluded no new interface hazards were identified.

Then Invensys performed an Interface Analysis during the implementation phase. Invensys verified the Test System Application Program (TSAP) source code interfaces with hardware, software and other components were corrected, consistent, complete, accurate and testable. Invensys also verified no new hazards were introduced.

An interface analysis was performed for protection set I and then a separate analysis for protection sets II-IV.

As a result of the interface analyses, Invensys identified two interface hazards to track its status and mitigation during software development. One hazard was related to the Tricon keyswitch, and the other with the out-of-service switch. These hazards were evaluated as part of the Hazard Analysis described below in Section 3.4.2.1.1.3, "Hazard Analysis," of this safety evaluation.

The NRC staff determined that performance of the Interface Analysis was consistent with the guidance provided in the SSP and, therefore, the Safety Analysis provides objective evidence that the system interface requirements have been correctly implemented.

3.4.2.1.1.2 Criticality Analysis

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

Invensys characterized the PPS application software to be SIL-4 because operation of the system will affect operation of the reactor protection system (RPS) and engineered safety features actuation system (ESFAS) functions. The SIL assignment was reviewed and verified throughout the software development to confirm this level assignment was not lowered.

Invensys found the result of the evaluation is that the SIL-4 assignment is correct. No anomaly was found.

The NRC staff determined that performance of the criticality analysis was consistent with the guidance provided in the SSP and therefore provides an adequate means to ensure the SIL assigned to the PPS application software.

3.4.2.1.1.3 Hazard Analysis

The Hazard Analysis is an evaluation of the protection set software for undesirable outcome(s) resulting from development defects or erroneous operation of the PPS. The evaluation includes screening or analysis methods to categorize, eliminate, reduce, and/or mitigate hazards. During the requirements phase, Invensys evaluated the functional requirements of the PPS to determine potential hazards of the Tricon protection set. Invensys identified 31 conditions, which were then assessed to identify their consequences (e.g., system behavior is allowed per the Interface Requirements Specification requirement) or if new hazards were introduced. The result of the assessment was the identification of a new hazard associated with the test-in-trip/test-in-bypass design.

During the design phase, Invensys verified that the software design correctly implemented the software requirements and introduced no new hazards. Invensys performed the following analyses: design logic, design data, design constraint, and timing and sizing.

In the design logic analysis, Invensys determined all requirements were correctly incorporated in the system design and now new hazards were introduced. Note that Invensys raised a concern regarding communication between the Tricon and its maintenance work station. This item was analyzed as a postulated initiating event, even though it was not considered a hazard. The design data analysis showed data definition was consistent with Invensys software requirements, and read-only tags were created to avert unintentional use of safety-related data. Also, this analysis found if the system halts, parameters will behave as configured (e.g., remain as is or return to default values). In the design constraint analysis, Invensys did not identify limitations or constraints associated with data equations, algorithms, and solutions. Lastly, the timing and sizing analysis did not identify insufficient resources to satisfy the timing and sizing requirements.

As a result of these analyses performed during the design phase, Invensys identified four postulated initiating events, which were assessed to evaluate if the TSAP design could effectively mitigate credible common-cause events. For each postulated initiating event, Invensys performed an event tree analysis to determine whether the initiating event develops into a failure or it is sufficiently mitigated by the design. Invensys found the postulated initiating events are mitigated by the design (e.g., system detection and alarm).

In the implementation phase, Invensys verified TSAP correctly implement the software design and no new hazards were introduced. Invensys performed the same analyses performed during the design phase to determine if potential hazards can cause the TSAP to behave unexpectedly. Invensys evaluated the hazards identified and determined the design include the means to mitigate them.

In the test phase, Invensys verified the validation testing tool and methods could not modify the TSAP or introduce new hazards. Invensys found unintended modifications to the TSAP was not possible with the testing tool and no new hazards were introduced during the test phase.

The NRC staff determined that performance of the hazard analysis was consistent with the guidance provided in the SSP. This analysis provides objective evidence the system safety requirements have been correctly implemented, and provides reasonable assurance that no new hazards have been introduced into the system as a result of software. Furthermore, all software elements that can affect safety were identified, and safety problems and resolutions identified during the analyses have been documented and dispositioned in an appropriate manner. All software requirements, including design and code elements, have been implemented in a manner which will not adversely affect the safety of the system.

3.4.2.1.1.4 Risk Analysis

The Risk Analysis evaluates the frequency of occurrence, severity of the consequence(s) associated with a hazard, and mitigation plans.

Invensys evaluated the hazards identified in the Hazard Analysis for consequence severity and occurrence frequency. The Safety Analysis describes the result of the quantitative risk analysis, including estimates of the frequency of the hazard and the associated severity. The Safety Analysis also includes a mitigation plan.

Invensys did not identify new hazards during the design, implementation, and testing phase. The NRC staff determined that performance of the Risk Analysis was consistent with the guidance provided in the SSP.

3.4.2.1.2 ALS Platform

Westinghouse's Diablo Canyon Process Protection System ALS Subsystem software hazard analysis and the "Independent Verification and Validation Summary Report," Revision 1, 6116-00500, October 2015 (Reference 104), describe the software safety analysis activities performed.

Westinghouse performed a Preliminary Hazard Analysis (PHA) to identify possible hazards to the PPS, evaluate each of the hazards and describe their expected impact in the protection set software functionality. The PHA was included in the "ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Reference 153). The IV&V found discrepancies during the review of the PHA. These discrepancies were captured in an OnTime™ ticket. Westinghouse resolved these discrepancies and an updated hazard analysis was performed (Reference 104).

The PHA identified abnormal situations and events. It also identified potential consequences and actions to mitigate them. The NRC staff reviewed the PHA and observed the Westinghouse identified 33 hazards. The NRC staff confirmed correlation in the PHA to the activities prescribed in the "Software Safety Plan" (SSP), Revision 2, 6116-10020, January 2015 (Reference 133).

3.4.2.1.2.1 Interface Analysis

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

The interface of the ALS-102 field programmable gate array (FPGA) logic are communication interfaces with other ALS boards through the Reliable ALS Bus (RAB), and Test ALS bus (TAB) and TxB channel to communicate with the process plant computer and the ALS maintenance work station, respectively. The ALS-102 RAB interface was analyzed and verified as part of ALS platform V&V effort in the Advanced Logic System Topical Report (Reference 30). There was no further analysis of the RAB interface for the DCPP PPS application.

The ALS-102 TAB interface was analyzed and verified as part of the ALS platform V&V effort. Also, Westinghouse evaluated the interface for the TxB. TxB communication was reviewed as part of software evaluation. WEC summarized software design and testing evaluation in the Independent Verification and Validation Summary Report.

The NRC staff determined that performance of the Interface Analysis was consistent with the guidance provided in the SSP and IV&V plan.

3.4.2.1.2.2 Criticality Analysis

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

During the planning and concept phase, Westinghouse assigned SIL-4 to the ALS portion of the PPS (Reference 104). The SIL assignment was reviewed and verified throughout the phases of the software lifecycle to confirm this level assignment was not lowered.

The NRC staff determined that performance of the criticality analysis was consistent with the guidance provided in the SSP and therefore provides an adequate means to ensure the SIL assigned to the PPS application software.

3.4.2.1.2.3 Hazard Analysis

As described previously, WEC prepared a PHA report included in included in the "ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Reference 153), per IEEE Std. 1012-1998. In addition, as part of the IV&V review, WEC performed a detailed analysis of the Diablo Canon PPS FPGA logic. The results are documented in the IV&V summary report (Reference 104).

WEC subsequently used this information to analyze the software hazard associated with the ALS portion of the PPS replacement, including the ALS Service Unit. The results of this evaluation through the various phases of the lifecycle are documented in the software hazard analysis. In particular, WEC identified and evaluated hazards that could potentially challenge the ALS system to perform its safety functions. In addition, for each hazard, WEC identified actions to be taken to mitigate or resolve these hazards. The hazards are summarized in the software hazards analysis report.

During each phase, WEC reviewed the hazards identified from the previous phase to verify that additional hazards were not introduced, and that previously identified hazards, actions were identified to mitigate them. At the completion of the lifecycle, WEC determined all potential software hazards were identified during system design, documentation review analysis and testing, and proper actions identified to mitigate them. Further, WEC concluded that the results of the analysis indicate that the PPS software demonstrates a low probability of causing hazards.

Based on the information documented in the PHA and software hazard analysis, the NRC staff determined that performance of the risk analysis was consistent with the guidance provided in the SSP.

3.4.2.1.2.4 Risk Analysis

Westinghouse performed a risk analysis to evaluate the risks associated with the hazards identified by the hazard analysis. Westinghouse used the OnTime™ tickets associated with software issues to identify potential risks. Westinghouse also performed managerial risk identification in accordance with its Management Plan. WEC documented overall project risks in the IV&V summary report, 6116-00500, Revision 1 (Reference 104). Specifically, WEC summarized risks identified and evaluated through the phases of the lifecycle.

WEC used its OnTime™ to record anomalies identified during risk and hazard analyses. As part of the risk analysis, IV&V team assessed them to determine if they posed any risk to the implementation of the DCPP PPS project. WEC confirmed all open items were addressed and OnTime™ tickets and Corrective Action, Prevention and Learning were closed.

The NRC staff determined that performance of the risk analysis was consistent with the guidance provided in the SSP.

3.4.2.2 V&V Analysis and Reports

The "Software Verification and Validation Plan (SVVP)," 993754-1-802-P, Revision 3 (Reference 118), and "Independent Verification and Validation, Diablo Canyon PPS VV Plan," 6116-00003, Revision 3 (Reference 135), describe the V&V tasks carried out by each subsystem vendor (see Section 3.4.1.6 of this safety evaluation). Standard Review Plan (SRP) BTP 7-14, Section B.3.2.2, "Acceptance Criteria for Software Verification and Validation Activities" (Reference 46), states that the acceptance criterion for software V&V implementation is that the tasks in the SVVP have been carried out in their entirety. Documentation should exist that shows that the V&V tasks have been successfully accomplished for each life cycle activity group. In particular, the documentation should show that the requirements, design, code, integration, and installation design outputs satisfy the appropriate software or core logic development functional and process characteristics.

V&V activity summary reports as well as the final V&V reports for both Tricon and the ALS subsystems were reviewed by the NRC staff to determine if V&V activities were being effectively performed to ensure development of quality software and core logic for the DCPP PPS. The results of these evaluations are described below.

3.4.2.2.1 Tricon IV&V Summary Report Evaluation

The following subsections describe the safety evaluation activities pertaining to the development of the Tricon software application.

3.4.2.2.1.1 Requirements Phase V&V Activity Summary Report

Ten V&V tasks performed during the requirements phase of the PPS software development process were identified and evaluated in the Tricon "V&V Requirements Phase Summary Report," 993754-1-860-P, Revision 1, dated October 30, 2012 (Reference 152). The NRC staff reviewed these tasks and confirmed correlation to the activities prescribed in the SVVP, 993754-1-802-P, Revision 3 (Reference 118), Section 5.2.2, "Requirements Phase." The NRC staff confirmed for each task, an evaluation of the required characteristics such as correctness, consistency, completeness, accuracy, readability, and testability was performed. One discrepancy found during these tasks was reported via the Action Request Report process to facilitate resolution. This discrepancy related to a document control issue associated with the Project Management Plan.

The software safety metrics identified four hazards. Three of which were resolved during the requirements phase. One hazard associated with the Software Requirements Specification (SRS) remained unresolved; however, its risk assessment and mitigation plan was evaluated and a determination was made that this hazard does not present a serious challenge to the replacement PPS design.

Control hazard efforts included engineering controls and administrative controls. Hazard status tracking in subsequent phases was also identified as a necessary control action. A hazard tracking list is being maintained as an attachment to the safety analysis to facilitate tracking of hazards and hazard controls. It is expected that this hazard will be mitigated during the design phase.

The NRC staff determined that performance of the requirements phase V&V tasks was consistent with the guidance provided in the SVVP and, therefore, provides an adequate means to ensure sufficient quality and functionality of the requirements phase outputs.

3.4.2.2.1.2 Design Phase V&V Activity Summary Report

Eleven V&V tasks performed during the design phase of the PPS software development process were identified and evaluated in the "V&V Design Phase Summary Report," 993754-11-861-P, Revision 3, dated January 15, 2016 (Reference 154). The NRC staff reviewed these tasks and confirmed correlation to the activities prescribed in the SVVP Section 5.2.3, "Design Phase" (Reference 118). The NRC staff confirmed for each task an evaluation of the required characteristics such as correctness, consistency, completeness, accuracy, readability, and testability was performed. Two anomalies were identified during the design phase. For the first, incorrect quantities were reported in a Bill of Materials document. This issue was addressed using the system integration deficiency report (SIDR) process. The second was a failure to incorporate a design review checklist into the Hardware Requirements Specification and Hardware Design Description documents. This anomaly was entered into the corrective action program. Both of these anomalies were resolved prior to completion of the design phase. No internal programmatic deficiencies were identified during the design phase.

The NRC staff determined that performance of the design phase V&V tasks was consistent with the guidance provided in the SVVP and, therefore, they provide an adequate means to ensure sufficient quality and functionality of the design phase outputs.

The software safety metrics identified one new hazard during the design phase. One additional hazard was carried forward from the requirements phase. Both of these hazards were subsequently mitigated. Upon re-entry into the design phase, all hazards were mitigated. Therefore no hazards were deferred into the implementation phase of the PPS project.

3.4.2.2.1.3 Tricon Implementation Phase V&V Activity Summary Report

Eighteen V&V tasks performed during the implementation phase of the PPS software development process were identified and evaluated in the "V&V Implementation Phase

Summary Report, PPSI," Revision 1, 993754-11-862-P, dated August 7, 2014 (Reference 155), and "V&V Implementation Phase Summary Report, PPSII-IV," Revision 1, 993754-12-862-P, dated January 15, 2016 (Reference 156). The NRC staff reviewed these tasks and confirmed correlation to several of the activities prescribed in the SVVP Section 5.2.4, "Implementation Phase" (Reference 118). There were two prescribed activities in the SVVP that did not have corresponding activities in Section 3.2 of the implementation phase V&V activity summary report. These were:

(2) Verify that the input/output list is correct and ensure implementation requirements are adequately incorporated, and

(9) Nuclear IV&V shall be responsible for system test equipment staging to perform the validation test.

The NRC staff noted that protection set input/output lists were included as implementation phase input documents; however, the summary reports made no mention of a specific V&V activity to ensure correctness of these lists. It can be inferred that performance of test equipment staging for the validation test was completed prior to performance of the performance of the informal dry-run of the FAT as described in task number 13; however, there is no specific activity listed to ensure accomplishment of this task. The licensee subsequently revised the V&V summary report to include a description of these completed activities. The NRC staff then verified these activities as having been satisfactorily performed during the regulatory audit on June 3-5, 2014 (Reference 38).

The NRC staff confirmed that an evaluation of the required characteristics was performed for each of the implementation phase V&V tasks. Discrepancies or anomalies found during these tasks were reported and the system integration deficiency report, interim change notice, and corrective action report processes were invoked to facilitate resolution of issues.

One of the deficiency reports remained unresolved at the completion of the Implementation phase. This was CAR 2507 which is an issue with the emulation test driver used for system verification tests. No evaluation of risks associated with this unresolved issue was provided in the Technical and Management Risks section of the summary report and the report recommended exiting the implementation phase with this condition present. Additionally, the report states that "all deficiencies are resolved," and that "all output documents are issued." These statements seem to conflict with the information in Table 5-3, and with the conditions of the provisional release in that only protection set I implementation is complete.

The NRC staff reviewed CAR 2507 and discussed its implications with the Invensys staff. Verification tests which use the emulator tool were performed on PPS software; however, the reported test results did not rely upon the emulators test result reporting functions. Instead, numerical test results were manually compared with the verification test criteria by IV&V personnel and were evaluated to determine if specific pass/fail criteria were met. The verification tests performed on the DCPP PPS therefore did not rely on the emulator reporting function affected by this issue and the verification test results remain valid.

The report states that no new hazards were introduced into the system during the implementation phase and it states that *"all hazards are properly mitigated"* in Section 7 of the report. The NRC staff confirmed this to be consistent with the previous V&V summary report.

The NRC staff determined that performance of the implementation phase V&V tasks was consistent with the guidance provided in the SVVP and, therefore, provides an adequate means to ensure the quality and functionality of the implementation phase outputs.

3.4.2.2.2 ALS IV&V Summary Report Evaluation

Verification and validation (V&V) tasks for all phases of the DCPP PPS ALS core logic development process were performed and documented in the Diablo Canyon PPS "Independent Verification and Validation Summary Report," 6116-00500, Revision 1 (Reference 104). The following subsections discuss NRC staff evaluations of phase-related V&V tasks performed for the ALS PPS subsystem.

3.4.2.2.2.1 ALS – Concept Phase Activities

The NRC staff reviewed concept phase tasks performed and confirmed correlation to the activities prescribed in the "Diablo Canyon PPS VV Plan," 6116-00003, Revision 3, Section 4.3, "Acquisition Support V&V Activity (Concept Phase)" (Reference 135). A cursory review of the project concept documents was performed to establish the initial approach to the V&V efforts. The NRC staff noted discrepancies discovered during performance of concept phase IV&V tasks were reported and subsequently resolved using the OnTime™ ticketing system. One discrepancy found during these tasks identified the fact that the PPS specification documents did not clearly define scope for the individual PPS subsystems. To address this, Westinghouse developed scoping tables to identify and distinguish specifications for the Westinghouse ALS portion of the PPS from those assigned as part of Invensys and PG&E scope. The NRC staff reviewed these scoping tables during its June 22-26, 2015, regulatory audit in Warrendale, Pennsylvania, and found them to be an acceptable means of defining specification scope for the ALS subsystem (Reference 39).

3.4.2.2.2.2 ALS – Planning Phase Activities

The NRC staff reviewed planning phase tasks performed and confirmed correlation to the activities prescribed in the "Diablo Canyon PPS VV Plan," Section 4.4, "Planning V&V Activity (Planning Phase)" (Reference 135). For all project planning documents, an evaluation of the required characteristics including consistency, style, traceability, unambiguity, and verifiability was performed. One notable deficiency identified during the IV&V review of the management plan was that the management plan failed to clearly identify the scope split between vendor and the licensee. The IV&V activities also identified the management plan had referred to several outdated procedures and processes. These and other discrepancies discovered during performance of planning phase IV&V tasks were reported and are being resolved using the OnTime™ ticketing system.

3.4.2.2.2.3 ALS – Requirements Phase Activities

The NRC staff reviewed requirements phase tasks performed and confirmed correlation to the activities prescribed in the "Diablo Canyon PPS VV Plan," Section 4.5, "Concept V&V Activity (Requirements Phase)," and Section 4.6, "Requirements V&V Activity (Requirements Phase)" (Reference 135). An evaluation of the required characteristics including correctness, accuracy and completeness, was performed as part of the hardware/software/user requirements allocation analysis.

When performing the hazard analysis IV&V task, the IV&V organization reviewed the preliminary software hazards analysis report and found inadequate identification of software hazards. An OnTime™ ticket was used to report this finding and the preliminary software hazards analysis was revised to remove erroneous hazards identified. The NRC staff performed an audit activity to review the actions taken to resolve this issue and found that these actions were effective in correcting this hazards identification issue. Subsequent hazards analysis activities were also performed to ensure each identified hazard was appropriately addressed in the PPS design.

Seven anomalies were identified by the IV&V team during the traceability analysis V&V task and all were entered into the OnTime™ system to facilitate resolution. The NRC staff chose one of these anomalies related to the ALS board non-volatile memory configuration specification for review during the audit. The objective of this audit activity was to confirm corrective actions taken adequately addressed the identified discrepancy. The NRC staff found the corrective actions taken to correct the non-volatile memory specifications were effective and subsequent documentation accurately reflected the systems non-volatile memory configurations.

As part of the software requirements evaluation activity, the IV&V team identified numerous anomalies associated with the IV&V simulation environment and system test planning activities. Three of the system specifications documents were modified to resolve these anomalies: the ALS-102 FPGA requirements specification, the ALS board non-volatile memory configuration specification and the communications protocol specification. These documents then became part of the requirements phase baseline.

3.4.2.2.2.4 ALS – Development Stage Activities (Design, Implementation, and Test V&V Activities)

The DCPP PPS management plan defines the development stage of the ALS subsystem consisting of the design, implementation, and test phases of the development lifecycle. The NRC staff reviewed design, implementation, and test phase tasks performed and confirmed correlation to the activities prescribed in the "Diablo Canyon PPS VV Plan" Section 4.7, "Design V&V Activity (Design Phase)," Section 4.8, "Implementation V&V Activity (Implementation Phase)," and Section 4.9, "Test V&V Activity (Test Phase)," respectively (Reference 135). For each development stage V&V task, an evaluation of the required characteristics was performed.

During the traceability analysis activity, the IV&V team used a three-step approach to ensure correctness, consistency, and completeness of the requirements traceability efforts. These steps included: a regression analysis of baseline requirements and linking, performance of tracing from software requirements to lower level design statements, and performance of reverse tracing from lower level design statements back to software requirements. The regression analysis activity assessed changes that were introduced after the requirements phase requirements traceability matrix (RTM) release to assess how newly introduced requirements were integrated into the system design and traceability structure.

Several anomalies were discovered during traceability analysis. Though each of these anomalies was identified in the OnTime™ issue resolution program, several iterations of the RTM were required before all of them could be resolved. The NRC staff confirmed that each of the associated OnTime™ tickets were closed prior to final release of the PPS plant logic configuration. The NRC staff observed consistent use of OnTime™ ticket tracking through the various revisions of the RTM. Deferral of anomaly resolution with concurrence of the IV&V group was noted and follow-up activities to ensure ultimate anomaly resolution were performed prior to release of plant logic configurations for operation.

A software design evaluation was performed to determine if field programmable gate array (FPGA) design specification documents were sufficient to satisfy the requirements of the software requirements specification (SRS), avoid introduction of unintended features, and provide necessary information to support the generation of the FPGA design. The NRC staff noted the OnTime™ program was used to document and track resolution of anomalies identified during this activity. The report states that anomalies relating to readability, testability, completeness, and change control were initiated and that most of these anomalies had been resolved satisfactorily. One exception was an OnTime™ ticket relating to project requirements tracing deficiencies. Resolution of this anomaly was deferred following a determination that it did not impact the safety of the deliverable FPGA.

The NRC staff noted hazards analysis activities identified several system deficiencies which were corrected via the OnTime™ ticket process. No additional system hazards were identified during the PPS development stages.

The performance of risk analysis activities was documented in the Independent Verification and Validation Summary Report (Reference 104); however, no specific risk analysis reports were generated. Instead, the vendor relied upon anomalies recorded the OnTime™ ticketing system in as well as test execution and verification activities to provide a means of providing evidence for completion of risk analysis tasks.

The NRC staff determined that performance of the ALS development stage V&V tasks was consistent with the guidance provided in the Diablo Canyon PPS VV Plan and, therefore, provides an adequate means of ensuring the quality and functionality of the ALS portion of the DCPP PPS.

3.4.2.3 Configuration Management Activities

The software configuration management plan (SCMP) describes the software configuration management tasks that are to be carried out by the licensee and vendors (see Section 3.4.1.7, "Software/Core Logic Configuration Management Plan," of this safety evaluation). The acceptance criteria for software configuration management activities are included in BTP 7-14, Section B.3.2.3, "Acceptance Criteria for Software Configuration Management Activities" (Reference 46). This acceptance criterion requires that the tasks in the SCMP be carried out in their entirety. Documentation should exist that shows that the configuration management tasks for that activity group have been successfully accomplished. In particular, the documentation should show that: (1) configuration items have been appropriately identified; (2) configuration baselines have been established for the activity group; (3) an adequate change control process has been used for changes to the product baseline; and (4) appropriate configuration audits have been held for the configuration items created or modified for the activity group.

Licensee

PG&E maintains records of all project documentation and drawings, as well as records of changes, in the Nuclear Power Group library, which is the licensee's repository for project documents. In addition, the "Software Configuration Management Plan (SCMP)," dated March 18, 2013 (Reference 143), requires creation of valid backup to support recovery of any software product developed for the PPS replacement project. All project software (executable files, source code, etc.) is stored in the Digital Systems Engineering SourceSafe as described in the licensee's letter dated May 9, 2013 (Reference 13). Section 3.1.3, "Backup and Disaster Recovery Libraries," of the SCMP describes the media to be used for storage of files. To access these files in SourceSafe, PG&E personnel requires special software, permissions, and a login account to modify, delete, or add files.

PG&E measures software configuration management, system status, and performance to identify problems and inefficiencies in processes. Section 3.3.2, "SCM Metrics Reports," of the SCMP (Reference 143) describes the type of software configuration management metrics reported. In addition, PG&E uses a configuration status account to track and record modifications and enhancements to configuration items.

The SCMP establishes the process for functional changes and modifications to application software and configuration control. In particular, when modifications are required, the applicant sponsor prepares a design change package, and then he/she is responsible for implementing functional changes. System modifications are documented using software change package or configuration change package. In addition, modifications will be requested in accordance with the "Plant Modification Request and Approval" described in the licensee's letter dated May 9, 2013 (Reference 13). After the change package is prepared, the system coordinator will assess the modification, approve it, and assign a change level. Section 3.2.2, "Evaluating Changes (Classification of Modifications)," of the SCMP describes activities to be performed for each change level. PG&E uses SAP (electronic business management software) notifications and orders tracked changes (Reference 13). Both SAP orders and software change packages or configuration change packages are entered in the PG&E record management system and are handled as quality records.

Tricon

Section 3, "SCM Activities," of the "Software Configuration Management Plan (SCMP)," Revision 1, 993754-1-909 P, dated December 18, 2012 (Reference 116), describes the identification, naming, and description of configuration items, including documents supplied by PG&E. Invensys Operations Management (IOM) uses a master configuration list for configuration control of all configuration items, project documents, test system application program (TSAP) versions, and documentation of final system configuration. During the June 3-5, 2014, regulatory audit (Reference 38), the NRC staff reviewed the master configuration list, and observed how IOM personnel used the master configuration list to identify configurable items that are tracked, stored, and controlled.

IOM maintains all project records in the nuclear integration records. The nuclear integration records are access-controlled and write-key protected. The project manager and project administrator are the only people with access to remove, replace, and modify files in the nuclear integration record; team members can only read or download personal copies of these files. During the November 13-16, 2012, regulatory audit (Reference 36), the NRC staff observed how the nuclear integration record is accessed and the documents maintained.

Modifications to configuration items were made during design and development activities. These requests were recorded in interim change notices. Section 3.2.1.2, "Changes - Interim Change Notice (ICN)," of the SCMP describes the requirements for interim changes.

Invensys tracked software configuration management indicators for baselines and changes, as well as status of requested changes and implementation of changes. These are accounted by the form by which the change was initiated and logged.

Modifications due to anomalies were dispositioned in accordance with Project Procedures Manual (PPM) 10.0, "Nonconformance and Corrective Action." PPM 10.0 describes the process to control nonconforming items and to identify appropriate corrective actions for nuclear applications. A nonconforming condition is documented on PPM Form 10-1, System Integration Deficiency Report (SIDR) Form. System integration deficiency reports are recorded in the SIDR log, which is maintained by the project administrator in the nuclear integration record. During the regulatory audit on June 3-5, 2014 (Reference 38), the NRC staff reviewed examples of SIDRs created to identify errors or problems encountered during testing.

Any changes to the final approved design documents are reviewed and approved in the same manner as the original design, in accordance with PPM 2.0. In addition, all IOM engineering documents and changes to released documents requested by PG&E must go through a formal review and sign-off body called the Change Control Board. Approval and release by the Change Control Board is reflected on an engineering change order. This process is described in Section 3.2.3, "Approval or Rejection of Changes," of the SCMP (Reference 116).

ALS

The Westinghouse "ALS Configuration Management Plan," Revision 11, 6002-00002-P, March 2015 (Reference 146), and "Management Plan," Revision 8, 6116-00000, September 2015 (Reference 105), define the ALS software configuration management activities for the DCPP PPS project. Section 6.1, "Configuration Management Plan," of the Management Plan describes the types of configuration items and levels for the DCPP PPS project. Summaries of the configuration items are created and documented in DCPP PPS "Configuration Management Report, Release 4.2.0 for Baseline 6116-00401 Rev. 4," Revision 7, 6116-00400, October 2015 (Reference 147), and "Configuration Management Baseline Report," Revision 4, 6116-00401, October 2015 (Reference 148).

The baseline report documents the design basis for the DCPP PPS project used for the development of both hardware and software that will be delivered to PG&E. During the June 22-26, 2015, regulatory audit (Reference 39), the NRC staff reviewed an example from PPS Configuration Management Baseline Report that was created for this audit.

The Management Plan identifies and describes the organization responsible for configuration management activities. In addition, Westinghouse established a Configuration Control Board to review requests for engineering changes. Requests for engineering changes are used to manage changes to the baseline and configuration items. During the June 22-26, 2015, audit, the NRC staff observed how this process was used to control and change baselines and configuration items.

Westinghouse uses its Enterprise Document Management System as the official repository for all DCPP PPS replacement approved documents and configuration items. During the audit on June 22-26, 2015, the NRC staff observed how the project team used the Enterprise Document Management System and other Westinghouse repositories for project files.

The NRC staff determined the software configuration management processes and activities performed meet the requirements of IEEE Std. 828-1998, "IEEE Standard for Software Configuration Management Plans" (Reference 77), and ANSI/IEEE Standard 1042-1987, "IEEE Guide to Software Configuration Management" (Reference 78), and are therefore acceptable. In particular, the NRC concludes that both vendors established a process to control software items through a librarian, and it also provides a process to control code or documentation changes through a Configuration Control Board. The software configuration management activities adequately address the guidance in BTP 7-14 (Reference 46).

3.4.2.4 Testing Activities

The acceptance criterion for testing activities is contained in the SRP BTP 7-14, Section B.3.2.4, "Acceptance Criteria for Testing Activities" (Reference 46). This section states that Section 7.2, "Regression Analysis and Testing," of RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 2, July 2013 (Reference 73) and RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, July 2013 (Reference 79), that endorses IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation" (Reference 80), and RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (Reference 81) that endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing" (Reference 82), identify acceptable methods to satisfy software testing requirements.

Software testing consists of testing the smallest testable units, and then integrating those units into larger testable units, and testing that integrated unit. This process is repeated until finally the system is tested after installation. The following subsections describe the testing activities conducted for each of the Diablo Canyon PPS subsystems:

Tricon

Tricon platform and PPS application test planning is described and evaluated in Section 3.4.1.8, "Software/Core Logic Test Plan," of this safety evaluation. The Tricon test plans describe the testing activities for verification and validation, system integration, and factory acceptance testing (FAT) to be performed during product application development to ensure PPS level requirements are met prior to installation into the plant.

Test Specifications for the Diablo Canyon PPS Tricon subsystem were provided in the DCPP PPS "System Validation Test Specification (VTS)," Revision 1, 993754-1-812-P, dated April 4, 2014 (Reference 140). The Validation Test Specification defines how test are performed, as well as how test procedures and test cases are developed for each system component and function of the DCPP PPS.

The Invensys Software Verification Test Specification (SVTS) defines how tests are performed, as well as how test procedures and test cases are developed for each software component and function. Both the "Software Verification Test Plan (SVTP)," Revision 1, 993754-1-868-P, dated April 3, 2014 (Reference 139), and the SVTS describe the testing approach, test tools, and test environments to be used for verification testing. These documents identified the criteria to pass/fail the software verification testing. Invensys followed its Project Procedures Manual (PPM) 10.0, Nonconformance & Corrective Action, to document and resolve problems or anomalies identified during testing. Section 3.4.1.2, "Software/Core Logic Development Plan," of this safety evaluation provides additional information about system integration deficiency reports.

The NRC staff concludes that the Tricon Validation Test Specifications is compliant with the criteria of IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation" (Reference 80), and therefore acceptable. The NRC staff reviewed the Tricon subsystem FAT reports "Protection Set I, Factory Acceptance Test Report," Revision 3, 993754-11-854-1-P, dated January 14, 2016 (Reference 157), "Protection Set II, Factory Acceptance Test Report," Revision 0, 993754-12-854-1-P, dated December 12, 2014 (Reference 158), Protection Set III, Factory Acceptance Test Report," Revision 0, 993754-13-854-1-P, dated December 12, 2014

(Reference 159), and Protection Set IV, Factory Acceptance Test Report," Revision 0, 993754-14-854-1-P, dated December 12, 2014 (References 160), and confirmed satisfactory completion of all test cases.

ALS

The Advanced Logic System (ALS) platform and PPS application test planning is described and evaluated in Section 3.4.1.8, "Software/Core Logic Test Plan," of this safety evaluation. The ALS test plans describe the testing activities for verification and validation (V&V), system integration, and FAT to be performed during product application development to ensure PPS level requirements are met prior to installation into the plant.

Test Specifications for the DCPP PPS ALS subsystem were provided in the "System Test Design Specification," Revision 5, 6116-70030, June 2015 (Reference 150). The test specification establishes the scope, boundaries, objectives, and case descriptions for the system-level testing of the DCPP PPS. The NRC staff concludes that the ALS Test Specification to be compliant with the criteria of IEEE Std. 829-1983 (Reference 80) and therefore acceptable.

The Test Design Specification was used to develop individual test cases which are documented in the DCPP PPS Test Case Specification. The Test Case Specification includes detailed descriptions of the automated tests executed during the DCPP PPS FAT. The test case descriptions include features tested, required inputs/outputs, test sequence, and the pass/fail criteria derived from the requirements. The NRC staff reviewed several test cases during thread audits on June 22-26, 2015, to confirm satisfactory implementation of selected system requirements. During the audit, the NRC staff also observed a demonstration of a test case performance. Results of these audits can be found in the ALS audit report (Reference 39). The "Requirements Traceability Matrix," Revision 3, 6116-00059, November 2014 (Reference 161), included the test case number of the requirements or design features covered during testing, such as FAT. The NRC staff reviewed the ALS subsystem "Factory Acceptance Test Report," 6116-70034; Protection Set II, Revision 0, August 2015 (Reference 162), and confirmed satisfactory completion of all test cases.

The design team performed tests at the component and board level to confirm design requirements were met. During these tests, if an anomaly was encountered, the design team used the OnTime™ ticket process described in previous sections.

Combined PPS Testing Activities Evaluation Conclusions

Testing activities for both PPS subsystems were observed to be consistent with the requirements of the Software Requirements Specifications and the Software Design Descriptions. The test programs provided comprehensive test coverage of the entire integrated digital PPS. The NRC staff observed appropriate adherence to the test program procedures. Discrepancies discovered during the test evaluations were appropriately documented and addressed. The FAT adequately verified that all intended application-specific functions were properly implemented.

Testing of the ALS and Tricon subsystem's smallest testable units were accomplished during the respective system platform type testing and generic system qualification. Integration of these units into the DCPP integrated PPS was then performed by the vendors Westinghouse and Tricon by performing application development processes described in Section 3.4.1, "Software/Core Logic Planning Documentation," of this safety evaluation.

3.4.2.5 Requirements Traceability Matrix (RTM) Evaluation

Evaluation criteria for the use of an RTM is contained in SRP BTP 7-14, Section A.3, "Definitions" (Reference 46). Section A.3 states, in part, that: "An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement." This is further clarified in Section B.3.3, "Acceptance Criteria for Design Outputs," in the subsection on Process Characteristics. This section states that the RTM should show what portion of the software requirement, software design description, actual code, and test requirement addresses each system requirement.

The Functional Requirements Specification (FRS) (Reference 126), the Interface Requirements Specification (IRS) (Reference 98), and the Transfer Functions Design Input Specification (TFS) (Reference 99) for the DCPP PPS include the system requirements for both the Tricon and ALS portions of the system. The TFS also provides information necessary for implementation of system requirements. Each vendor, Westinghouse and Invensys, used the FRS, IRS, and TFS to determine the specific requirements to be implemented in the associated subsystem. A traceability matrix was developed by each vendor to ensure that all system requirements would be transferred to the design of the applicable subsystem. Invensys refers to the traceability matrix for the Tricon as a Project Traceability Matrix (PTM) and Westinghouse refers to the traceability matrix for the ALS as a Requirements Traceability Matrix (RTM). Figure 3.4.2.5-1 below represents the relationship between the licensee's FRS/IRS/TFS and the requirements documents created by the vendors during PPS development.

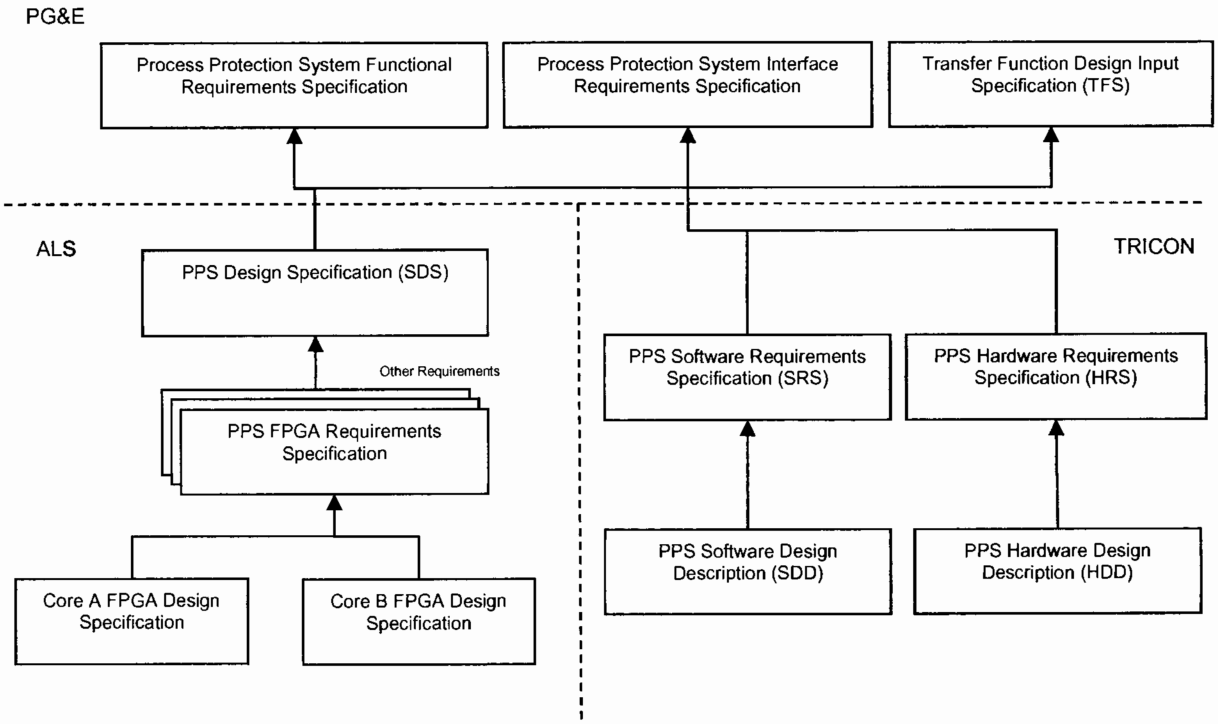

PG&E
Process Protection System Functional Requirements Specification
Process Protection System Interface Requirements Specification
Transfer Function Design Input Specification (TFS)
ALS
TRICON
PPS Design Specification (SDS)
Other Requirements
PPS FPGA Requirements Specification
Core A FPGA Design Specification
Core B FPGA Design Specification
PPS Software Requirements Specification (SRS)
PPS Hardware Requirements Specification (HRS)
PPS Software Design Description (SDD)
PPS Hardware Design Description (HDD)

Figure 3.4.2.5-1

Both the ALS RTM and the Tricon PTM provide a means by which system design requirements can be traced between the design implementation documents and the FRS, IRS, and TFS. A separate evaluation for each of these traceability matrices is provided below.

ALS Requirements Traceability Matrix

The ALS "Requirements Traceability Matrix" (RTM), Revision 3, 6116-00059, November 2014 (Reference 161), is composed of a single table A-1 in Appendix A of the RTM. This table:

- identifies requirements from the PG&E FRS, IRS, and TFS that are applicable to the ALS portion of the PPS,
- establishes requirements traceability between the PPS FRS and the "ALS System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127),
- establishes requirements traceability between the PPS IRS and the ALS System Design Specification,

- establishes requirements traceability between the ALS System Design Specification and the "ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, May 2013 (Reference 163), and
- establishes requirements traceability between the ALS-102 FPGA Requirements Specification and the "ALS-102 Core A FPGA Design Specification," Revision 0, 6116-10203, May 2013 (Reference 164), and "ALS-102 Core B FPGA Design Specification," Revision 0, 6116-10204, dated April 18, 2013 (Reference 165).

The tables are also intended to ensure that low level derived requirements generated in the ALS System Design Specification or FPGA requirement specifications are captured for the purpose of clearly identifying integration and testing scope. The ALS RTM is used as a means of delineating scope of work for the licensee and the vendor.

Tricon Project Traceability Matrix (PTM)

The "Project Traceability Matrix" (PTM), Revision 1, 993754-1-804-P, dated October 17, 2012 (Reference 103), was used for managing the Tricon subsystem software requirements through the software development lifecycle phases. This PTM was used for the DCPP PPS project to provide assurance that all requirements were implemented into the integrated system during the design process. Requirements tracing was performed using PTM to ensure that all software requirements from the system requirements documents including the Functional Requirements Specification (FRS) and the Interface Requirements Specification (IRS) are addressed in the Tricon System Requirements Specification and, thereafter, throughout the implementation and testing activities.

As outlined in the "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), the independent validation and verification (IV&V) organization is responsible for performing the software requirements traceability analyses activities associated with the PTM. Software requirements traceability analyses verification and validation (V&V) activities are performed first in the requirements phase of the software development lifecycle and are repeated subsequently during each phase through to the test phase after which time the final V&V activity summary report is generated.

The licensee prepared a "System Level Requirements Traceability Matrix (RTM)," March 2016 (Reference 188) to capture and trace requirements not included in the V&V scope of the vendors (Invensys and WEC). These are PPS requirements to be implemented and controlled by the licensee independently from the vendor development activities. The NRC staff reviewed the system-level RTM and determined it provides an adequate process for establishing traceability for licensee-implemented PPS requirements. However, many of the licensee actions for implementing requirements have not yet been performed. An inspection follow-up activity is therefore included in Section 3.14.3, "Licensee Site Inspection Follow-up Items," of this safety evaluation to confirm implementation of licensee scope requirements prior to system startup.

The ALS RTM, Tricon PTM, and licensee's system-level RTM show that each of the requirements delineated in the FRS and the IRS is broken down into sub-requirements for the DCPP PPS application. The traceability matrices also indicate which portion of the implementation documents and test requirements are being credited to address each system requirement. The NRC staff concludes that the requirements tracing processes as implemented in the ALS RTM, Tricon PTM, and licensee's system-level RTM provide reasonable assurance that all requirements are correctly implemented in the DCPP PPS application hardware and software and are therefore acceptable.

3.4.3 Software Design Outputs

3.4.3.1 Software Requirements Specification

The acceptance criterion for software requirements specification is contained in Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.3.1, "Requirements Activities - Software Requirements Specification" (Reference 46). This section states that Regulatory Guide (RG) 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (Reference 83), endorses IEEE Std. 830, "IEEE Recommended Practice for Software Requirements Specifications" (Reference 84). IEEE Std. 830 describes an acceptable approach for preparing software requirements specifications for safety system software. Additional guidance is also provided in NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," dated June 11, 1993, Section 3.2.1, "Software Requirements Specification [SRS]," and Section 4.2.1, "Software Requirements Specifications" (Reference 131).

The basis specifications for the DCPP PPS are the Functional Requirements Specification (FRS) (Reference 126), the Interface Requirements Specification (IRS) (Reference 98), and the Transfer Functions Design Input Specification (Reference 99). These documents were the starting point for all of the project design and development efforts.

Tricon PPS Subsystem SRS

The PPS "Software Requirements Specification (SRS)," Revision 4, 993754-11-809-P, dated January 21, 2014 (Reference 166), "Software Requirements Specification (SRS), Protection Set II," Revision 2, 993754-12-809-P, dated October 17, 2012 (Reference 167), "Software Requirements Specification (SRS), Protection Set III," Revision 2, 993754-13-809-P, dated October 17, 2012 (Reference 168), and "Software Requirements Specification (SRS), Protection Set IV," Revision 2, 993754-14-809-P, dated October 17, 2012 (Reference 169), provide the software requirements for the Tricon PPS subsystem.

The Tricon SRS conforms to the guidance of IEEE Std. 830-1998 (Reference 84), as endorsed by RG 1.172 (Reference 83). The Tricon SRS is consistent with the content and organization prescribed by IEEE Std. 830-1998. The NRC staff notes that each of the specific software requirements in the Tricon SRS is uniquely identified by a requirement number and that the origin of each requirement is provided or can be derived using the "Project Traceability Matrix," Revision 1, 993754-1-804-P, dated October 17, 2012 (Reference 103).

ALS PPS Subsystem SDS and FPGA Requirements Specifications

For the ALS PPS subsystem, the "System Design Specification," Revision 9, 6116-00011, September 2015 (SDS) (Reference 127), and the "ALS-102 FPGA Requirements Specification," 6116-10201, Revision 1, May 2013 (Reference 163), are used to capture system programmable logic implementation requirements. These documents serve a similar purpose as a Software Requirements Specification (SRS) would for a computer-based system; however, they are developed to support the programmable logic-based ALS subsystem.

The ALS System Design Specification and ALS-102 FPGA Requirements Specification conform to the guidance of IEEE Std. 830-1993 (Reference 84) as amended by RG 1.172 (Reference 83).

The NRC staff reviewed the requirements documents listed above as well as the V&V reports (see Section 3.4.2.2, "V&V Analysis and Reports," of this safety evaluation). Portions of the SRS documents were also reviewed by NRC staff members during four thread audits conducted from 2012-2015 during this safety evaluation (References 36, 37, 38, and 39). During these audits, the Requirements Traceability Matrix documents were used to trace the requirements from the licensee requirements to the Tricon and ALS subsystem SRS documentation. Some of these requirements were traced from the specification through the design process and into validation test processes.

The SRS documentation for ALS and Tricon was found to comply with the characteristics necessary to facilitate the development of quality software and programmable logic for use in nuclear safety applications. The NRC staff determined that each of the DCPP requirements evaluated was appropriately included in the associated SRS documentation. The NRC staff also concludes that the subject matter of the SRS documentation is adequately controlled by the licensee's administrative programs.

3.4.3.2 Software Architecture – Description

The acceptance criterion for the software architecture description is contained in the BTP 7-14, Section B.3.3.2, "Design Activities - Software Architecture Description" (Reference 46). This section states that the Software Architecture Description should describe all of the functional and software development process characteristics listed. NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Section 3.3.1, "Hardware and Software Architecture," and Section 4.3.1, "Hardware/Software Architecture Specifications" (Reference 131), also contain relevant guidance. When performing this review, the NRC staff should be able to refer to the architecture to understand how the software works, the flow of data, and the deterministic nature of the software. The architecture should be sufficiently detailed to allow the reviewer to understand the operation of the software.

Tricon Software Architecture

The software architecture of the Tricon PPS subsystem is described and illustrated within the "Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102). Section 3.3, "Software/Core Logic Architecture," of this safety evaluation also provides a description of the Tricon platform software architecture. The functional and software development process characteristics of the software architecture were evaluated by the NRC staff. The SDD defines communication architecture information which shows how various software components of the PPS interact.

The software architecture used for the Tricon PPS subsystem is implemented within the TriStation 1131 tool environment. Requirements for the development of the application software are derived from the Functional Requirements Specification (FRS) (Reference 126), the Interface Requirements Specification (Reference 98) and the Transfer Functions Design Input Specification (Reference 99).

The software architecture description of the DCPP PPS Tricon subsystem was evaluated against the requirements of BTP 7-14, Section B.3.3.2, "Design Activities - Software Architecture Description" (Reference 46), and found to be sufficiently detailed to allow the NRC staff reviewers to understand the operation of the Tricon application software. The software architecture description as documented in the SDD describes the functional and software development process characteristics listed in BTP 7-14. Relative guidance provided by NUREG/CR-6101, Sections 3.3.1 and 4.3.1 (Reference 131), was also reviewed and the DCPP PPS Tricon software architecture description was determined to be compliant.

The SDD was referred to during the NRC staff reviews. It provided mapping information necessary to determine how the various system software components interfaced with the Tricon hardware on which they run. The NRC staff concludes that the SDD adequately describes how the Tricon application software works. The flow of data between internal software modules and components as well as between the safety processors and external systems is defined within the SDD. The software is deterministic in nature. An evaluation of the PPS deterministic behavior is provided in Section 3.17, "Deterministic System Behavior," of this safety evaluation. The software architecture as described in the SDD is sufficiently detailed to allow the reviewer to understand the operation of the software.

ALS Logic Architecture

The ALS subsystem of the DCPP PPS uses technology that does not use software while the system is in operation. Instead, the ALS system uses software to generate a hardware layout that is implemented in a field programmable gate array (FPGA) circuit board. Because of this, the operational ALS subsystem architecture is hardware and not software-based.

The FPGA logic architecture of the ALS PPS subsystem is described and illustrated within the PPS "ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, May 2013 (Reference 163), the "ALS-102 Core A FPGA Design Specification," Revision 0, 6116-10203, May 2013 (Reference 164), and "ALS-102 Core B FPGA Design Specification," Revision 0, 6116-10204, dated April 18, 2013 (Reference 165). Section 3.3, "Software/Core Logic Architecture," of this safety evaluation also provides a description of the ALS platform core logic architecture. The functional and FPGA logic development process characteristics of the ALS architecture were evaluated by the NRC staff. The FPGA specifications define communication architecture information which shows how various components of the PPS ALS subsystem interact.

The FPGA logic architecture used for the ALS PPS subsystem is implemented using standardized platform circuit boards and application-specific FPGA logic programming of the ALS-102 boards. The NRC staff performed an evaluation of the FPGA logic development processes during the safety evaluation of the ALS platform. A description of this process and the results of this evaluation are documented in Section 3.2 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). Requirements for the development of the FPGA application logic are derived from the Functional Requirements Specification (FRS) (Reference 126), the Interface Requirements Specification (Reference 98), and the Transfer Functions Design Input Specification (Reference 99).

The core logic architecture description of the DCPP PPS ALS subsystem was evaluated against the requirements of SRP BTP 7-14, Section B.3.3.2, "Design Activities - Software Architecture Description" (Reference 46), and found to be sufficiently detailed to allow the NRC staff reviewers to understand the operation of the ALS application logic. The core logic architecture description as documented in the FPGA specifications describes the functional and FPGA development process characteristics listed in SRP BTP 7-14. Relative guidance provided by NUREG/CR-6101, Sections 3.3.1 and 4.3.1 (Reference 131), was also reviewed and the DCPP PPS ALS core logic architecture description was determined to be compliant.

The FPGA specifications were referred to during the NRC staff reviews. They provided mapping information necessary to determine how the various system components interfaced with other PPS components. The NRC staff concludes that the FPGA specifications adequately describe how the ALS application logic works. The flow of data between internal FPGA logic modules as well as between the ALS boards and external systems is defined within the FPGA specifications. The FPGA logic is deterministic in nature. An evaluation of the PPS deterministic behavior is provided in Section 3.17, "Deterministic System Behavior," of this safety evaluation. The FPGA logic architecture as described in the FPGA specification documents is sufficiently detailed to allow the reviewer to understand the operation of the FPGA logic.

3.4.3.3 Software Design Description

The acceptance criteria for software design description are contained in SRP BTP 7-14, Section B.3.3.3, "Design Activities - Software Design Specification" (Reference 46). This section states that the software design should accurately reflect the software requirements, and that NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Section 3.3.2, "Software Design Specification," and Section 4.3.2, "Software Design Specifications," contain relevant guidance (Reference 131).

Tricon Software Design Description

Portions of the digital DCPP PPS Tricon subsystem "Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102), were reviewed by the NRC staff to determine if the above regulatory requirements were satisfied. The functional and software development process characteristics of the SDD were evaluated and determined to be acceptable for use in nuclear safety software applications. Thread audits were conducted on November 13-12, 2012 (Reference 36), and June 3-5, 2014 (Reference 38), at the Invensys facilities in Lake Forest, California. During these audits, several requirements were checked and traced through to the function block diagrams in the TriStation 1131 development environment. The SDD was understandable and contained sufficient information to facilitate implementation of requirements into the development environment. A review of the design phase validation and verification (V&V) summary report was also conducted (see Section 3.4.2.2.1.2, "Design Phase V&V Activity Summary Report," of this safety evaluation) and the NRC staff concluded that the V&V team performed an adequate job of assuring the SDD was developed and used in a manner that resulted in the development of quality software capable of performing all safety functions for the system.

The Tricon SDD was evaluated against the acceptance criteria for SDD contained in BTP 7-14, Section B.3.3.3. The SDD accurately reflected the software requirements included in the evaluation. The guidance of NUREG/CR-6101, Sections 3.3.2 and 4.3.2, was also reviewed and the SDD was determined to be compliant.

ALS Subsystem FPGA Design Descriptions

The ALS subsystem of the DCPP PPS uses technology that does not use software while the system is in operation; therefore, there is no SDD document for the ALS subsystem. Instead, the ALS system uses Core FPGA Design Specification documents to capture SDD equivalent information.

Portions of the digital DCPP PPS "ALS-102 Core A FPGA Design Specification," Revision 0, 6116-10203, May 2013 (Reference 164), and "ALS-102 Core B FPGA Design Specification," Revision 0, 6116-10204, dated April 18, 2013 (Reference 165), were reviewed by the NRC staff to determine if the above regulatory requirements were satisfied. The functional and software development process characteristics of the Core FPGA Design Specifications were evaluated and determined to be acceptable for use in nuclear safety software applications. Two thread audits were conducted on February 11-14, 2013 (Reference 37), and June 22-26, 2015 (Reference 39), at the Westinghouse facilities in Scottsdale, Arizona, and in Warrendale, Pennsylvania, respectively. During these audits, several requirements were checked and traced through to the Core FPGA Design Specifications. The Core FPGA Design Specifications were understandable and contained sufficient information to facilitate implementation of requirements into ALS subsystem. A review of the Design Phase V&V summary report was also conducted (see Section 3.4.2.2.2.3, "ALS - Requirements Phase Activities," of this safety evaluation) and the NRC staff concluded that the V&V team performed an adequate job of assuring the Core FPGA Design Specifications were developed and used in a manner that resulted in the development of quality FPGA logic capable of performing all safety functions for the system.

The Core FPGA Design Specifications were evaluated against the acceptance criteria for SDD contained in SRP BTP 7-14, Section B.3.3.3. The Core FPGA Design Specifications accurately reflect the FPGA requirements included in the evaluation. The guidance of NUREG/CR-6101, Sections 3.3.2 and 4.3.2, was also reviewed and the Core FPGA Design Specifications were determined to be compliant.

3.4.3.4 Failure Modes and Effects Analysis/Reliability Analysis

The failure modes and effects analysis (FMEA) is an analysis of potential failure modes within a system for determining the effects of failures on the system. A system reliability analysis is used to assess system and component reliability and availability with respect to pre-established goals. The reliability analysis is also used to confirm that the PPS design can support the surveillance test intervals to be implemented for the system. The FMEA and reliability analysis are used to address the single-failure and reliability requirements of the system. This information can then be used to assess the potential for an undetectable failure that could lead to a loss of a required safety function. There is no specific regulatory guidance on the required format, complexity, or conclusions concerning the FMEA or reliability analysis; however, the following guidance was used by the NRC staff as a means of determining the effectiveness of the FMEA and reliability analysis programs as recorded in the documents provided:

1. IEEE Std. 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 61)

2. Regulatory Guide (RG) 1.153, Revision 1, "Criteria for Safety Systems," June 1996 (Reference 72)

3. IEEE Std. 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Section 5.1, "Single-Failure Criterion," and the correction sheet dated January 30, 1995 (Reference 32)

4. IEEE Std. 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Section 5.15, "Reliability" (Reference 32)

Because the DCPP PPS is divided into two subsystems, each of these subsystems was independently assessed by the NRC staff to determine if the associated FMEA and reliability analysis are sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures.

Tricon

Invensys performed an FMEA as documented in "Failure Modes and Effects Analysis," Revision 1, 993754-1-811-P, dated February 21, 2014 (Reference 170), of the Tricon portion of the digital PPS using guidance contained in the Electric Power Research Institute (EPRI) technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), for qualifying commercially available programmable logic controllers for safety-related nuclear power plant applications. A systematic analysis of the design was performed to identify credible failures, evaluate the consequence and effects of failures, and to verify the design satisfies the single-failure criterion.

The NRC staff used RG 1.153, Revision 2, "Criteria for Safety Systems," November 2003 (Reference 60), which endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 61), to verify that the Tricon portion of the PPS design satisfies the single-failure criterion of IEEE Std. 603-1991 Section 5.1.

A total of 142 failure modes were postulated in the Invensys FMEA. These failure modes are divided into five types of failure and the results of this analysis are provided in FMEA Appendices A through E. The types of failure considered in the FMEA are:

A. Failure of Tricon subsystem safety-related components

B. Failure of Tricon subsystem non-safety-related components

C. Failure of safety-related software

D. Failures associated with input module signal loading

E. Failures associated with PPS buyout components

For each postulated failure mode, a failure category was assigned in order to identify the effect of the failure on system operation. The following four major categories were used:

C1 - States that result from one or more failures where the programmable logic controller remains operable as well as states where it is not operable

C2 - States where undetected failures have occurred

C3 - States where a failure in a single element has caused the programmable logic controller to fail

C4 - States where failures reduce the effectiveness of self-diagnostics

The effects on the PPS and on Tricon subsystem operability were also identified for each postulated failure mode. The NRC staff evaluation concentrated on failures that could be considered undetectable which are the category C2 failures. There were 33 failure modes categorized as undetectable (C2). These failure modes are considered to be undetectable by the system because they may not be revealed during normal system operation and would require additional measures to detect and mitigate the consequences of such a failure. For each undetectable failure, a description of the failure including a discussion of conditions for non-detectability was provided. The NRC staff reviewed the effects or criticality level for each of these failure modes and concluded none of these failures will affect continued operation of the Tricon PPS subsystem. This means that there is no resulting immediate loss of safety function; however, there may be a loss of system functional redundancy.

If the identification of failure modes through the use of administrative means such as channel checking and performance of surveillance testing is considered, then the number of credible failure modes that are considered as undetectable is reduced to none. As long as administrative controls and surveillance tests are implemented to identify the failure modes that are not otherwise detected by the system diagnostics or through other means, then there are no undetectable failure modes for the Tricon portion of the PPS that would result in the inability for the system to perform its assigned safety functions.

Tricon Software Failure Modes

Tricon software failure modes are analyzed in Appendix C of the FMEA (Reference 170). These failure modes are design errors that are introduced to the system either during development activities or during subsequent intentional or unintentional changes made to system software. The effects of random external interactions that can affect memory values within the system were considered in the FMEA. Such a failure would result in an alarm indication and operator response is credited for the mitigation.

One of the postulated software failure modes was identified as being undetectable. This was the "Erroneous data and I/O outputs" software fault. This failure would however cause erratic operation of the affected Tricon and the analysis stated that redundant PPS channels are unaffected; therefore, Tricon PPS safety functions would not be impacted by this failure. In the case of a common-cause software fault of this nature, the PPS Tricon safety functions could become compromised; however, the effects of such a failure are considered in the "Diablo Canyon Power Plant, Topical Report: Process Protection System Replacement, Diversity & Defense-in-Depth Assessment," Revision 1, August 2010 (DCPP D3 analysis) (Reference 97). The DCPP D3 analysis was performed with the assumption that all safety functions performed by the Tricon portion of PPS could become disabled as a result of a software common-cause failure. Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation provides additional information on PPS diversity as well as an evaluation of measures to cope with the effects of a Tricon software common-cause failure.

Tricon Reliability Analysis

Invensys performed the "Reliability Analysis," Revision 0, 993754-1-819-P, dated October 11, 2013, of the Tricon portion of the digital PPS (Reference 171). The stated purpose of the Reliability Analysis includes providing a quantitative reliability analysis of the Tricon's performing the reactor trips and the engineered safety features actuation system (ESFAS) functions.

The NRC staff reviewed the results of the Tricon Reliability Analysis and determined the availability values presented in Tables 2-1 and 2-2 to be consistent with expected performance specifications for safety-related protection systems in nuclear power plants.

Section 3.5.3, "System Reliability," of the PPS "Functional Requirements Specification," October 2012 (Reference 126), states, in part, that "system diagnostics and self-testing features shall be incorporated in the design to provide automatic detection (where possible) of component failures or degradation of operability." The licensee stated that the system self-testing features are being incorporated into the system design as a means of achieving high reliability. The NRC staff determined that the Tricon portion of the PPS is designed to be highly reliable by using multiple layers of redundancy and including self-testing features and is therefore acceptable for use in the DCPP PPS.

ALS

Westinghouse CS Innovations performed a reliability analysis and FMEA documented in "Diablo Canyon PPS ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Reference 153), of the ALS portion of the PPS using guidance contained in the references listed below to verify that the design satisfies the single-failure criterion of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995 (Reference 32).

1. MIL-HDBK-217F, Notice 2, "Military Handbook: Reliability Prediction of Electronic Equipment," U.S. Department of Defense, February 1995 (Reference 172).

2. MIL-HDBK-338B, "Military Handbook: Electronic Reliability Design Handbook," U.S. Department of Defense, October 1998 (Reference 173).

3. IEEE Std. 352-1987 [reaffirmed 1999], "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," Institute of Electrical and Electronics Engineers (Reference 174).

4. IEEE Std. 577-2004, "Standard Requirements for Reliability Analysis in the Design Operation of Safety Systems for Nuclear Power Generating Facilities," Institute of Electrical and Electronic Engineers (Reference 175).

5. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronic Engineers (Reference 33).

A systematic analysis of the design was performed to identify all credible failures, evaluate the consequence and effects of failures, and to verify that the ALS portion of the PPS design satisfies the single-failure criterion of IEEE Std. 603-1991 Section 5.1.

In the Westinghouse CS Innovations Reliability Analysis and FMEA, a total of 108 failure modes were postulated. For each of these failure modes, a determination of criticality, likelihood, and detectability was made. The NRC staff evaluation concentrated on failures that could be considered undetectable. The FMEA assigned a degree of detectability for each failure mode from 1 to 10 according to the following criteria:

Failure Detectability Codes:

1. Revealed by diagnostic, specified corrective action is evident from status indication.

2. Revealed by diagnostic, additional troubleshooting needed to localize the fault.

3. Revealed by diagnostic, automatic default action needed to prevent an adverse effect.

4. Revealed by diagnostic, graceful degradation of control mode needed to cope.

5. Revealed through change in plant state caused by failure.

6. Evident through operator observation, but no direct indication of fault.

7. No loss of function, but would be revealed by additional failure.

8. Revealed by planned surveillance test, but not by diagnostics.

9. Could be revealed by an as-built, in-place test that is not included in the planned surveillance program.

10. Failure mode cannot be detected without disassembling equipment to isolate component, or requires plant shutdown to perform test.

Of the 108 postulated failure modes, 39 were rated with a detectability code of 6 or higher. These failure modes are considered to be undetectable by the system because they might not be revealed during normal system operation and would require additional measures to detect and mitigate the consequences of such a failure. The highest criticality level identified for these failure modes is 2, which is considered to be of very minor consequence. This means that there is no resulting immediate loss of function; however, there may be a loss of system functional redundancy.

If the identification of failure modes through the use of administrative means such as channel checking and performance of surveillance testing is considered, then the number of credible failure modes that are considered as undetectable is reduced to none. As long as administrative controls and surveillance tests are implemented to identify the failure modes of the ALS system that are not otherwise detected by the system diagnostics, self-test, or through other means, then there are no undetectable failure modes for the ALS portion of the PPS that would result in the inability for the system to perform its assigned safety functions.

There are several failure modes identified in the FMEA where the system effects entries provide a description of functions that are not affected by the failure mode instead of stating what the effects of the failure mode are. The staff noted that for these cases, the systematic effects of the failure mode were not clear. An NRC staff request for additional information (RAI) regarding these failure effects was sent to the licensee by letter dated August 7, 2012 (Reference 35). In its RAI response dated May 9, 2013 (Reference 13), the licensee provided clarification that these system effects are being evaluated within the context of the local effects that are also provided in the FMEA. Application-specific compensating features that influence the systematic effects of these failure modes are thus accounted for within the analysis.

In the ALS subsystem FMEA, software faults are not considered to be credible failure modes of the system and therefore none are postulated. Though software-based tools are used at various stages of the ALS system development processes, the implemented system which performs the safety functions of the PPS is composed of a hardware realization of a logic structure, so no software is required or is being relied upon for operation of the ALS subsystem. The NRC staff recognizes that software faults of the tools used during system development can lead to faults in the system design; however, these faults should be identified and corrected through the verification and validation (V&V) activities that are included in the development lifecycle. As such, these faults do not need to be considered as system failure modes for the purposes of the FMEA.

ALS Reliability Analysis

The reliability analysis of the ALS portion of the digital PPS (Section 5 of the "Diablo Canyon PPS ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012; Reference 153) was also reviewed by the NRC staff. This Reliability Analysis provides calculated values for mean time between failure, repair time analysis, reliability block diagram analysis, calculated probability of failure on demand, spurious actuation rate analysis, and a discussion of surveillance test intervals.

The NRC staff reviewed the results of the ALS Reliability Analysis and confirmed the availability values to be consistent with expected performance specifications for safety-related protection systems in nuclear power plants.

Section 3.5.3, “System Reliability,” of the Functional Requirements Specification (Reference 126), states that “[s]ystem diagnostics and self-testing features shall be incorporated in the design to provide automatic detection (where possible) of component failures or degradation of operability.” The licensee stated that the system self-testing features are being incorporated into the system design as a means of achieving high reliability. The NRC staff determined that the ALS portion of the PPS is designed to be highly reliable by using multiple layers of redundancy and including self-testing features and is, therefore, acceptable for use in the DCPP PPS.

Conclusions

The NRC staff reviewed the DCPP digital PPS FMEA and Reliability Analysis documentation and has determined that the level of detail is adequate for a system with this degree of complexity. The FMEAs are sufficiently detailed to provide a useful assessment of the potential failures and the effects of those failures. The NRC staff agrees with the licensee’s determination that the FMEAs provide reasonable assurance that single-failure criterion is met for all creditable single failures and all failures caused by a single-failure. The FMEAs conclude that an input signal or system failure, including power supply or input power failure, will cause the digital PPS to fail in a predefined safe state and will annunciate that failure to the operators. Based on the NRC staff’s review of the FMEAs, there is reasonable assurance that all credible failure modes have been properly identified and evaluated for the DCPP PPS.

3.4.3.5 System Failure Modes and Effects Analysis

The licensee performed a system-level FMEA for the digital PPS as documented in “System Level Failure Modes & Effects Analysis (FMEA), Document No. 15-0681-FMEA-001, Revision 0, March 2016 (Reference 177). This system FMEA evaluates PPS equipment not included in the FMEAs performed by the platform vendors (i.e., those FMEAs evaluated in Section 3.4.3.4, “Failure Modes and Effects Analysis/Reliability Analysis,” of this safety evaluation). The system FMEA evaluates interfaces between the Tricon and ALS platforms and was conducted in accordance with the guidance provided in IEEE Std. 379-2000, “IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems” (Reference 61), as endorsed by RG 1.53, Revision 2, “Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems,” November 2003 (Reference 60).

The system FMEA identified a new vulnerability being introduced to the PPS by this modification. While the existing Eagle 21 digital process protection system (PPS) provides separate analog outputs to the main control room and hot shutdown panel indicators, the new design has hot-leg and cold-leg temperature indicators in the same loop as the PPS input without isolation. A credible fire rendering the main control room uninhabitable could therefore also cause hot shutdown panel indications to fail. To address this identified hazard, transfer switches are being used to allow switching the resistance temperature detector inputs to feed new hot shutdown panel indicators instead of the PPS in the event of a fire. The licensee is also installing incipient fire detection devices inside the susceptible cabinets. Installation of these devices were approved in license conditions for DCPP, Units 1 and 2, issued in the

April 14, 2016, license amendment to revise the fire protection program in accordance with 10 CFR 50.48(c) (Reference 178).

The NRC staff reviewed the system-level PPS FMEA and determined the FMEA is sufficiently detailed to provide a useful assessment of the potential system component failures and the effects of those failures. The NRC staff agrees with the licensee's determination that the FMEA provides reasonable assurance that single-failure criterion are met for all creditable single failures and all failures caused by the single-failure. The system FMEA concludes that component, system level or interface failures, including vital power supply or subsystem power source failures, will not cause the digital PPS to fail to a state which is not considered in the plant accident analysis. The PPS will also annunciate failures to the operators. Based on the NRC staff's review of the FMEA, there is reasonable assurance that credible failures have been properly identified and evaluated for the DCPP PPS.

3.4.3.6 Code Listings

The criteria for the code listings are contained in Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.3.4, "Implementation Activities - Code Listings" (Reference 46). This section states that NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," June 1996 (Reference 179), contains relevant guidance. The code listings should have sufficient comments and annotations that the intent of the code developer is clear. This is not only so the reviewer can understand and follow the code, but also so future modifications of the code are facilitated. Undocumented code should not be accepted as suitable for use in safety-related systems in nuclear power plants. The documentation should be sufficient for a qualified software engineer to understand.

Tricon Function Block Diagrams

For the DCPP PPS Tricon subsystem Test System Application Program (TSAP) application, structured text and function block diagrams (FBDs) are translated into executable code by the TriStation 1131 Developers Workbench. Because programming interactions take place at the graphical user interface, the structured text and FBDs can be considered to be functionally equivalent to annotated source code. The structured text and FBDs within the TriStation 1131 environment were reviewed by the NRC staff during the thread audit activities conducted on November 13-16, 2012 (Reference 36), and June 3-5, 2014 (Reference 38).

The NRC staff bases its acceptance of the structured text and FBDs on the ability to understand and follow the signal paths, and to understand the functionality implemented by the TriStation FBDs. These FBDs contain provisions for commenting; however, detailed descriptions of how each FBD operates are documented in the DCPP "Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102). Several of these descriptions were evaluated by the NRC staff and were determined to provide sufficient information for a qualified software engineer to understand. The verification and validation (V&V) effort for the implementation phase was reviewed (see Section 3.4.2.2.1.3, "Tricon Implementation Phase V&V Activity Summary Report," of this safety evaluation). The test for the requirement was examined to determine if the test adequately verified the resulting system met the requirement.

The FBDs are sufficiently documented via the associated descriptions and annotations provided in the SDD such that the intent of the code developer is clear. This facilitates future modifications of the FBDs. No undocumented code or function blocks were identified during the evaluation of the FBDs. The documentation was determined to be sufficient for a qualified software engineer to understand. The functional and process characteristics were determined to be appropriate and adequate for use in nuclear safety software applications. Based upon this review, the NRC staff determined that the TSAP application code was appropriate for safety-related use in the DCPP PPS Tricon subsystem.

3.4.3.7 System Build Documents

The acceptance criteria for the system build documentation are contained in Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, Section B.3.3.5, "Integration Activities - System Build Documents" (Reference 46). This section states that NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," Section 3.5.1, "System Build Documents," and Section 4.5.1, "System Build Documents" (Reference 131), contain relevant guidance. The build documentation is generally needed to verify that the software actually delivered and installed on the safety system is the same software that underwent the V&V process and was tested. Any future maintenance, modifications, or updates will require that the maintainers know which version of the programming to modify, and therefore the system build documentation is closely tied to the configuration management plan. The items, including programming, should check to ensure that the programming listed in the build documentation is identified by version, revision, and date, and that this is the version and revision that was tested.

<u>Tricon</u>

For the DCPP PPS Tricon software, the master configuration list reflects the state of the software configuration items. The master configuration list is maintained through the testing, commissioning and final documentation phases of the project as identified in the "Software Configuration Management Plan (SCMP)," Revision 1, 993754-1-909-P, dated December 18, 2012 (Reference 116). Application function block diagrams (FBDs) as augmented by the Tricon technical requirements list constitute the build documentation for the Tricon subsystem.

Once the application FBDs are completed, the TriStation 1131 Developer's Workbench software tool is used to convert the FBDs into executable files and to load these files onto the PPS processors. The TriStation 1131 tool assigns version numbers to the application files. These assigned version numbers provide a basis for tracking system development progress and for maintaining software configuration control. A software development checklist defines a process for building a program, which includes steps for generation of the application software and for loading the project software and configuration files onto the PPS hardware. The master configuration list is used to capture and control software configuration information for all software configuration items.

The NRC staff reviewed these procedures and determined that the software development checklist processes, when used in conjunction with established software library and control instructions, provides adequate measures to ensure that downloaded software and program components have been directly derived from the verified and validated FBDs.

Comparison of software configuration documentation to the software installed in the delivered PPS equipment will be performed upon plant installation. Site inspection follow-up item 5 in Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation is included to provide confirmation of this activity.

<u>ALS</u>

For the ALS subsystem, the application logic configuration information is recorded in the DCPP PPS ALS board configuration drawings. These drawings are used to capture board and non-volatile memory part and version numbers which are unique to each logic implementation. The configuration drawings are maintained through the testing, commissioning, and final documentation phases of the project as identified in the "ALS Configuration Management Plan," Revision 11, 6002-00002-P, March 2015 (Reference 146). The ALS field programmable gate array (FPGA) specifications in conjunction with ALS board configuration drawings constitute the application-specific logic build documentation for the ALS subsystem.

Comparison of the ALS logic configuration documentation to the installed FPGA logic in the delivered PPS equipment will be performed upon plant installation. Site inspection follow-up item 3 in Section 3.14.2, "ALS Site Inspection Follow-up Items," of this safety evaluation is included to provide confirmation of this activity.

The NRC staff concludes that the build documentation for the DCPP PPS Tricon software and ALS logic provides an adequate level of assurance that software and logic delivered and installed onto the safety system hardware is the same software and logic that underwent the V&V processes and was tested. The build documentation provides the necessary configuration version information such that future maintenance, modifications, or updates to the software or logic can be satisfactorily performed in conjunction with the configuration management program. Program items included in the build documentation are adequately identified by version, revision, and date. The final comparison of software and logic configuration item data to the delivered equipment can be inspected by the NRC during system installation.

3.5 Equipment Environmental Qualification

3.5.1 Environmental Qualification of System

The Commission's regulations for environmental qualification of electric equipment important to safety for nuclear power plants are provided in 10 CFR 50.49. However, as stated in

10 CFR 50.49(c), requirements for (1) dynamic and seismic qualification of electric equipment important to safety, (2) protection of electric equipment important to safety against other natural phenomena and external events, and (3) environmental qualification of electric equipment important to safety located in a mild environment are not included within the scope of 10 CFR 50.49. A mild environment is an environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences.

Two objectives of the digital process protection system (PPS) platform environmental testing are (1) to demonstrate through testing that the system will not experience failure due to abnormal service conditions of earthquake, temperature, humidity, radiation, electromagnetic, and radio frequency interference, and (2) to verify those tests bound the worst-case DCPP plant-specific environmental conditions for all accidents and transients that the digital protection system is required to mitigate.

Some criteria for environmental qualifications of safety-related equipment at DCPP are provided in General Design Criterion (GDC) 2, 1967, "Performance Standards," and GDC 4, 1987, "Environmental and dynamic effects design bases." Additionally, 10 CFR 50.55a(h), "Protection and safety systems," incorporates Institute for Electrical and Electronics Engineers (IEEE) Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Reference 32), which address both system-level design issues and quality criteria to qualify components. Section 5.4, "Equipment Qualification," of IEEE Std. 603-1991 states that the equipment qualification requirements for the safety systems shall be in accordance with IEEE Std. 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

The DCPP PPS equipment will be located in a mild environment. Regulatory Guide (RG) 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007 (Reference 93), states that guidance described in IEEE Std. 323-2003 (Reference 94) is appropriate for satisfying the environmental qualification of safety-related computer-based instrumentation and control systems for service in mild environments at nuclear power plants subject to certain enhancements and restrictions. Clause 3.14, of IEEE Std. 323-2003, defines the mild environment as, "An environment that would at no time be significantly more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences."

Environmental qualifications are necessary to ensure instrumentation and control systems meet design basis and performance requirements when the equipment is exposed to the normal and adverse environments associated with its location.

3.5.1.1 Temperature/Humidity

The replacement PPS will be located in the DCPP cable spreading room within the same 16 cabinets that currently house the Eagle 21 PPS. Section 3.11.2.1, "Accident Environments," of the DCPP Final Safety Analysis Report Update (FSARU) describes qualification tests and analyses for accident environments and Section 3.11.2.2, "Normal Environments," provides this information for normal environments. "Environmental Conditions for EQ [Equipment Qualification] of Electrical Equipment," included as Appendix A of Design Criteria Memorandum (DCM) T-20 provides information specific to environmental conditions for qualifying electrical equipment.

Section 3.1.4, "Environmental Conditions," of the DCPP PPS "Functional Requirements Specification," October 2012 (Reference 126), requires mild environment qualification to meet the following ambient environmental conditions of the cable spreading room:

Temperature: 40-104 degrees Fahrenheit (°F)
Relative Humidity (RH) (percent Non-condensing): 0-95 percent RH
Pressure: Atmospheric

Tricon temperature and humidity testing was evaluated in Section 3.3.4 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29), and ALS environmental testing was evaluated in Section 3.3.2 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The following sections summarize the temperature and humidity evaluations for each of the platforms comprising the DCPP PPS.

Tricon

Tricon environmental qualification testing was performed by National Technical Systems Laboratories from December 13, 2006, to January 15, 2007, in Boxborough, Massachusetts. Tests were conducted on Tricon V10 platform components in accordance with the Electric Power Research Institute (EPRI) technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), and IEEE Std. 381-1977, "IEEE Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations" (Reference 180). Section 6.2.1.1.B of EPRI TR-107330 requires that modules be arranged to simulate the maximum expected temperature rise across the chassis for any reasonable arrangement of the modules included for qualification. The test specimen included four Tricon V10 programmable logic controller (PLC) chassis populated with main processor, input, output, communication, chassis interface, and chassis power supply modules as well as external termination panels and interfacing cable assemblies. The Tricon test specimen met its performance requirements during and following exposure to abnormal environmental conditions of 35 °F to 140 °F and 5 percent to 95 percent relative humidity (RH) (non-condensing) according to a time varying profile.

During these tests, the Tricon test specimen operated as intended during and after exposure to the environmental test conditions. Normal operating performance data (inputs, outputs, and diagnostic indicators) were monitored during testing to demonstrate operation as intended. The specimen passed operability tests (1) following 48 hours of operation at high temperature and humidity, (2) following 8 hours of operation at low temperature and humidity, and (3) upon completion of the test. The test specimen also passed a prudency test following 48 hours of operation at high temperature and humidity. Section D.5.4.1, "Atmospheric," of DI&C-ISG-06, "Task Working Group #6: Licensing Process, Interim Staff Guidance," Revision 1, dated January 19, 2011 (Reference 24), states that typically the most limiting combination of temperature and humidity occurs at high values of both. Tricon testing was performed at high temperature and humidity levels that bound conditions for the DCPP plant site specified in Section 3.1.4, "Environmental Conditions," of the DCPP PPS "Functional Requirements Specification," October 2012 (Reference 126).

As part of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29), the NRC staff reviewed the Invensys Operations Management "Environmental Test Report," Document No. 9600164-525, Revision 0, dated July 17, 2007 (Reference 181), and determined that the Tricon V10 test specimen met the requirements of EPRI TR-107330, Sections 4.3.6 and 6.3.3, and IEEE Std. 381-1977.

ALS

Environmental qualification tests were conducted on ALS platform components in accordance with IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 66), as endorsed by RG 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Revision 1, dated June 1984 (Reference 65), and IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 94), as endorsed by RG 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," Revision 0, March 2007 (Reference 93). The manufacturer produced configuration controlled specifications, plans, and procedures with acceptance and performance criteria for performing environmental type testing on seven standardized circuit boards, a backplane, and a chassis. The manufacturer justified the configuration of its type-tested equipment through its choice of board configurations (e.g., least filtering, highest baud rate, etc.) with the potential to be most susceptible to environmental effects and therefore most likely to reveal unacceptable performance. The manufacturer's "ALS EQ Plan," Revision 8, 6002-00004, December 2012 (Reference 182), defines its environmental qualification approach and the "ALS Platform EQ Summary Report," Revision 2, 6002-00200, January 2013 (Reference 183), provides a detailed summary of the environmental qualification testing and results.

The ALS test specimen was tested to an environmental envelope consistent with a typical mild environment that included potential synergistic effects between temperature, humidity, and input voltage on the seven standardized circuit boards. The test specimen met its performance requirements during and following exposure to abnormal environmental conditions of 40 °F to 140 °F and 35 percent to 95 percent RH with variations in power supply voltage. In addition, the manufacturer determined the worst-case synergistic effect for the technology of the standardized circuit boards was high temperature and high voltage based on the performance of on-board power supply circuitry. The manufacturer also performed supplemental tests at high temperature and low voltage to evaluate potential adverse synergistic effects on data communications and response time. As part of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30), the NRC staff determined that the environmental qualification conforms to RG 1.209, Regulatory Positions 1, 2, and 4.

The ALS platform safety evaluation describes a worst-case synergistic effect involving temperature and voltage. A relationship between temperature and humidity is not described; therefore, this report evaluates the temperature and humidity ranges individually with respect to the conditions for the DCPP plant site. The NRC staff determined that the ALS platform temperature testing bounds the plant-specific temperature conditions because the tested temperature range is broader than that specified in Section 3.1.4, "Environmental Conditions," of the DCPP PPS Functional Requirements Specification (Reference 126). In addition, the NRC staff determined that the ALS platform humidity testing bounds the plant-specific conditions even though testing was performed to a narrower range than that specified in Section 3.1.4 of the Functional Requirements Specification. This narrower testing range is acceptable because: (1) testing was performed at the upper humidity limit for the plant site, and (2) ALS "System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127), Requirement R1610 as well as the Functional Requirements Specification, Section 3.1.6.3, "Grounding," requirement address the potential for electrostatic discharge at humidity levels below the tested range.

The NRC staff also reviewed the "Advanced Logic System and Line Sense Module Equipment Qualification Summary Report," Revision 0, EQ-QR-120-PGE, September 2014 (Reference 184). This report shows that the line sense module (LSM) was similarly tested to environmental conditions of 40 °F to 140 °F and 35 percent to 95 percent RH with variations in power supply voltage. The LSM was tested at the Westinghouse test facility in New Stanton, Pennsylvania, between August 7, 2014, and August 13, 2014. The licensee stated in Section 5.2.2.2, "LSM Test Results," of the Advanced Logic System and Line Sense Module Equipment Qualification Summary Report that the LSM was compliant with applicable safety functions and acceptance criteria during all environmental conditions. Based on this information, the NRC staff determined that the LSM environmental qualification conforms to IEEE Std. 323-2003 endorsed by RG 1.209.

Section 7.2, "Installation Limitations," of the Advanced Logic System and Line Sense Module Equipment Qualification Summary Report specifies ALS equipment installation limitations.

During the June 22-26, 2015, NRC audit at Westinghouse facilities (Reference 39), the NRC staff reviewed the test results of an informal experiment where the worst-case location (i.e., above-the-rack power supplies) maximum cabinet temperature reached 100 °F without forced ventilation. In addition, inspection item 4 included in Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation requires the licensee to demonstrate the maximum temperature, including temperature rise, within each cabinet containing ALS components does not exceed the platform specification.

Conclusion

Since the temperature and relative humidity environmental conditions within any cabinet in the DCPP cable spreading room are enveloped by the Tricon and ALS (including LSM) platform qualification testing, the NRC staff determined that IEEE Std. 323-2003 criteria are met and, therefore, the PPS is qualified for the DCPP cable spreading room temperature and humidity environment. It is therefore acceptable for the PPS Tricon and ALS (including LSM) subsystem equipment to be installed into the DCPP cable spreading room.

3.5.1.2 Radiation

Clause 6.3.1.9 of IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 94), states, in part, that

> In the type test, all materials or components, for which radiation causes significant aging, shall be irradiated to simulate the effects of the radiation exposure. If normal and accident radiation doses and dose rate are demonstrated to have no effect on the safety function(s) of the equipment, then radiation testing may be excluded, and the justification should be documented.

Digital systems susceptibility to radiation is discussed in RG 1.209, Revision 0 (Reference 93). RG 1.209 states that the radiation threshold is different for different types of digital technology, ranging from complementary metal oxide semiconductor technology, which can be susceptible as low as 1 kilorad (krad) exposure to bipolar devices, which are not susceptible until 1000 krad.

The DCPP Functional Requirements Specification (Reference 126) does not include a specified radiation level. Instead, Section 3.1.4.1.4, "Radiation," specifies the radiation environmental condition for qualification as "N/A (mild environment)" because no appreciable radiation levels are expected to exist during normal plant operation or during anticipated operational occurrences in the cable spreading room where the PPS equipment will be installed.

Tricon radiation withstand testing was evaluated in Section 3.3.3, "Radiation WITHSTAND Test," of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29). However, the ALS test specimen was not subjected to radiation withstand testing and therefore was not evaluated in the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The following sections describe the radiation qualification of these subsystems for use in a mild environment.

Tricon

Radiation withstand testing was performed by National Technical Systems Laboratories at a gamma irradiation test facility at the University of Massachusetts from December 13-14, 2006. Testing was performed to the requirements in Section 4.3.6.1, "Normal Environmental Basic Requirements," and 4.3.6.2, "Abnormal Environmental Basic Requirements," of EPRI technical report (TR)-107330 (Reference 101) and in accordance with the general requirements in

IEEE Std. 381-1977 (Reference 180). The test specimen included chassis, power supplies, modules, external termination assemblies, and interconnecting cabling. The Tricon test specimen met all applicable performance requirements after application of radiation test conditions of 1 krad plus margin with each test run just over 2 hours in duration.

The Tricon portion of the PPS will be installed into cabinets in the cable spreading room where total integrated dose is expected to be significantly less than 1 krad. This was confirmed by the NRC staff's review of Section 2.4.3.4 of Design Criteria Memorandum (DCM) T-20, Appendix A, "Environmental Conditions for EQ of Electrical Equipment." Therefore, the NRC staff determined the radiation test conditions envelop the mild environmental conditions for the DCPP plant site specified in Section 3.1.4, "Environmental Conditions," of the DCPP PPS Functional Requirements Specification (Reference 126).

ALS

The ALS platform equipment was not subjected to radiation withstand testing and is not intended or qualified for use in environments where significant radiation levels are present. The licensee's threshold for radiation qualification is 1 krad total integrated dose outside containment (Section 3.5 of DCM T-20, "Environmental Qualification"), which corresponds to the RG 1.209 threshold for commercial off-the-shelf circuits using metal oxide semiconductor technology. Therefore, the NRC staff determined that excluding radiation withstand testing is acceptable because (1) ALS components will be installed into cabinets in the cable spreading room where the total integrated dose is expected to be significantly less than 1 krad (Section 2.4.3.4 of DCM T-20, Appendix A), and (2) the total integrated dose is significantly below the licensee's threshold for radiation qualification and the threshold for susceptibility in RG 1.209.

Conclusion

Since the DCPP cable spreading room radiation levels are expected to be significantly less than 1 krad during normal plant operation and during anticipated operational occurrences, the NRC staff determined that IEEE Std. 323-2003 criteria are met and, therefore, the PPS is qualified for the DCPP cable spreading room radiation environment. It is therefore acceptable for the PPS Tricon and ALS subsystem equipment to be installed into the DCPP cable spreading room.

3.5.1.3 Seismic

Regulatory Guide (RG) 1.100, Revision 3, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," September 2009 (Reference 185), describes methods that the NRC staff considers acceptable for use in seismic qualification of electrical and active mechanical equipment. The RG provides an endorsement of IEEE Std. 344-2004, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear

Power Generating Station" (Reference 186), with exceptions and clarifications. Clause 5 of IEEE Std. 344-2004, states:

> The seismic qualification of equipment should demonstrate an equipment's ability to perform its safety function during and/or after the time it is subjected to the forces resulting from one [Safe Shutdown Earthquake (SSE)]. In addition, the equipment must withstand the effects of a number of [Operating Basis Earthquakes] prior to the application of an SSE.

An Operating Basis Earthquake is a seismic event during which all equipment necessary for continued plant operation without undue risk to the health and safety of the public is required to remain functional. A Safety Shutdown Earthquake is the maximum considered earthquake in the design of a nuclear power plant and the earthquake for which structures, systems, and components important to safety are designed to remain functional.

Regulatory Guide (RG) 1.61, Revision 1, "Damping Values for Seismic Design of Nuclear Power Plants," March 2007 (Reference 187), establishes evaluation guidance for applicants and licensees regarding the acceptable damping values that the NRC staff use in the seismic response analysis of Seismic Category 1 nuclear power plant structures, systems and components.

Section 4.3.9, "Seismic Withstand Requirements," of the Electric Power Research Institute (EPRI) technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), provides additional guidance for establishing seismic withstand requirements for digital protection systems.

Section 3.1.5, "Seismic Requirements," of the DCPP Functional Requirements Specification (Reference 126) establishes the seismic criteria for the PPS. These criteria are applicable to both the Tricon and ALS PPS subsystems. Section 3.1.5 states that PPS Class I equipment shall be qualified to Seismic Category I levels by test, analysis, or a combination thereof, to satisfy the requirements of IEEE Std. 344. Section 3.1.5.1 refers to seismic response spectra requirements as identified in Design Criteria Memorandum (DCM) C-17, "Hosgri Response Spectra"; DCM C-25, "Design Earthquake Response Spectra for Structures, Systems and Components"; and DCM C-30, "Double Design Earthquake Response Spectra for Structures, Systems, and Components." Section 3.1.5.2 states the requirement for seismic qualification of equipment and components in accordance with DCM T-10, "Seismic Qualification of Equipment."

Final Safety Analysis Report Update Plant-Specific Seismic Requirements

Section 1.2.1.6, "Seismology," of the DCPP Final Safety Analysis Report Update, Revision 22 (FSARU), May 2015 (Reference 52), states, in part, that

> Seismological investigations were undertaken to determine the potential for earthquakes in the site area, to form a basis of the establishment of seismic design criteria, and to evaluate the adequacy of seismic design margins for the plant....

This seismic design basis is further described in FSARU Chapter 2.5, "Geology and Seismology."

The maximum ground acceleration that would occur at the DCPP site has been estimated for each of the postulated earthquakes. The maximum rock accelerations that would occur at the DCPP site are estimated as:

> Earthquake A . . . . 0.10 g
> Earthquake B . . . . 0.12 g
> Earthquake C . . . . 0.05 g
> Earthquake D . . . . 0.20 g

In addition to the maximum acceleration, the frequency distribution of earthquake motions is important for evaluating the effect of earthquakes on plant structures and equipment.

Section 3.7, "Seismic Design," of the FSARU describes the seismic design for DCPP. The maximum DCPP vibratory accelerations at the plant site would result from either Earthquake B or Earthquake D-modified postulated earthquakes, depending on the natural period of the vibrating body. Earthquake A and Earthquake C are centered some distance from the plant site with corresponding lower maximum rock acceleration levels; therefore, they are not likely to control. The accelerations for Earthquake B were increased by 25 percent to 0.15 g. This increase provides the required margin of safety to compensate for possible uncertainties in basic earthquake data. Earthquake D-modified is based on the March 1957 San Francisco earthquake with frequency content modified to more closely match Earthquake B. In addition, subsequent studies showed the seismic potential of the Hosgri Fault from which the Hosgri Earthquake is postulated.

DCPP FSARU Figures 2.5-20, 2.5-21, and 2.5-29 through 32 present the response acceleration spectra for free-field ground motion at the plant site from Earthquake B, Earthquake D-modified, and Hosgri Earthquake, respectively. For design purposes, the response spectra for each damping value from Earthquake B and Earthquake D-modified are combined to produce an envelope spectrum. The acceleration for any period on the envelope spectrum is equal to the larger of the two values from the Earthquake B spectrum and the Earthquake D-modified spectrum.

The response acceleration spectra represent rock accelerations for the earthquake events. However, the 16 PPS cabinets are located in the cable spreading room which is at the 128-foot (ft) elevation within the Auxiliary Building. Therefore, response acceleration spectra are needed at the higher elevation where this equipment is located.

Response acceleration spectra for various nodes (corresponding to different locations at different elevations) in the Auxiliary Building are calculated from the acceleration time-histories at the mass points. FSARU Figures 3.7-16 through 3.7-25 and 3.7-21A through 3.7-21I show typical spectra. In addition to these spectra for the Auxiliary Building, maximum absolute accelerations, relative displacements, story shears, overturning moments, and torsional moments are listed in Tables 3.7-12 through 3.7-23. Also, the natural periods for all significant modes of the Auxiliary Building are listed in Tables 3.7-9 through 3.7-11 of the FSARU. The maximum allowed accelerations at the 140-ft elevation for the Design Earthquake are given in Table 3.7-12 with corresponding values for the Hosgri Earthquake in Tables 3.7-17 and 3.7-18.

PPS Seismic Specification Analysis

For establishing the seismic response spectra (i.e., required response spectra), Section 3.1.5.1 of the DCPP Functional Requirements Specification (Reference 126) specifies the following references that include the earthquake response spectra and building displacements:

- DCM C-17 for the Hosgri response spectra,
- DCM C-25 for the Design Earthquake response spectra for structures, systems, and components,
- DCM C-30 for the Double Design Earthquake response spectra for structures, systems, and components, and
- DCM C-28, "Maximum Building Displacements."

The DCM C-30 levels for the Auxiliary Building are identified as twice those given in DCM C-25.

The closest analyzed node within the Auxiliary Building above the 128-ft cable spreading room is Node #2 which is at the 140-ft elevation. Even though this node is at the 140-ft elevation, it would be applicable to the 128-ft cable spreading room because in a typical building structure, the response spectra will be higher at higher elevations. Also, at elevated locations, the horizontal component includes contributions of the horizontal ground motion as well as the torsional response. Response spectra at the 140-ft floor elevation are given in DCM C-25 for the envelope of Earthquake B and Earthquake D modified (also identified as the Design Earthquake) and include:

- N-S Horizontal Spectra Identification Number D-AB-B-NS-140-01-00
- N-S Torsional Spectra Identification Number D-AB-B-TN-140-01-00

- E-W Horizontal Spectra Identification Number D-AB-B-EW-140-01-00

For flexible components, DCM C-25 identifies the vertical acceleration as two-thirds of the horizontal ground response spectra for the envelope of Earthquake D modified and Earthquake B. In addition, for the Double Design Earthquake spectra in the Auxiliary Building, DCM C-30 specifies using Design Earthquake horizontal spectra in DCM C-25 and doubling the values.

DCM C-17 gives the corresponding response spectra for the Hosgri Earthquake and includes information for both the 140-ft and 128-ft elevations. For example, it includes the following spectra in Attachment H:

- Vertical, Slab 5, Node 49 Spectra Identification Number H-AB-N-VR-140-10-03

- Vertical, Slab 5, Node 206 Spectra Identification Number H-AB-N-VR-140-14-03

The information provided in DCM C-17 and DCM C-25 are for the specific node where the analysis was performed. The equipment-specific location spectra are obtained by adding the horizontal acceleration component to the torsional acceleration component multiplied by a distance from the center of mass of the node to the equipment floor location. In addition, it is appropriate to include equipment response to go from the response at the equipment floor location to the response at a specific location in the equipment. The response at a specific location in the equipment is the in-equipment response spectra.

The NRC staff evaluated the response spectra provided in these documents and confirmed the seismic specifications for the 140-ft elevation of the Auxiliary Building [as defined in DCM C-25 response spectra D-AB-B-NS-140-01-00 and D-AB-B-EW-140-01-00] to be consistent with the established FSARU seismic analysis data. The staff also confirmed that the damping values used for these required response spectra meet the criteria of RG 1.61, Revision 1. The NRC staff concludes that compliance with the established PPS seismic specification in Section 3.1.5.1 of the DCPP Functional Requirements Specification as well as supporting documents showing the licensee's in-equipment response spectra development provide reasonable assurance that FSARU analysis conclusions will be supported by the replacement PPS.

PPS Equipment Seismic Qualification

For specifying the design bases for seismic qualification of equipment, Section 3.1.5.2, "Seismic Qualification," of the DCPP Functional Requirements Specification (Reference 126) states that Design Class I PPS equipment and components shall meet the design bases for seismic qualification in accordance with DCM T-10.

Section 4.1e of DCM T-10 states that Design Class I equipment is seismically qualified to perform its nuclear safety function during and after a Double Design Earthquake or the postulated 7.5M Hosgri Earthquake. It refers to DCM T-24 for seismic qualification of plant instrumentation and controls. DCM T-24 has specific qualification requirements for each category of instrument.

Tricon seismic withstand testing was evaluated in Section 3.3.5 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29), and ALS seismic testing was evaluated in Section 3.3.3 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). In addition, during a June 22-26, 2015, NRC audit at Westinghouse facilities (Reference 39), the NRC staff determined the licensee used finite element analysis to qualify the rack enclosures for the PPS subsystems. The licensee developed finite element models for different rack configurations and, using time history analysis, generated the in-equipment response spectra for comparison to the subsystem test response spectra or required response spectra from seismic testing. The following sections summarize the testing and analysis and its applicability to the plant-specific environment.

ALS Subsystem Seismic Qualification

An evaluation of the seismic qualification of the ALS platform components was performed by the NRC staff as part of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The manufacturer's "ALS EQ Plan," Revision 8, 6002-0004, December 2012 (Reference 182), defines its seismic qualification approach and the "ALS Platform EQ Summary Report," Revision 2, 6002-00200, January 2013 (Reference 183), provides a detailed summary of the seismic qualification testing and results. The manufacturer performed seismic type tests at the Westinghouse test facility located in New Stanton, Pennsylvania, between February 7 and February 12, 2012. This testing included baseline verification tests and performance monitoring during seismic conditions. The testing was done in two phases (i.e., Phases A and B). The two different phases represent two different required response spectra. For each phase, the test specimen was subjected to five Operating Basis Earthquake test runs (i.e., OBE-A and OBE-B) and one Safe Shutdown Earthquake test run (i.e., SSE-A and SSE-B). Section 1.2 of the ALS Platform EQ Summary Report states that seismic qualification performed on the ALS platform equipment met the technical requirements of IEEE Std. 344-1987 (Reference 189), as endorsed by RG 1.100, Revision 2, and IEEE Std. 344-2004 (Reference 186), as endorsed by RG 1.100, Revision 3.

The ALS Platform EQ Summary Report provides plots (see Figures 5-110 through 5-115) that indicate the test configuration had several resonances between 40 Hertz (Hz) and 100 Hz. Sample time histories and response spectra were provided for Operating Basis Earthquake and Safe Shutdown Earthquake levels of testing. The data provided show statistical independence based on correlation. In addition, the data show stationarity based on time block power spectral densities of the seismic time histories.

Functional testing identified anomalies during SSE1 and SSE3 test runs at SSE-A test levels (see Table 5-20 of the ALS Platform EQ Summary Report). The first anomaly occurred because one monitoring channel was out of specification during the test run. This anomaly was attributed to connectors on the supporting equipment being pulled tightly when a wire was caught on a wheel of the movable data collection cabinet. The second anomaly occurred because the test sample was not correctly reset from the previous test run. The NRC staff's evaluation concluded that the manufacturer's seismic qualification conforms to the RG 1.100 endorsements of IEEE Std. 344.

Additionally, the NRC staff reviewed the "Advanced Logic System and Line Sense Module Equipment Qualification Summary Report," EQ-QR-120-PGE (Reference 184). This report describes the seismic testing of the LSM conducted at the Westinghouse test facility in New Stanton, Pennsylvania, between October 1 and October 8, 2012. Figure 4-7 of this report shows the Safe Shutdown Earthquake required response spectra, and it is similar to Figure 4-7 in the ALS Platform EQ Summary Report, which was reviewed as part of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30), except it does not include the 10 percent margin. However, the licensee shows the 10 percent margin in its test response spectra versus required response spectra plots included in Section 5.3.2.2, "LSM Test Results" (Reference 184). In these plots, the licensee demonstrated that the test response spectra envelopes the required response spectra except at low frequencies where it determined the criteria of Clause 8.6.3.1 of IEEE Std. 344-2004 were met. The NRC staff determined that based on the information provided in Advanced Logic System and Line Sense Module Equipment Qualification Summary Report, including hardware changes identified in Section 6.2, that the LSM is seismically qualified consistent with the requirements of IEEE Std. 344-2004 endorsed by RG 1.100, Revision 3.

The licensee reviewed Westinghouse Seismic Test Report, EQLR-224B, to show that the DCPP plant-specific seismic requirements are being met for the ALS subsystem. The review states that the test response spectra enveloped the OBE-A/SSE-A and OBE-B/SSE-B required response spectra from a CSI test procedure. However, this review also looked into the demand in-equipment response spectrum of the PPS racks into which the ALS equipment is to be installed. It considered the in-equipment response spectrum for one node at the top of a rack and one at the middle of the rack. It concluded that the OBE-B/SSE-B required response spectra envelop the in-equipment response spectrum over all frequency ranges with ample margin; however, the OBE-A/SSE-A front to back and side to side required response spectra do not completely envelop the demand in-equipment response spectrum.

To confirm the DCPP PPS implementation of the ALS subsystem remains compliant with established seismic criteria, the NRC staff compared the in-equipment response spectrum which was developed based on the seismic response spectra associated with the 140-ft elevation of the Auxiliary Building with the test response spectra attained during ALS seismic qualification tests. The NRC staff determined that IEEE Std. 344-2004 criteria are met and based on the above explained seismic tests and the test results, the ALS subsystem digital PPS components are qualified for use at DCPP.

Tricon Subsystem Seismic Qualification

An evaluation of the seismic qualification of the Tricon platform components was performed by the NRC staff as part of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29). The manufacturer's Master Test Plan defines its seismic qualification approach and the Seismic Test Report provides a summary of the seismic qualification testing and results. The manufacturer performed seismic testing at the National Technical Systems Laboratories in Acton, Massachusetts, between January 16, 2007, and February 16, 2007. This testing was conducted for conformance to IEEE Std. 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Station" (Reference 189), and EPRI technical report TR-107330, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 1, January 1997 (Reference 101).

Five Operating Basis Earthquake tests at the 9.75 g level (Figure 7-1 of the Seismic Test Report) and one Safe Shutdown Earthquake test at the 14 g level (Figure 7-2 of the Seismic Test Report) were conducted on the Tricon test specimen. Test equipment limitations resulted in a reduced test response spectra during the performance of seismic testing. Specifically, in the low-frequency region (i.e., below 6 Hz), limitations of the table velocity and displacement prevented achieving the full EPRI TR-107330 response spectra. The NRC staff evaluation concluded the Tricon V10 equipment is qualified to the limits shown in Figures 3.3.5-1 through 3.3.5-3 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report. Note that Section 8.0 of the Seismic Test Report states that the chassis alarm relays were not seismically qualified as part of seismic testing. The NRC staff determines this is acceptable because the chassis alarm relays are not relied upon in the DCPP PPS to perform a safety function.

To confirm the DCPP PPS implementation of the Tricon subsystem remains compliant with established seismic criteria, the NRC staff compared the in-equipment response spectrum developed based on the seismic response spectra associated with the 140-ft elevation of the Auxiliary Building with the reduced test response spectra attained during Tricon seismic qualification tests. The NRC staff determined the test response spectra enveloped the in-equipment response spectrum and the Tricon subsystem is qualified for use at DCPP.

The licensee submitted a design calculation summary report, "PPS Seismic Qualification" (Reference 176), to evaluate the new PPS cabinet configurations for design basis load conditions. This includes evaluation of the structural adequacy of the existing cabinets as augmented by a new rack support system, and seismic qualification of the new PPS components. The applicable load conditions include Design Earthquake, Double Design Earthquake, and Hosgri Earthquake loads.

The seismic analyses were performed using the SAP2000 computer code which is referenced in of the DCPP Final Safety Analysis Report Update (Section 3.8.2.1.4.6.2 and Table 3.8-6) as a computer program used in current licensing basis static and dynamic analyses. The seismic analyses demonstrates that the seismic equipment qualification for the PPS replacement equipment bounds the plant-specific seismic response for the locations in which the PPS replacement equipment is to be installed for design basis earthquakes.

Four cabinet configurations were considered in the calculations, one for each PPS protection set, because of differences between PPS protection set designs. All four cabinet configurations have the same existing frame structures; however, the licensee will be attaching new rack members to the existing frames in order to improve the seismic performance attributes of the cabinets. This is being done to ensure PPS equipment will meet seismic performance requirements for the installed plant environment.

The design calculation summary report includes a comparison of the required in-equipment response spectra with the test response spectra for both the Tricon and ALS PPS subsystems. Some items required specific analysis, evaluation, or justification. These analyses, evaluations, or justifications were included in an attachment to the report which concluded that these items are qualified for the seismic loads of the design environment of the PPS cabinets. The in-equipment response spectra versus test response spectra comparisons showed that safety-related PPS components are adequate under design basis conditions provided analysis assumptions are verified and recommended cabinet modifications are performed during plant installation of the PPS.

The NRC staff reviewed the seismic calculation and analyses results and determined that design seismic acceleration levels within the PPS cabinets will not exceed the established Tricon or ALS subsystem seismic qualification levels for required frequency ranges. Process protection system equipment will thus not be subjected to seismic acceleration levels beyond the previously established qualification levels for the associated PPS components. The PPS equipment is therefore adequately qualified to meet system performance requirements when subjected to the seismic environments of the plant installation site and is acceptable for use at DCPP.

Conclusion

Because the plant-specific in-equipment response spectrum are enveloped by the test response spectra for both Tricon and ALS (including LSM) subsystems, the NRC staff determined the requirements of IEEE Std. 344-2004 are met and, therefore, the PPS is qualified for the DCPP cable spreading room seismic environment. It is therefore acceptable for the PPS Tricon and ALS subsystem equipment to be installed into the DCPP cable spreading room.

3.5.1.4 Electromagnetic Compatibility

Regulatory Guide (RG) 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” October 2003 (Reference 87), endorses Military Standard MIL-STD-461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment” (Reference 89), and the International Electrotechnical Commission (IEC) 61000 series of electromagnetic interference/radio-frequency interference (EMI/RFI) test methods for the evaluation of safety-related instrumentation and controls (I&C) systems in relation to conducted and radiated EMI/RFI and power surges (Reference 90).

Electric Power Research Institute (EPRI) technical report TR-102323, Revision 2, “Guideline for Electromagnetic Interference Testing in Power Plants,” November 2000 (Reference 191), provides alternatives to performance of site-specific EMI/RFI surveys to qualify digital plant safety I&C equipment in a plant's electromagnetic environment. On April 17, 1996, the NRC issued a safety evaluation for EPRI TR-102323 (Reference 192) and concluded that the recommendations and guidelines in EPRI TR-102323 provide an adequate method for qualifying digital I&C equipment for a plant's electromagnetic environment without the need for plant-specific EMI/RFI surveys if the plant-specific electromagnetic environment is confirmed to be similar to that identified in EPRI TR-102323.

Section 4.3.7 of EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), refers to EPRI TR-102323 levels as part of its EMI/RFI withstand requirements and Section 4.3.8 refers to EPRI TR-102323 as part of electrostatic discharge withstand requirements. The EPRI TR-107330 presents a specification in the form of a set of requirements to be applied to the generic qualification of programmable logic controllers (PLCs) for application and modification to safety-related I&C systems in nuclear power plants. It is intended to provide a qualification envelope corresponding to a mild environment that should meet regulatory acceptance criteria for a wide range of plant-specific safety-related applications. The qualification envelope that is established by compliance with the guidance of EPRI TR-107330 consists of the maximum (i.e., extremes) environmental and service conditions for which qualification was validated and the range of performance characteristics for the PLC platform that were demonstrated under exposure to stress conditions.

Revision 1 of RG 1.180 states in the discussion section that both RG 1.180 and EPRI TR-102323 present acceptable means for demonstrating electromagnetic capability compliance. An applicant has the freedom to choose either document. It should be noted that for some types of testing, the maximum acceptable limits for emissions or susceptibility are different and, therefore, it is possible that tested equipment may meet the requirements of one test, and not meet the requirements of the equivalent test from the other document. RG 1.180 acknowledges this to be acceptable as long as the requirements for a complete suite of EMI/RFI emissions and susceptibility criteria are met with no mixing and matching of test criteria and methods.

Tricon EMI/RFI testing was evaluated in Section 3.3.6 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29) and ALS electromagnetic capability testing was evaluated in Section 3.3.4 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The Tricon and ALS subsystem tests were designed to evaluate conducted and radiated emissions, conducted and radiated susceptibility, surge withstand capability, and electrostatic discharge for test specimen components functioning in a Class 1E application. During testing, Tricon and ALS test specimens were powered, operating, and monitored for performance. Test specimen components included various software and configuration modifications intended to facilitate operational and functional performance monitoring while under test.

System power requirements are provided in Sections 2.4 and 2.6 of the DCPP Interface Requirements Specification (Reference 98). Section 2.1 of the DCPP Interface Requirements

Specification also provides specifications for the input/output power supplies. Alternating current (AC) sources are the same as were used for the Eagle 21 system. The AC distribution diagrams were reviewed by the NRC staff and were determined to be acceptable.

Tricon

Electromagnetic interference/radio-frequency interference (EMI/RFI) testing was performed by National Technical Systems in Boxboro, Massachusetts, in accordance with relevant provisions of EPRI TR-102323, Revision 1, "Guidelines for Electromagnetic Interference Testing in Power Plants," January 1997 (Reference 193); EPRI TR-107330 (Reference 101); and using test procedures and envelopes included in RG 1.180, Revision 1 (Reference 87). The Tricon test specimen consisted of four Tricon chassis populated with selected input, output, communication, and power supply modules. The test specimen also included external termination assemblies provided for connection of field wiring to the Tricon input and output modules. Section 3.3.1 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29) provides additional information on the Tricon test system configuration. The EMI/RFI testing was used to demonstrate the suitability of the Tricon V10 platform for qualification as a safety-related device with respect to radiated and conducted emissions, radiated and conducted susceptibility, surge withstand capability, and electrostatic discharge.

As part of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report, the NRC staff reviewed the EMI/RFI Test Report and determined that the tested Tricon V10 system met the EMI/RFI test acceptance criteria and is qualified up to the tested limits described in the safety evaluation, with exceptions as noted. The NRC staff determined that the Tricon V10 PLC system did not fully meet the guidance of RG 1.180, Revision 1, for conducted emissions, radiated emissions, and susceptibility. The following components being used in the DCPP PPS did not fully comply with the levels defined in RG 1.180:

- 8310 High Density Power Module (120 Volts Alternating Current (VAC)) with respect to conducted emissions under CE101 and CE102 testing,

- Digital Output Module 3601T (115 VAC) in combination with External Termination Panel Model 9663-610N with respect to conducted susceptibility under International Electrotechnical Commission (IEC) 61000-4-6 testing.

In addition, IEC 61000-4-10 radiated susceptibility testing compliance is indeterminate due to test execution anomalies. As a result, the licensee is required to determine that the DCPP-specific EMI/RFI requirements are enveloped by the capabilities of the Tricon V10 system as approved in the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report. The NRC staff's request for additional information (RAI) 71 dated December 23, 2015 (Reference 237), was written to confirm the licensee had met this requirement. In its RAI response dated January 25, 2016 (Reference 20), the licensee provided documentation which identified a final CE102 (high frequency) test performed with a Corcom

Model 30VSK6 line filter installed. With the line filter installed, the MIL-STD-461-E CE102 conducted emissions were acceptable.

ALS

Initial electromagnetic capability qualification tests were performed on representative ALS platform components by Elite Electronic Engineering in Downers Grove, Illinois. Additionally, as a Westinghouse commercially dedicated test service provider, Washington Laboratories, Ltd., performed supplemental electromagnetic capability type tests in New Stanton, Pennsylvania. The ALS test specimen included the seven standardized circuit boards of the platform as well as a backplane and an ALS chassis. The testing included baseline verification tests and performance monitoring during electromagnetic capability conditions (except test specimen performance monitoring was not performed during emissions testing).

The results of these tests were evaluated by the NRC in Section 3.3.4, "Electromagnetic Compatibility Testing," of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The NRC staff determined that the ALS qualification (1) conforms to the RG 1.180 endorsement of MIL-STD-461E suite of tests for radiated and conducted emissions; (2) conforms to the RG 1.180-endorsed IEC suite of tests for radiated and conducted susceptibility as well as surge and electrical fast transient withstand capability; and (3) is consistent with IEC 61000-4-2 for the manufacturer's electrostatic discharge testing and installation limitation.

Additionally, the NRC staff reviewed the Advanced Logic System and Line Sense Module Equipment Qualification Summary Report, EQ-QR-120-PE (Reference 184). This report shows that the Line Sense Module (LSM) was tested for radiated emissions, conducted and radiated susceptibility, surge withstand capability (surge withstand capability), and electrostatic discharge. Three LSM test specimens were tested at the Westinghouse test facility in New Stanton, Pennsylvania between July 7, 2014, and July 21, 2014. The licensee shows its test results in Section 5.1.2.2 of the LSM Equipment Qualification Summary Report and states that the LSM was compliant with applicable safety functions and acceptance criteria during all credited electromagnetic capability tests. Furthermore, the licensee demonstrates radiated emissions compliance by showing its results in Figures 5-7 through 5-11. The NRC staff determined the LSM electromagnetic capability qualification conforms to the RG 1.180 endorsement of MIL-STD-461E and IEC suite of tests for radiated emissions, conducted and radiated susceptibility, surge withstand capability (surge withstand capability), and electrostatic discharge.

3.5.1.4.1 Radiated and Conducted Emissions

The DCPP PPS replacement Functional Requirements Specification (Reference 126) Section 3.1.6.2, "Emissions," states, in part, that "the PPS equipment shall be qualified by test, analysis or a combination thereof, to not create an electromagnetic environment that will adversely affect the operation of safety-related Class 1E equipment operating in the same location (cable spreading room). The qualification shall follow the guidance of Regulatory Guide 1.180...."

The Tricon and ALS test specimens were tested using RG 1.180-endorsed MIL-STD-461E CE101 and CE102 test methods for conducted emissions and RE101 and RE102 test methods for radiated emissions. In addition, the DCPP PPS will be configured with rack power supplies qualified to RG 1.180, Revision 1 and EPRI TR-107330 requirements.

Tricon radiated and conducted emissions testing was evaluated in Section 3.3.6 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29) and ALS radiated and conducted emissions testing was evaluated in Section 3.3.4.1 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The test results and NRC staff's evaluation are summarized in the following sections.

Tricon

The Tricon system 120 VAC chassis power supplies did not fully comply with the allowable equipment emissions levels defined in RG 1.180, Revision 1, for the MIL-STD-461E testing (CE101 and CE102). The frequencies and levels of emissions recorded during these tests are provided below.

MIL-STD-461E, Test Method CE101: Conducted Emissions, 30 Hertz (Hz) to 10 kiloHertz (kHz):

- 120 VAC Chassis Power Supply Line Lead. Conducted emission exceeded at:

  - 179.7 Hz by 11.2 decibel micro Ampere (dBμA)
  - 299.8 Hz by 13.8 dBμA
  - 419.7 Hz by 13.0 dBμA
  - 538.8 Hz by 8.9 dBμA
  - 659.7 Hz by 2.1 dBμA
  - 899.6 Hz by 1.5 dBμA

- 120 VAC Chassis Power Supply Neutral Lead. Conducted emission exceeded at:

  - 179.9 Hz by 11.0 dBμA
  - 299.8 Hz by 14.9 dBμA
  - 419.3 Hz by 13.1 dBμA
  - 539.7 Hz by 9.6 dBμA
  - 659.9 Hz by 2.8 dBμA

MIL-STD-461E, Test Method CE102: Conducted Emissions, 10 kHz to 2 MegaHertz (MHz):

- 120 VAC Chassis Power Supply Line Lead. Conducted emissions exceeded at:
  - 50.0 kHz by 1.5 dBμA

Note: The Tricon system 230 VAC Chassis Power Supply modules were also noncompliant with the allowable equipment emissions levels defined in RG 1.180, Revision 1, for MIL-STD-461E, CE101; however, these modules are not being used in the PPS replacement; therefore, the emission levels for these modules are not relevant to this modification.

To address the excessive emission levels of the 120 VAC chassis power supply modules, the licensee is including a Corcom Model 30VSK6 line filter on the input of the 120 VAC power supply for the PPS replacement design. With use of the Corcom Model 30VSK6 line filter on the input of the 120 VAC power supply, the high frequency conducted emissions meets the guidance of RG 1.180.

ALS

The ALS platform was tested to the MIL-STD-461E series of tests endorsed by RG 1.180. This includes compliance with CE101, CE102, RE101, and RE102 test methods. As part of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30), the NRC staff reviewed the ALS EQ Plan (Reference 182) and the ALS Platform EQ Summary Report (Reference 183), and determined that the manufacturer's electromagnetic capability emissions qualification conforms to the RG 1.180 endorsement of MIL-STD-461E. Because CE101 testing was exempted based on power quality being maintained and a measurement of total harmonic distortion, by letter dated January 25, 2016 (Reference 20), in response to request for additional information (RAI 71) dated December 23, 2015 (Reference 237), the licensee confirmed that power quality would be maintained and the PPS replacement would meet the requirements for exemption to CE101 testing.

For the LSM, the NRC staff reviewed Advanced Logic System and Line Sense Module Equipment Qualification Summary Report (Reference 184) and, based on the results in Section 5.1.2.2, including the radiated emissions plots in Figures 5-7 through 5-11, determined that the manufacturer's radiated emissions qualification conforms to the RG 1.180 endorsement of MIL-STD-461E.

3.5.1.4.2 Radiated and Conducted Susceptibility

The DCPP PPS Functional Requirements Specification (Reference 126) Section 3.1.6.1, "Susceptibility" states, "[t]he PPS shall be qualified by test, analysis, or a combination thereof, to function without fault or error in an electromagnetic environment in accordance with the guidance of Regulatory Guide 1.180…."

Both Tricon and ALS test specimens were subjected to the International Electrotechnical Commission (IEC) suite of tests. Tricon radiated and conducted susceptibility testing was evaluated in Section 3.3.6 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29) and ALS radiated and conducted susceptibility testing was evaluated in Section 3.3.4.2 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The test results and NRC staff's evaluation are summarized in the following sections.

Tricon

The following Tricon test specimen discrete and analog input/output hardware, does not fully comply with the minimum susceptibility thresholds required by RG 1.180, Revision 1, for the following electromagnetic interference/radio-frequency interference (EMI/RFI) susceptibility tests:

IEC 61000-4-3 Testing: Radiated Susceptibility, 26 MHz to 1 gigaHertz (GHz):

- Resistance temperature detector (RTD) Signal Conditioning Module 1600083-600 [3]
- RTD Signal Conditioning Module 1600083-200 [3]
- RTD Signal Conditioning Module 1600024-030 [3]
- RTD Signal Conditioning Module 1600024-020 [3]

IEC 61000-4-6 Testing: Conducted Susceptibility, 150 kHz to 80 MHz:

- RTD Signal Conditioning Module 1600081-001 [3]
- Digital Output Module 3601T (115 VAC) with External Termination Panel (ETP) 9663-610N

IEC 61000-4-10 Testing: Radiated Susceptibility, Damped Oscillatory Magnetic Field:

- Due to test execution anomalies, the results of this testing were determined not to be valid. Therefore, compliance with IEC 61000-4-10 is indeterminate.

The 120 VAC power to the Tricon is to be supplied by Class 1E vital instrument power with appropriate quality requirements and design practices in place. Based on testing performed for another similar application at DCPP (power supplies located in a Tricon chassis located in safety-related Auxiliary Building and fuel handling ventilation control system cabinets), no appreciable difference in the harmonic distortion of the instrument alternating current (AC) system was observed before and after the power supplies were installed. Therefore, the RG 1.180 criteria for exemption from CE101 testing are met for the PPS replacement Tricon equipment.

[3] The NRC staff notes that RTD Signal Conditioning modules are not being used in the DCPP PPS application; therefore, the susceptibility levels for these modules are not relevant to this modification.

The NRC staff determined that the plant-specific EMI requirements are enveloped by the capabilities of the 3601T Tricon digital output modules used in the DCPP PPS application. Though these modules showed susceptibility to conducted EMI/RFI at a certain frequency range and amplitude in the form of spurious changes of state during qualification testing, the plant environment is not expected to exceed the levels at which these modules were successfully tested. A plant EMI/RFI survey was performed at the installation site to confirm compatibility of the PPS to this environment. The results of this test did not identify significant EMI or RFI interference levels at the susceptible frequencies.

ALS

The ALS test specimen was tested in accordance with the IEC suite of tests endorsed by RG 1.180. In addition, it was tested for radiated susceptibility above 1 gigahertz (GHz) in accordance with the MIL-STD-461E RS103 test method. As part of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30), the NRC staff reviewed the manufacturer's ALS EQ Plan (Reference 182) and ALS Platform EQ Summary Report (Reference 183) and determined that the manufacturer's electromagnetic capability susceptibility qualification conforms to the RG 1.180-endorsed IEC suite of tests. Note that Section 7.2 of the Advanced Logic System and Line Sense Module Equipment Qualification Summary Report (Reference 184) specifies installation limitations that must be followed to maintain the qualified use of the equipment. For the safety power supply, Section 7.2 states (i.e., Installation Limitation C) that:

> Safety Power Supply - A safety-related power supply must be present in the installation to provide protection to the ALS hardware on the power lines. This power supply must meet the requirements of U.S. NRC Regulatory Guide 1.180 ... for medium exposure for [electromagnetic capability], the technical requirements of IEEE Std 344-2004 ... as endorsed by U.S. NRC Regulatory Guide 1.100 ... for seismic qualification, and the technical requirements of IEEE Std 323-2003 ... as endorsed by U.S. NRC Regulatory Guide 1.209....
>
> [Clarification - Qualification of the 48 VDC chassis power supplies, 48 VDC wetting power supplies, and the 24 VDC loop power supplies that support the ALS and LSM equipment are PG&E scope.]

The design of safety power supplies for the ALS subsystem are part of the licensee's scope of this modification and were therefore not included in the vendor-supplied PPS equipment. At the time of this evaluation, the licensee was performing preliminary design activities for the PPS power distribution system. During the regulatory audit performed on June 22-26, 2015, (Reference 39), the NRC staff reviewed this design and the power supply specifications identified in the PPS Interface Requirements Specification (IRS) (Reference 98), Section 2.4, "System Power Requirements." The IRS includes a requirement for power filters to reduce the conducted noise to acceptable levels in accordance with RG 1.180 criteria. The staff confirmed these filters were being included in the design of the PPS power distribution system.

Additionally, the IRS includes specification 2.6.2, "Harmonic Distortion Limitations," which requires measurements of total harmonic distortion to be made before and after installation of PPS equipment.

For the LSM, the licensee shows in Table 5-3 of the Advanced Logic System and Line Sense Module Equipment Qualification Summary Report that it performed the RG 1.180-endorsed IEC suite of tests for radiated and conducted susceptibility. The LSM test results show it is compliant in accordance with Performance Criterion A. In addition, during the June 22-26, 2015, audit at Westinghouse facilities, the NRC staff performed a confirmatory review of radiated susceptibility testing on the LSM. The NRC staff confirmed the testing was performed in accordance with IEC 61000-4-3 and satisfied the requirements of that standard.

3.5.1.4.3 Surge and Electrical Fast Transient

Both Tricon and ALS test specimens were subjected to the IEC suite of tests. Tricon electrical fast transient testing was evaluated in Section 3.3.6 and surge withstand testing in Section 3.3.7 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29). ALS surge withstand testing and electrical fast transient testing were evaluated in Section 3.3.4.3 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The NRC staff's evaluations are summarized in the following sections.

Tricon

The Tricon test specimen was tested on power leads and signal leads using the IEC 61000-4-4 test method. As part of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report, the NRC staff reviewed the Electrical Fast Transient Test Report and determined that the Tricon V10 exhibits acceptable performance against electrical fast transients as addressed in RG 1.180, Revision 1.

The Tricon test specimen power supplies and signal lines were tested using IEC 61000-4-5 and IEC 61000-4-12 test methods. As part of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report, the NRC staff reviewed the Surge Withstand Test Report and determined that the Tricon V10 meets the surge withstand performance criteria in EPRI TR-107330, EPRI TR-102323, Revision 1, and RG 1.180, Revision 1.

ALS

The ALS test specimen was tested in accordance with the IEC suite of tests endorsed by RG 1.180. As part of the ALS platform safety evaluation for the Advanced Logic System Topical Report, the NRC staff reviewed the ALS EQ Plan (Reference 182), and the ALS Platform EQ Summary Report (Reference 183) and determined that the manufacturer's electromagnetic capability surge and electrical fast transient qualification conforms to the RG 1.180-endorsed IEC suite of tests.

For the LSM, the licensee shows in Table 5-3 of Advanced Logic System and Line Sense Module Equipment Qualification Summary Report (Reference 184) that it performed the RG 1.180-endorsed IEC suite of tests for surge and electrical fast transient testing. The LSM test results show it is compliant in accordance with Performance Criterion A.

3.5.1.4.4 Electrostatic Discharge

Both Tricon and ALS test specimens were subjected to IEC 61000-4-2 testing. Tricon electrostatic discharge testing was evaluated in Section 3.3.8 of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report (Reference 29) and ALS electrostatic discharge withstand testing was evaluated in Section 3.3.4.4 of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30). The NRC staff's evaluations are summarized in the following sections.

Tricon

As part of the Tricon V10 platform safety evaluation for the Triconex Approved Topical Report, the NRC staff reviewed the Electrostatic Discharge Test Report and determined that the Tricon V10 met the EPRI TR-107330, Section 4.3.8, and EPRI TR-102323, Revision 1, criteria for electrostatic discharge performance.

ALS

As part of the ALS platform safety evaluation for the Advanced Logic System Topical Report, the NRC staff reviewed the ALS EQ Plan (Reference 182) and the ALS Platform EQ Summary Report (Reference 183) and determined the manufacturer's electrostatic discharge testing and installation limitation are consistent with the RG 1.180 reference to IEC 61000-4-2. In addition, inspection item 3 included in Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation includes verifying electrostatic discharge precautions are being used during equipment installation.

For the LSM, the licensee shows in Table 5-3 of Advanced Logic System and Line Sense Module Equipment Qualification Summary Report (Reference 184) that it performed IEC 61000-4-2 electrostatic discharge testing. The LSM test results show it is compliant in accordance with Performance Criterion A.

Conclusion

Because the plant-specific electromagnetic capability environment is enveloped by the electromagnetic capability testing for both Tricon and ALS (including LSM) subsystems and the licensee has demonstrated its compliance with power quality and installation limitations, the NRC staff determines the PPS is qualified for the DCPP cable spreading room consistent with the guidance in RG 1.180. It is therefore acceptable for the PPS Tricon and ALS subsystem equipment to be installed into the DCPP cable spreading room.

3.5.2 Power Quality

The replacement PPS uses the same electrical power sources as the Eagle 21 PPS. Each PPS replacement protection set is powered from a separate 120 Volts alternating current (VAC) vital bus via a Class 1E uninterruptible power supply. Each of these 120 VAC vital buses is supplied from two different power sources: a 480 VAC motor control center and a 125 Volt (V) vital direct current (DC) bus.

Safety-related 480 VAC from vital AC motor control center is fed to the uninterruptible power supply where power is rectified and converted to 120 VAC.

Safety-related vital DC bus power is fed to uninterruptible power supply as immediate backup supply. The vital DC bus is backed up by the safety-related 125 VDC station battery, which is charged from vital 480 VAC. Inverter output is fed through a static switch with integral manual bypass switch to vital instrument AC power distribution panels.

See Section 3.9.5.1, "IEEE 603-1991, Clause 8.1, Electrical Power Sources," of this safety evaluation for evaluation of PPS electrical power sources to IEEE 603 criteria.

3.6 Defense-in-Depth and Diversity

Paragraph 10 CFR 50.55a(h), "Protection and safety systems," states that protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32), and the correction sheet dated January 30, 1995. Clause 5.1, of IEEE Std. 603-1991, requires, in part, that "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…."

Section 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," requires, in part, various diverse methods of responding to ATWS.

Criterion 12, 1967, "Instrumentation and Control Systems," of the DCPP FSARU, requires that "Instrumentation and controls shall be provided as required to monitor and maintain variables within prescribed operating ranges."

Criterion 14, 1967, "Core Protection Systems," of the DCPP FSARU requires that "Core protection systems, together with associated equipment, shall be designed to act automatically to prevent or to suppress conditions that could result in exceeding acceptable fuel damage limits."

Criterion 15, 1967, "Engineered Safety Features Protection Systems," of the DCPP FSARU requires that "Protection systems shall be provided for sensing accident situations and initiating the operation of necessary engineered safety features."

Criterion 19, 1967, "Protection Systems Reliability," of the DCPP FSARU requires that "Protection systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed."

Criterion 20, 1967, "Protection systems redundancy and independence," of the DCPP FSARU requires that "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."

Criterion 21, 1967, "Single Failure Definition," of the DCPP FSARU requires that "Multiple failures resulting from a single event shall be treated as a single failure."

Criterion 22, 1967, "Separation of Protection and Control Instrumentation Systems," of the DCPP FSARU requires that "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."

Criterion 23, 1967, "Protection Against Multiple Disability of Protection Systems," of the DCPP FSARU requires that "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."

Criterion 26, 1967, "Protection Systems Fail-Safe Design," of the DCPP FSARU requires that "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."

RG 1.53, Revision 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," November 2003 (Reference 60), clarifies the application of the single-failure criterion and endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 61). Clause 5.5, "Common-cause failures," of IEEE Std. 379-2000, identifies diversity and defense-in-depth (D3) as a technique for addressing common-cause failures, and Clause 6.1, "Procedure," identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems"

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-19, Revision 6 (Reference 49), provides the NRC staff position and guidance for the diversity and defense-in-depth (D3) evaluation to address the concern regarding common-cause failure (CCF) vulnerabilities with regard to the use of digital computer-based instrumentation and control (I&C) systems.

For operating reactors, BTP 7-19 specifies that licensees address the following points:

- Point 1 - The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.

- Point 2 - In performing the assessment, the vendor or applicant shall analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

- Point 3 - If a postulated common-cause failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

- Point 4 - A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.

If a postulated CCF could disable a safety system, then a diverse means that may be a non-safety system of sufficient quality but not be subject to the same CCF should be required to perform either the same function or a different function.

Section 3 of BTP 7-19 specifies the acceptance criteria regarding the radiological consequences and the integrity of the reactor coolant pressure boundary and containment for the best-estimate analysis of plant response to the design basis events occurring in conjunction with each single postulated CCF. If a CCF results in a plant response that requires reactor trip and/or engineer safety features actuation, then a diverse means that is not subject to or failed by the postulated failure should be provided to perform the reactor trip and/or engineered safety features function.

The Staff Requirements Memorandum on "SECY-93-087 – Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993 (Reference 194), describes the NRC's position regarding D3. Guidance on the evaluation of D3 is provided in BTP 7-19. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994 (Reference 195), summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

Evaluation

While the NRC considers CCFs in digital systems to be beyond design basis, the digital safety systems should be protected against CCFs. The licensee or applicant should perform a D3 analysis to demonstrate that vulnerabilities to CCFs are adequately addressed.

The licensee completed a D3 analysis in accordance with NUREG/CR-6303 and BTP 7-19 (Reference 97).

The DCPP D3 analysis was performed with the assumption that all safety functions performed by the Tricon portion of the process protection system (PPS) could become disabled to a software CCF. The licensee used realistic assumptions to perform best-estimate analyses of licensing basis plant responses. The licensee identified necessary back-up systems as well as manual operator actions necessary for accomplishing required safety functions. For the DCPP PPS, diverse means of performing safety functions associated with the reactor coolant flow, pressurizer pressure, and containment pressure instruments are provided by a second diverse Advanced Logic System (ALS) core logic implementation. Both of the ALS core logic implementations within each PPS protection set are safety-related and are qualified to perform safety functions under associated event conditions.

The NRC staff performed a safety evaluation review of the DCPP D3 assessment for the PPS upgrade. The details of this review can be found in the safety evaluation dated April 19, 2011 (Reference 196), for the DCPP D3 assessment of the PPS. This safety evaluation concluded the D3 assessment performed was consistent with the guidance of BTP 7-19 with the assumption that a software common-cause failure would result in total failure of the Tricon portion of the PPS. The NRC staff determined that there is adequate diversity within the plant design that the plant responses to design basis events concurrent with potential software CCF of the PPS meet the acceptance criteria specified in BTP 7-19.

3.6.1 ALS System Diversity

The Advanced Logic System Topical Report (Reference 30) identifies intended applications of the ALS platform in various diversity configurations to support different nuclear power plant systems, including a digital reactor trip system (RTS) and the engineered safety features actuation system (ESFAS). The Advanced Logic System Topical Report clarifies certain ALS platform design attributes, which have been specifically constructed to mitigate the likelihood of software common-cause failures, provide a foundation that licensees may use in their D3 analysis to construct reliable safety systems. These design attributes are intended to justify the elimination of a diverse actuation system for some plant-applications. The topical report references the "ALS Diversity Analysis," 6002-00031, Revision 2, January 2013 (Reference 141), which provides an overview of key design attributes for the ALS platform needed to eliminate the consideration of CCF.

The DCPP ALS subsystem of the PPS includes the following design features;

- Two separate ALS chassis within each PPS protection set.
- Independently developed application core logic within each of the two ALS-102 core logic boards in each protection set.
- Independently developed input/output board core logic configurations for each of the two ALS chassis within each protection set.
- Two different core logic implementations within each core logic board.

The following figure illustrates how these design features are incorporated into the PPS ALS subsystem:

[[

]]

Figure 3.6.1-1. DCPP ALS Core Diversity Design

The NRC staff evaluated the ability of ALS platform design and process attributes to either preclude or limit logic implementation related CCFs. Section 9, "Diversity," of the Advanced Logic System Topical Report identifies two design attributes, which are intended to mitigate the likelihood of common-cause programming failures as sources that could disable a safety function. The topical report refers to these two attributes as Core Diversity and Embedded Design Diversity.

Core Diversity as implemented in the DCPP PPS application generates two redundant logic implementations for placement within each field programmable gate array (FPGA) for each standardized circuit board. The two redundant logic implementations (represented as the relation between Core A1 and Core A2 and between Core B1 and B2 in Figure 2) use the same hardware descriptive language files per standardized circuit board. However, each logic implementation is produced using different synthesis directives. Therefore the synthesis tool is used as a means of making the core logic in the #1 implementations different than the core logic in the #2 implementations.

Embedded Design Diversity provides an additional level of diversity to that provided by Core Diversity. **[[**

]] The DCPP application defines the configuration and arrangement of the PPS and creates two different sets of FPGA design variants.

[[

]]

Figure 3.6.1-2. DCPP ALS Core Diversity Implementation Processes

The NRC staff compared the ALS platform approach for the DCPP PPS to the Strategy D diversity approach described in NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," February 2010 (Reference 197). The PPS approach is characterized by use of the same technology (e.g., the same platform and logic device) for the diverse components being compared. In a Strategy D classification, the principal feature characterizing the strategy is that basic components (e.g., hardware parts, software blocks, system architectural structure, etc.) of diverse systems are the same.

The PPS approach differs from Strategy D in that different "software blocks" (i.e., FPGA programs) exist because of the Embedded Design Diversity used for the primary and diverse actuation system. For the DCPP PPS, one set of FPGA design variants performs the safety function (Core A) while an alternative set of design variants provides the identical diverse actuation (Core B).

The NRC staff determined the ALS platform provides lifecycle diversity that produces differences in susceptibility to CCF sources with respect to personnel cognition and resultant human actions. Additional diversity is provided by the use of different tools between the implementation and test teams.

3.6.2 Diversity between ALS and Tricon Subsystems

A comparison between the Tricon and ALS platforms was made by the NRC staff. The following characteristics were evaluated with the results shown:

- The design architectures of the Tricon and ALS subsystems are completely different.
- The ALS subsystem uses FPGA technology while the Tricon uses microprocessor technology.
- The ALS platform components are produced by different manufacturers than components used in the Tricon subsystem.
- The ALS subsystem initiation paths are separate and independent from the Tricon subsystem safety functions which are subject to a software CCF.
- The PPS sensors are not digital devices and are not subject to the effects of a software CCF.
- The ALS system does not share the same sensors used for the Tricon subsystem with the exception of reactor coolant system (RCS) temperature elements and the pressurizer pressure signal.
- All PPS RCS temperature signals are processed through the ALS subsystem prior to being sent to the Tricon subsystem for over power delta temperature (OPDT) and over temperature delta temperature (OTDT) processing. This dependency of the Tricon safety functions on the ALS subsystem is accounted for in the D3 analysis and in the PPS time response analysis. A PPS software CCF is assumed to render these functions inoperable.
- The pressurizer pressure signals are used by the Tricon subsystem for calculation of OPDT and OTDT trip setpoints. These signals are shared at the transmitter analog output and are isolated to meet diversity requirements.

The NRC staff determined that the ALS and Tricon subsystems of the PPS are sufficiently independent and diverse from each other such that any failure of either subsystem will not result in a condition that is not accounted for in the plants accident analysis.

3.6.3 Manual Operator Actions

Manual operator actions may be credited for responding to events in which the protective action could be subject to a common-cause failure (CCF). A licensee or applicant should provide sufficient information and controls (safety or non-safety) in the main control room that are independent and diverse from the protection system (i.e., not subject to the CCF).

For the Eagle 21-based PPS, the following events require manual operator actions for event mitigation following a design-basis accident when a software CCF of the PPS occurs.

- Loss of forced reactor coolant flow in a single loop above the P8 permissive.
- Accidental RCS depressurization, including steam generator tube rupture, steam line break, and loss-of-coolant accident indicated by low pressurizer pressure.
- Large break loss-of-coolant accident and steam line break indicated by high containment pressure.

Because the Tricon/ALS-based DCPP PPS allocates RCS flow, pressurizer pressure and containment pressure functions to the ALS subsystem, this PPS upgrade will eliminate the need for manual operator actions to be credited in the analysis for mitigation of the events following a design-basis accident when a software CCF within the PPS occurs. The ALS system is designed to maintain its safety functionality during a software CCF due to its use of redundant cores.

Though these manual operator actions are no longer required to be performed for mitigation of events associated with software CCF, they will remain functional when a software CCF within the PPS occurs. The licensee demonstrated that sufficient indications and controls that are independent and diverse from the PPS are being maintained in the main control room to ensure that operators will be provided with the information needed to satisfactorily perform manual operator actions in the event of a software CCF.

The modified PPS design is retaining means in the control room to perform manual initiation of automatically initiated protective actions at the division level. The means provided in the DCPP design minimizes the number of discrete operator manipulations and depends on the operation of a minimum of equipment. Based on this information, the NRC staff determined that the proposed modification to the DCPP PPS complies with this position and is therefore acceptable.

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-19 (Reference 46) states that a set of displays and controls (safety or non-safety) should be provided in the main control room for manual system level actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the reactor protection system. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same CCF that necessitated the diverse backup system; one example would be the use of hard-wired connections."

The DCPP safety system design provides a set of displays and controls in the main control room to support manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal, reactor coolant system integrity, and containment isolation and integrity. Manual controls associated with equipment that is actuated by the PPS are not directly interfaced with the PPS and are not being modified by this PPS upgrade. Instead, these controls provide input to the existing solid state protection system and will not be impacted by the PPS upgrade.

These displays and controls which will be used to support manual operator actions as described above are unaffected by the software CCF of the DCPP PPS. The NRC staff determined that the licensee has maintained sufficient instrumentation and controls that are not subject to the software CCF of the DCPP PPS to support the manual operator actions that would be available for response to a software CCF event.

3.6.4 Effects of Common-Cause Failure

Many possible types of protection system failures may occur as a result of failure to actuate. Among these, a simple failure of the total system might not be the worst-case failure, particularly, when analyzing the time required for identifying and responding to the condition. For this reason, the evaluation of failure modes as a result of software common-cause failure (CCF) should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate.

A failure or fault that is detected can be addressed; however, failures that are non-detectable may prevent a system actuation when required. Consequently, non-detectable faults are of concern.

The system failure modes that were considered for the DCPP PPS are listed in the failure modes and effects analyses. See Section 3.2.2.7 for the evaluation of failure modes and effects analyses (FMEAs) associated with the PPS. These FMEAs did consider failure modes that could result in a failure of the PPS to actuate when required as well as failure modes that would result in a partial actuation of the PPS. The FMEAs identified all of the indications that would be available to the operators for these failures, as well as, a list of failures that would be undetected. The DCPP PPS design includes diverse means of providing required safety functions in the event of a PPS software CCF. Based on this information, the NRC staff determined that the proposed modification to the DCPP PPS is acceptable.

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-19 (Reference 46) states that there are two design attributes that are sufficient to eliminate consideration of CCF—diversity and testability.

1. Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

2. Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100 percent tested).

The NRC staff determined that the Tricon portion of the DCPP PPS did not contain a sufficient amount of diversity to meet criteria 1 above. The NRC staff also determined that the Tricon subsystem complexity is such that the criteria 2 above cannot be satisfied. As a result of these determinations, the consideration of software CCFs could not be eliminated for the proposed Tricon portion of the PPS. Therefore, the licensee performed a diversity and defense-in-depth (D3) assessment (Reference 97) assuming that all safety functions associated with or relying upon Tricon system operation would fail to actuate.

The NRC staff determined that the ALS portion of the DCPP PPS did contain a sufficient amount of diversity to meet criterion 1 above. As a result of this determination, the consideration of software CCFs could be eliminated for the proposed ALS portion of the PPS. Therefore, the D3 assessment performed by the licensee did not assume any loss of safety functionality associated with the ALS system operation. The results of this assessment were evaluated by the NRC and are documented in a safety evaluation dated April 19, 2011 (Reference 196). This safety evaluation concludes that the D3 assessment performed was consistent with the guidance of BTP 7-19.

The NRC staff has established acceptance guidelines for D3 assessments and has identified four echelons of defense against CCFs, which are:

- Control system - The control system echelon consists of non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

- Reactor Trip System (RTS) - The reactor trip echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- Engineered Safety Feature Actuation System (ESFAS) - The ESFAS echelon consists of safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).

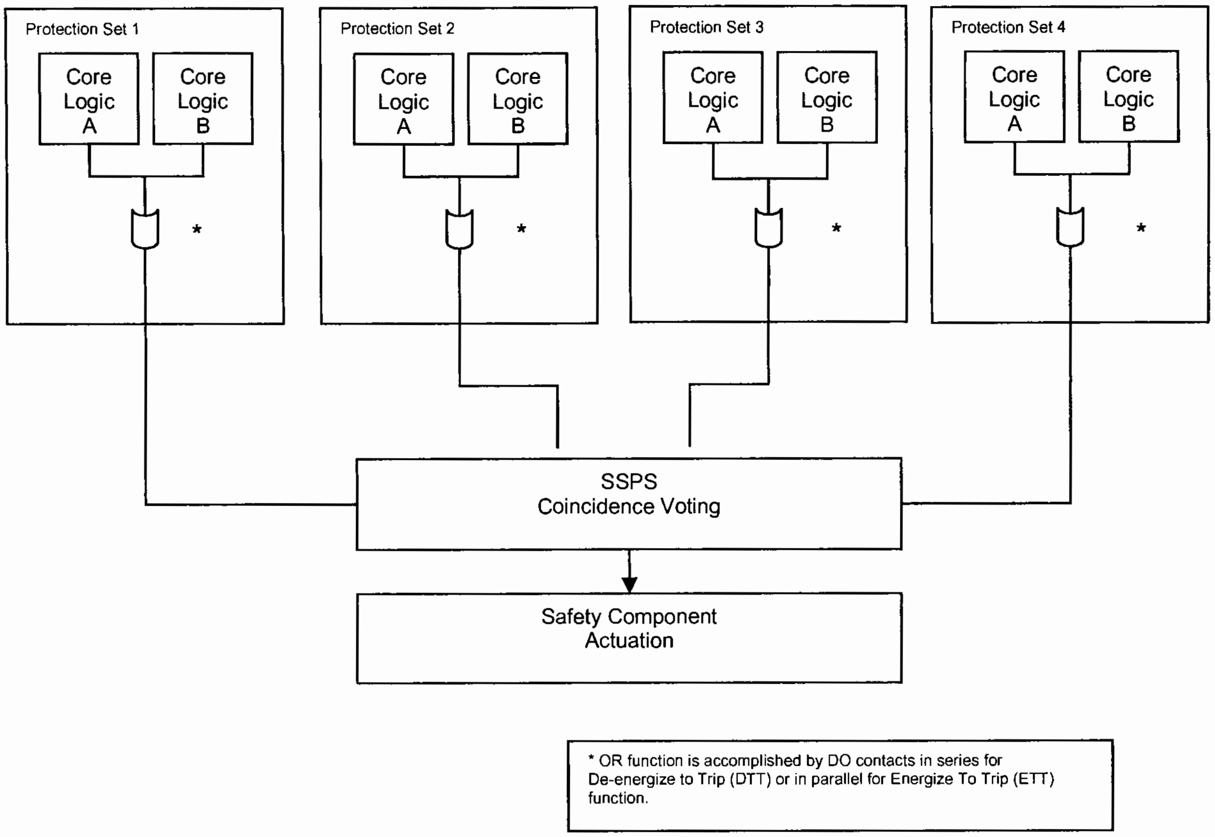
- Monitoring and Indication - The monitoring and indication echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

The DCPP PPS design integrates reactor-trip functions of the RPS with engineered safety features actuation functions of the ESFAS and therefore combines the middle two echelons of defense (RTS and ESFAS described above), into a common system. It was, therefore, necessary to evaluate the effects of a software CCF with the understanding that both of these layers of defense could be compromised during a software CCF event. The NRC staff confirmed that the D3 analysis accounted for the effects of PPS failures on both the RPS and ESFAS related functions of the system. Based on this information, the NRC staff determined that the proposed modification to the DCPP PPS complies with BTP 7-19 criteria for addressing the echelons of defense and is therefore acceptable.

If a postulated digital system CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is not subject to the same CCF, should be included in the overall system design. This diverse means should perform either the same function or a different function that will mitigate accidents or events that require the safety function assumed failed by the postulated CCF.

The NRC staff determined that a software CCF within the DCPP PPS could disable one or more safety functions of the system. The system design does include diverse means of accomplishing the digital systems safety functions associated with reactor coolant system flow, pressurizer pressure, and containment pressure. These diverse measures are performed by the diverse ALS core logic implementation which is included as a subsystem of the PPS.

Both of the diverse core logic implementations are designed to perform identical safety functions for each of the four PPS protection sets (see Figure 3.6.4-1 below). The actuation signals of the two ALS core logic boards are configured to ensure safety function operation even when one of the core logic boards fails as a result of a logic-based CCF failure. The opposite core logic board for each protection set is sufficiently diverse such that any logic fault in one of the cores would be limited to only that set of ALS boards (in all four protection sets) which share that specific core logic implementation. The DCPP PPS design does include a basis for these diverse measures.



* OR function is accomplished by DO contacts in series for De-energize to Trip (DTT) or in parallel for Energize To Trip (ETT) function.

Figure 3.6.4-1. ALS Diverse Core Logic Architecture

<u>Reference ALS Platform Topical Report D3 Evaluation Applicability</u>

An evaluation of a D3 methodology was documented in the Advanced Logic System Topical Report safety evaluation (Reference 30). This evaluation discusses the diversity features available for the ALS platform.

When compared to the existing licensed Eagle 21 PPS, the replacement PPS reduces reliance on manual operator actions associated with containment pressure, pressurizer pressure, and RCS flow. The modified system also retains the capability for operators to take manual actions so even though the likelihood of losing safety functionality of these parameters is less than it was for the Eagle 21 system, it is still considered in the plant's D3 best-estimate analysis.

3.6.5 Anticipated Transient without Scram Diversity Considerations

The anticipated transient without scram (ATWS) mitigation systems are required for compliance with 10 CFR 50.62. As defined in 10 CFR 50.62, an ATWS event is an anticipated operational occurrence followed by failure of the reactor trip portion of the protection system, and

10 CFR 50.62 identifies design requirements for ATWS mitigation systems and equipment. NUREG-0800 Standard Review Plan (SRP) Section 7.8, Revision 5, "Diverse Instrumentation and Control Systems," March 2007 (Reference 239), contains SRP acceptance criteria for diverse actuation systems.

Diablo Canyon Power Plant (DCPP) uses an ATWS mitigating system actuation circuitry (AMSAC) system to address ATWS regulatory requirements. The AMSAC system is described in Sections 7.6.1.4 and 7.6.2.4 of the DCPP Final Safety Analysis Report Update (FSARU) (Reference 52). The AMSAC system is independent and diverse from the reactor protection system (RPS) including the PPS portion of RPS. The AMSAC system trips the main turbine, starts auxiliary feedwater, and isolates steam generator blowdown on coincidence of low-low steam generator water level in three out of four steam generators.

The DCPP PPS license amendment request does not modify the existing AMSAC system; therefore, no review or evaluation of the AMSAC is required. However, a principal SRP acceptance criterion for the DCPP PPS is the diversity (i.e., independence from CCF) of the AMSAC system from the PPS. Figure 3.6.5-1 below represents the AMSAC system in relation to the digital PPS and shows how functional independence between these systems is established.

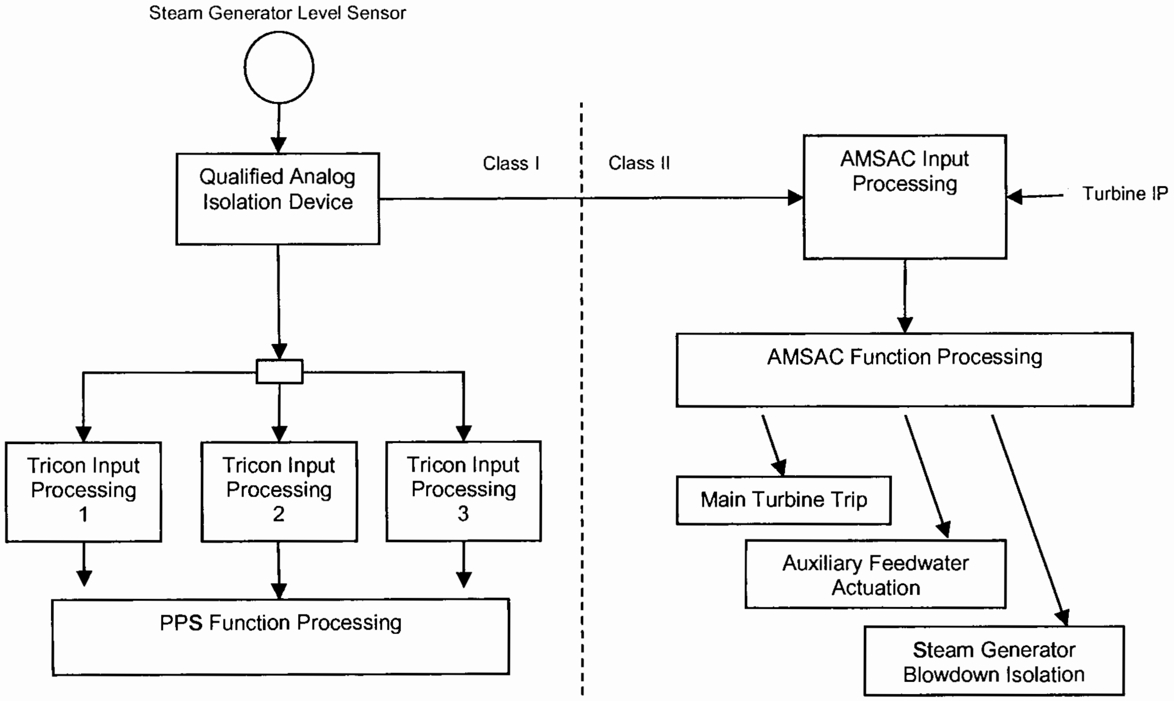

Steam Generator Level Sensor
Qualified Analog Isolation Device
Class I
Class II
AMSAC Input Processing
Turbine IP
AMSAC Function Processing
Tricon Input Processing 1
Tricon Input Processing 2
Tricon Input Processing 3
PPS Function Processing
Main Turbine Trip
Auxiliary Feedwater Actuation
Steam Generator Blowdown Isolation

Figure 3.6.5-1. AMSAC Interface

The steam generator level signals that are used for AMSAC actuation are derived from the same sensors that provide input to the Tricon PPS subsystem; however, these signals are provided to AMSAC through qualified analog isolation devices. The NRC staff confirmed through review of the Interface Requirements Specification for the DCPP PPS (Reference 98) that the steam generator level input signals used for AMSAC actuation are independent and isolated from the PPS. Because AMSAC does not rely on any processing functions performed by the Tricon subsystem, a failure of the Tricon subsystem would not affect the AMSAC functionality. Conversely, because the steam generator level signals to Tricon and to AMSAC are isolated from each other, a failure of the AMSAC system would not affect the safety functionality of the Tricon subsystem.

A comparison between the Tricon and ALS platforms and the platform on which the AMSAC system was developed was made by the NRC staff. The following characteristics were evaluated with the results shown:

- The design architectures are completely different.
- The AMSAC system is based on digital technology of a different vendor than either of the two PPS subsystem suppliers.
- The AMSAC system uses different microprocessors which are produced by different manufacturers than those used in the Tricon subsystem.
- The diverse AMSAC system is powered by a non-safety-related source.
- The quality of components in the AMSAC system is based on selection of known process electrical components that have proven reliability.
- The diverse AMSAC system initiation path is separate and independent from the Tricon PPS processors which are subject to a software CCF.
- The diverse AMSAC system initiation path is separate and independent from the ALS PPS core logic boards.
- Though the AMSAC system shares the same steam generator level sensors used for the PPS, these sensors are not digital devices and are not subject to the effects of a software CCF.
- The AMSAC output actuation signals are transmitted through relays that provide isolation between the safety-related control circuits actuated by AMSAC and the non-safety-related AMSAC system.

The licensee evaluated the PPS as part of the D3 assessment to confirm that diversity is maintained between it and the existing diverse AMSAC actuation system. The AMSAC system and the ALS portion of the PPS are provided by equipment that is not affected by the postulated software CCF within the PPS. The automatic diverse AMSAC actuation system is sufficient to maintain plant conditions within the BTP 7-19 criteria for all anticipated operational occurrences and design-basis accidents.

The NRC staff concludes that the integrated DCPP reactor protection, engineered safety features actuation and AMSAC systems provide an acceptable degree of diversity to address CCFs of the digital PPS. The NRC staff determined that there is reasonable assurance that the DCPP AMSAC system is sufficiently independent and diverse from the Tricon/ALS PPS and will continue to meet all of the requirements of 10 CFR 50.62 when a failure of the PPS occurs. On the basis of its review, the NRC staff concludes that DCPP PPS D3 assessment methodology is consistent with the NRC staff position stated in the SRP BTP 7-19 and is, therefore, acceptable.

3.7 Communications

By letter dated October 26, 2011 (Reference 1), the licensee stated that the process protection system (PPS) has been designed to meet the requirements of Institute for Electrical and Electronics Engineers (IEEE) Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Reference 32); IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33); and Regulatory Guide (RG) 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011 (Reference 71), among other design standards. Clause 5.6, "Independence," of IEEE Std. 603-1991 requires 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. NUREG-0800 Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.6, "Independence" (Reference 41), provides acceptance criteria for this requirement, and among other guidance, provides additional acceptance criteria for communications independence. Appendix 7.1-C, 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.

The IEEE Std. 7-4.3.2-2003, endorsed by RG 1.152, Clause 5.6, "Independence," provided guidance on how IEEE Std. 603 requirements can be met by digital systems. This clause of IEEE Std. 7-4.3.2, states that, in addition to the requirements of IEEE Std. 603, data communication between safety channels or between safety- and non-safety systems shall not inhibit the performance of the safety function. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.6, "Independence" (Reference 42), provides acceptance criteria for equipment qualifications. This section states that 10 CFR 50, Appendix A, General Design Criterion (GDC) 24, "Separation of protection and control systems," requires that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel that is common to the control and protection systems leaves intact all communications with the safety function processors starts in the same way, with the system satisfying all reliability, redundancy, and independence requirements of the protection system, and that interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired. Additional guidance on interdivisional communications is contained in the DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance," Revision 1, dated March 6, 2009 (Reference 34). DI&C-ISG-04 compliance is discussed further in Section 3.7.1, "Tricon-Based PPS Equipment Communications," of this safety evaluation.

The NRC staff has reviewed the overall design as discussed in the following subsections. As part of this review, the NRC staff evaluated applicability and compliance with SRP Section 7.9, "Data Communication Systems," March 2007 (Reference 240), SRP Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems" (Reference 218), and Branch Technical Position (BTP) 7-11, "Guidance on Application and Qualification of Isolation Devices" (Reference 44).

As discussed in Section 3.1.6, "Process Protection System Hardware Components," of this safety evaluation, the process protection system (PPS) replacement consists of four protection sets which are designed such that each protection set is independent of and protected from adverse influence from the other protection sets. The DCPP PPS is composed of a Tricon subsystem component and an Advanced Logic System (ALS) subsystem component (i.e., processors) as described in Section 3.1.6, "Process Protection System Hardware Components," of this safety evaluation.

Figure 3.7-1 below illustrates the communications architecture for a protection set.[4] The PPS replacement does not utilize any means of interdivisional safety-to-safety data communications. The licensee is maintaining divisional independence by not including any cross divisional communication links between protection sets. Specifically, the Tricon portion of the PPS replacement does not communicate data between redundant safety divisions. In the same manner, the ALS portion of the PPS replacement does not communicate data between redundant safety divisions. In addition, data communication does not occur between the Tricon and the ALS systems and other controllers in within divisions. Data communication does not occur between then Tricon and ALS. Note the ALS processes the analog temperature signals that will be used by the Tricon system to perform the over power delta temperature (OPDT) and over temperature delta temperature (OTDT) reactor trip safety functions. Specifically, the ALS will convert the resistance temperature detector resistance measurements signals representing the reactor hot-leg and cold-leg temperatures and transmit them to the Tricon as 4-20 milliampere analog inputs signals. The Tricon uses these signals to perform the safety function calculations and actuation bistable functions. The same level of communications separation is provided for all four protection sets.

[4] Figure 3.7-1 is an excerpt of Figure 3-3 of the LAR (Reference 12).

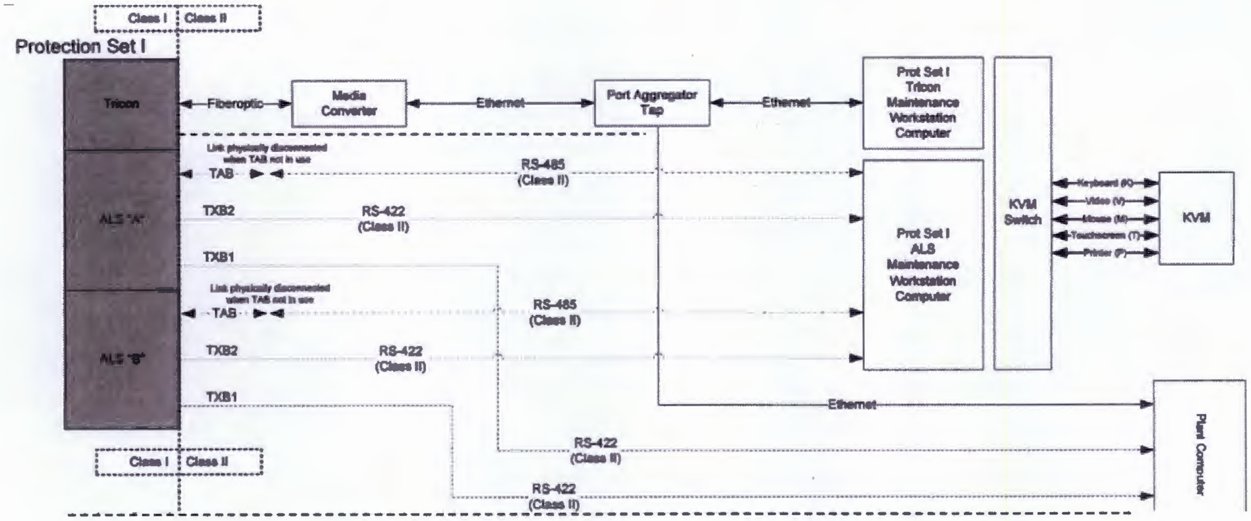


Figure 3.7-1. PPS Replacement Communications - Single Protection Set

Within each protection set, the PPS incorporates safety-to-non-safety communications with the plant computer system, the maintenance work station (maintenance work station) computers. Also, the Tricon communicates with its remote extender module (RXM) non-safety chassis. The plant computer system is part of the existing system, and it is not part of the scope of this license amendment request. Communication with the plant computer system is one way via the gateway switch. The DCPP gateway and gateway switch are part of an existing system and consequently were not included as changes requested in the license amendment request as described in the licensee's letter dated May 9, 2013 (Reference 13).

The Tricon transfers this data through the port aggregator tap. An unmanaged Ethernet switch is provided between the port aggregator network tap Port B and the Tricon maintenance work station to ensure continued multicast operation (and availability of Tricon data to the gateway computer) in the event of maintenance work station network communication failure. Without the Ethernet switch, multicast transmission would cease on loss of the link up to the maintenance work station computer. The ALS communicates this data using one of its transmit TxB communication port. Detailed information about this communication is provided below.

As mentioned in Section 3.1.7.1, each protection set includes two dedicated maintenance work stations, one maintenance work station is connected to and communicates with the ALS system, and the other maintenance work station is connected to the Tricon system, in the associated protection set. The two maintenance work stations cannot communicate with each other.

Other plant data for operators will be provided in the main control room for indication. This data will be provided through hard-wired direct connections (analog isolation devices, so no failure will affect the PPS).

Lastly, there is no communication pathway between the PPS and solid state protection system (SSPS). The PPS will send trip decisions to the SSPS as discrete electrical signals through interposing relays (providing electrical isolation between the PPS and SSPS). The SSPS will evaluate the signals and performs coincident logic functions at the reactor trip system (RTS) and engineered safety feature actuation system (ESFAS) levels.

3.7.1 Tricon-Based PPS Equipment Communications

As mentioned in Section 3.1.6.1.7, the Tricon portion of the PPS replacement does not communicate data between redundant safety divisions. The Tricon can communicate with safety and non-safety systems via the Tricon Communication Module (TCM) and the RXMs. Figure 3.7.1-1 illustrates the Tricon communication for the DCPP PPS. "PSIV" in Figure 3.7.1-1 indicates that only one of the four protection sets (i.e., Protection Set IV) is illustrated.

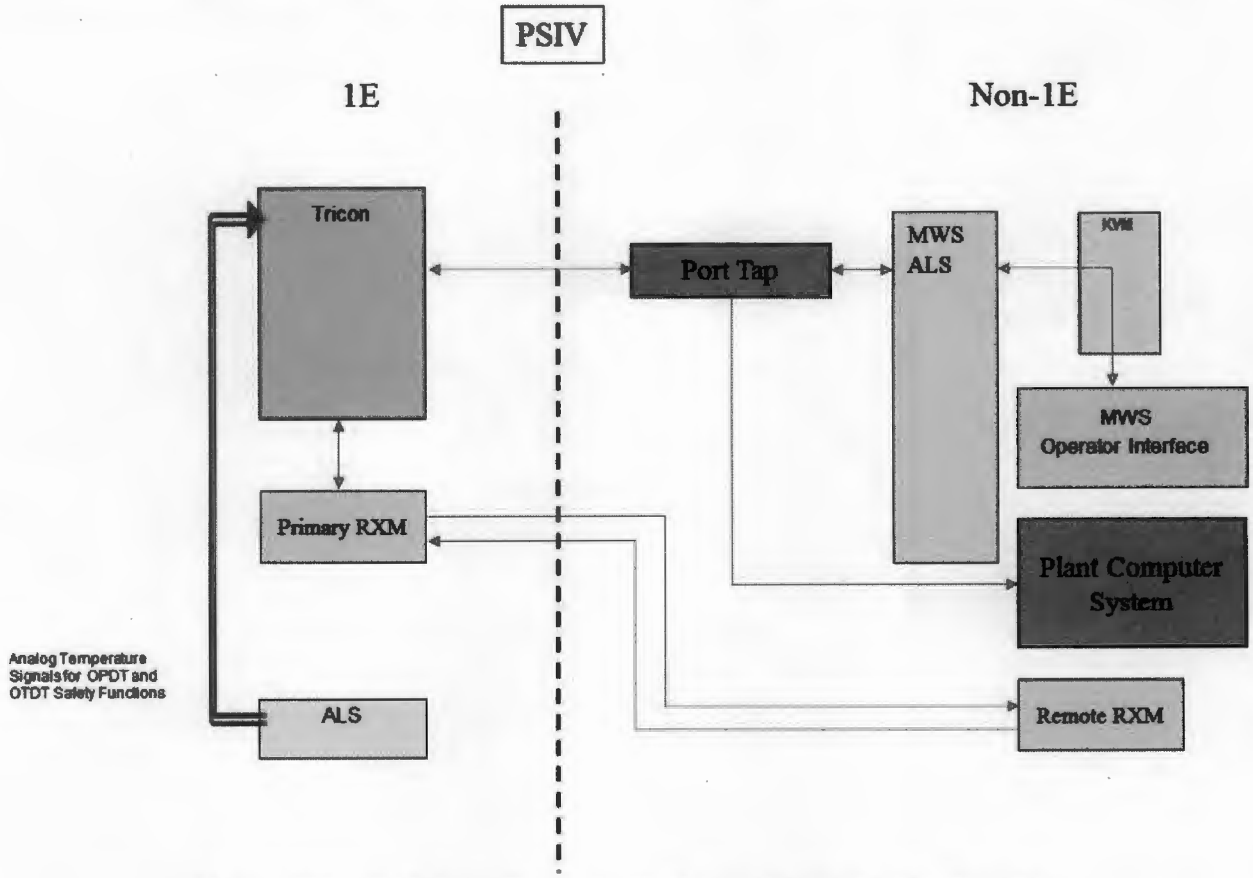


Figure 3.7.1-1. Tricon Communications - Single Protection Set

The main processors in the Tricon send data to the TCM via the triplicated Communications Bus (COMBUS). This communication path was evaluated during the review of the Triconex Approved Topical Report (Reference 29). In summary, the TCM handles all communication protocol tasks. The main processors contain the combined input/output communications and communications processor (IOCCOM), dual-port random access memory (DPRAM), and the embedded application processors that execute the safety control program. Valid messages received by the TCM are triplicated for transmission on the COMBUS and then send to the IOCCOM. The IOCCOM processor retrieves data from the DPRAM to send to either the input/output modules or the TCM, or deposits input/output data or communications messages into the DPRAM for use by the application processor. Separate queues are provided in the IOCCOM for input/output bus and communications messages. The IOCCOM checks the link-level format and the cyclical redundancy check of all messages from the TCM. If the IOCCOM determines that the message is valid and correct, the data are placed into DPRAM. As with the IOCCOM, the DPRAM provides separate memory areas and queues for communication messages and input/output data. These "bins" are separated according to input, output, read-only, read-write, and data type (i.e., Boolean, Reals, Integers). The DPRAM includes extensive memory protection via parity checks, cyclic redundancy checks, checksum, and other mechanisms. Therefore, communication failures won't affect operation of the main processors.

The Tricon portion of the PPS protection set provides data to its associated non-safety-related maintenance work station and the process plant computer gateway computer through the TCM and the port aggregator tap. The Tricon maintenance work station computers (described in Section 3.1.7.1, "Maintenance Work Station," of this safety evaluation) within a redundant safety division communicates only with the safety-related Tricon controller within that division. This communication is through the dedicated NetOptics Model PA-CU network port aggregator tap (described in Section 3.1.7.3, "Port Tap Aggregator," of this safety evaluation). The port aggregator tap has the following ports: Port A, attached to the TCM, Port B, connected to the maintenance work station, and Port 1, connected to the gateway computer. Ports A and B allow two-way communication, and Port 1 only allows one-way outbound communication. 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. The port aggregator tap copies all information that is flowing between Ports A and B to Port 1. There is no communication path from Port 1 to either Port A or Port B. This design ensures that no data or command messages can be sent from the gateway computers to the PPS processors, and consequently ensuring security of the PPS safety function. All communications to Port 1 is channeled through a set of internal operational amplifiers that prohibit the flow of data from the gateway computer to the TCM. This was tested and verified during the review of the Triconex Approved Topical Report (Reference 29).

The TCM uses cyclic redundancy checks, handshaking, and other protocol-based functions to ensure data communication integrity. In addition, the Tricon uses dedicated memory locations for communications (DPRAM). The DPRAM provides separate memory areas and queues for communication messages and input/output data. These "bins" are separated according to input, output, read-only, read-write, and data type (i.e., Boolean, Reals, Integers). The DPRAM includes extensive memory protection via parity checks, cyclic redundancy checks, checksum, and other mechanisms. In this manner, there is no direct communication between the Tricon application processor and the TCM interface with the maintenance work station. Instead, communication between the TCM and application processor is bridged through the DPRAM. Therefore, the TCM provides functional isolation by handling all communication with the plant computer system and the Tricon maintenance work station. Upon total loss of the TCM, the main processors continue to function.

The TCM provides electrical and functional isolation by handling all communications with external devices. Furthermore, through testing, Invensys demonstrated that the TCM will protect the safety processor in the Tricon from communication failures. This information is described in the Tricon safety evaluation for the Triconex Approved Topical Report. The Tricon includes two TCM cards in each main chassis (Slots 7L and 7-R). This provides two non-safety-related communication paths to the maintenance work station and the process plant computer gateway computer from each protection set to ensure continued communications if a single TCM fails.

During the hardware validation test, the independent verification and validation (IV&V) group tested the protection set communications paths to verify that there is no inbound communications path associated with port aggregator network tap Port 1. In particular, the IV&V group validated TCM modules allow the Tricon V10 to communicate with TriStation 1131 and maintenance work station, as specified in the "Validation Test Specification (VTS)," 993754-1-812-P, Revision 1 (Reference 140). The IV&V group records the results of these tests for protection sets II-IV in the hardware validation test reports.

Normally, the maintenance work station is connected as read-only to provide information for monitoring and local display. Bi-directional data communications are permitted under certain conditions between the Tricon and the maintenance work station associated the port aggregator tap device. In this case, the maintenance work station will support maintenance and calibration activities and surveillance functions. Bi-directional communication can only occur when the Tricon keyswitch is in the PROGRAM or REMOTE position. As described in Section 3.1.6.1.1, the Tricon main chassis includes a keyswitch to set the Tricon operating modes between RUN, PROGRAM, STOP, and REMOTE. The keyswitch is a physical interlock that prevents the Tricon for accepting "write" messages when the switch is not in the correct position. An alarm will be annunciated whenever the keyswitch is not in RUN position.

As described in the licensee's letter dated September 11, 2012 (Reference 7), and verified during the regulatory audit conducted June 3-5, 2014 (Reference 38), the keyswitch relies on software to effect disconnection of the maintenance equipment to modify the safety system software. Specifically, the Tricon keyswitch is implemented by a three-gang, four-position switch. The Tricon main processors will read and vote on the keyswitch position. The licensee's letter dated September 11, 2012, describes how this logic was implemented. Strict administrative control over the use the Tricon keyswitches is necessary to ensure operability of the PPS is maintained during system maintenance and surveillance activities. During these activities, the Tricon is taken out of service with site administrative procedures. Refer to Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation for associated site inspection follow-up item. Placing the keyswitch in REMOTE would allow writing of points by an external device.

The Tricon keyswitch must be in the PROGRAM position to allow modification of the application program. In this case, a non-safety computer will be used to upgrade module firmware and/or reprogram the application program installed on the Tricon V10 controller(s).

By letter dated April 30, 2014 (Reference 17), the licensee explained why the STOP position in the keyswitch was disabled for the DCPP PPS, which was described in Section 3.1.6.1.1, "Tricon Main Chassis," of this safety evaluation. Specifically, the licensee did not consider this position necessary to stop operation of the Tricon because technicians could place the keyswitch in PROGRAM to halt the main processors.

During the June 3-5, 2014, regulatory audit, the NRC staff observed the keyswitch logic and operation in the Test System Application Program (TSAP) for DCPP PPS. Operation of the keyswitch was also validated during the Tricon factory acceptance testing (FAT) by Factory Acceptance Test Reports 993754-11-854-1-P, Revision 3 (Reference 157), 993754-12-854-1-P, Revision 0 (Reference 158), 993754-13-854-1-P, Revision 0 (Reference 159), and 993754-14-854-1-P, Revision 0 (Reference 160).

As described in the licensee's letter dated September 11, 2012 (Reference 7), and the Software Design Description (SDD) 993754-11-810-P, Revision 0 (Reference 102), and verified during the June 3-5, 2014, audit (Reference 38), on-line testing and maintenance can be performed on selected of functions without removing the entire Tricon PPS from service, while the keyswitch is in RUN position. Manual out-of-service switches independent of the PPS instrumentation will be provided to perform these actions. As described in the Interface Requirements Specification (Reference 98), an out-of-service switch will be provided for the functions identified in the Interface Requirements Specification. The out-of-service switch will be wired to a Tricon digital input. When a switch is activated for a function, the Tricon allows the associated instrument channel to be taken out of service while maintaining the remainder of the safety division operable. The out-of-service switch only removes the selected function from service and no other function will be affected. In addition, an alarm will be annunciated when a function is taken out of service. This alarm will remain active until the out-of-service switch is returned to its normal position (Reference 38).

The Tricon only allows modification of any parameters if (1) the function has been taken out of service by the out-of-service switch and (2) that removal has been confirmed by the maintenance work station. After these two actions are performed, the Tricon will enable the limited access functions gate enable and gate disable to enable the maintenance work station to modify parameters in the selected function. Section 4.2.13.4 of the license amendment request describes these functions. Detailed description of these functions is provided in the Software Requirements Specifications 993754-11-809-P, Revision 4 (Reference 166), 993754-12-809-P, Revision 2 (Reference 167), 993754-13-809-P, Revision 2 (Reference 168), and 993754-14-809-P, Revision 2 (Reference 169). In addition, during the June 3-5, 2014, audit, Invensys explained the logic and implementation to place a channel in out-of-service. If the out-of-service is returned to its normal position during on-line testing, the Tricon will restore the function to normal operation. Consequently, data from the non-safety maintenance work station to the Tricon is only accepted if valid, error free, keyswitch is in the correct position, the memory tag name attribute is configured as "writeable," and the operator/technician has the necessary credentials to access the system to perform such actions.

The Tricon also incorporates a safety-related to non-safety-related communications link to a remote RXM chassis. The purpose of the remote RXM is to acquire and transfer input/output non-safety-related signals to support functions that are not safety-related PPS functions, such as signals to various main control board indicators. It represents an expansion chassis to be located several miles away from the main chassis. Non-safety-related RXM are only considered within a division. Secondary RXM can only communicate with its assigned primary RXM. Operation and data communication between the Tricon and the RXMs were evaluated in the safety evaluation for the Triconex Approved Topical Report (Reference 29).

In particular, input/output data from the RXM chassis is transferred via the input/output bus, which uses a single-threaded master/slave configuration with the IOCCOM as the bus master. Commands requesting information from the main processor are sent to the RXM via separate path than the responses from the input/output modules. The primary RXM will process this request and send a message to the secondary RXM requesting specific data. The secondary RXM cannot transmit data until a request from the primary RXM is received, since this request enable data transfer. The primary RXM includes an interposing processor to controls access to the secondary RXM, so unrequested messages are not allowed onto the primary RXM.

Communication data faults origination in the non-safety RXM would be mitigated by the data validation features of the processor in the safety-related primary RXM and the IOCCOM processor. This safety evaluation concluded that the RXM design provides adequate protection to the safety side of the input/output bus and the overall safety function. This safety evaluation also states that "all data received from a non-safety remote RXM must not be relied upon to perform the required safety function." For the DCPP PPS, the NRC staff confirmed that signals acquired by the remote RXM are not used to support mitigating functions for a common-cause failure of the Tricon.

3.7.2 ALS-Based PPS Equipment Communications

As stated previously, there are no communication paths between redundant safety divisions or protection sets in the ALS portion of the PPS replacement. There is no communication between the Tricon and ALS. The ALS processes the analog reactor coolant system temperatures that are used by the Tricon system to perform the over power delta temperature (OPDT) and over temperature delta temperature (OTDT) reactor trip safety functions. As described above, these signals are transmitted as 4-20 milliampere (mA) analog.

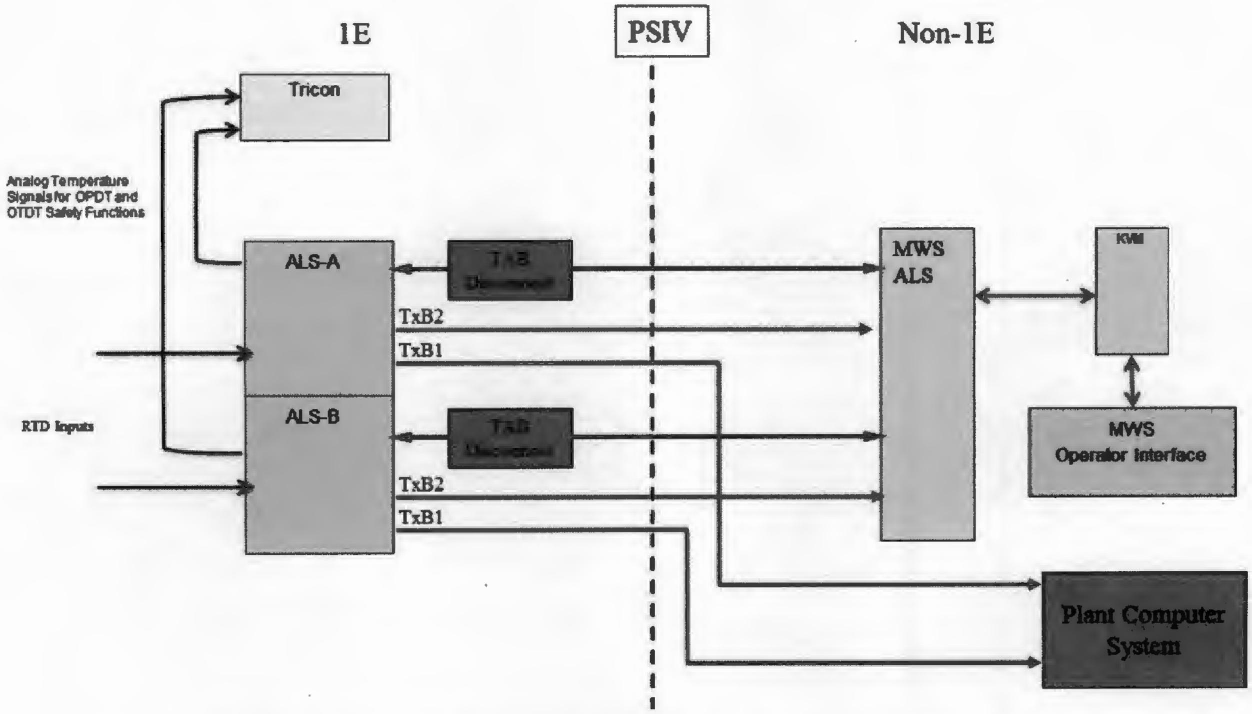


Figure 3.7.2-1. ALS Communications - Single Protection Set

The ALS does not require a Network Port Aggregator Tap to communicate with the plant computer system and the ALS maintenance work station. Instead, the ALS can communicate with external devices via the Test ALS bus (TAB) communication channel and ALS-102 communication channels (TxB1 and TxB2). Figure 3.7.2-1 illustrates the ALS communication for the DCPP PPS.

For testing and maintenance activities, authorized personnel would use the TAB. Use of the TAB data ink will be controlled through plant administrative procedures (refer to Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation for associated site inspections follow-up items). As described in the licensee's letter dated June 22, 2015 (Reference 19), the ALS system does not use a keyswitch to enable/disable the TAB data link. Changes to process variables are possible only when the TAB data link is physically connected to the ALS and the TAB enable digital input is active (Reference 19). The digital input value is used by the maintenance work station to allow access the displays where changes can be made. In particular, connection of the TAB allows access to the ALS-102 non-volatile memory, where tunable parameters are stored. PG&E defined these tunable parameters in the Transfer Function Design Input Specifications (Reference 99). In addition to these parameters, ALS support other registers, defined in "ALS-102 FPGA Requirements Specification," 6116-10201, Revision 1 (Reference 163), to display data in the ALS maintenance work station for periodic surveillance. Activation of the TAB will be alarmed in the control room. Also, the ALS-102 generates a trouble alarm on the front panel to indicate active TAB communication between the

ALS maintenance work station and the ALS chassis. The TAB can be connected to one of the ALS chassis (but not both) in a protection set. (The ALS PPS subsystem is composed of two independent and separate ALS chassis designated as ALS-A and ALS-B.) The chassis not connected with the TAB will continue to perform its safety function.

The Advanced Logical System Topical Report (Reference 30) describes the TAB communication protocol and includes the NRC staff's evaluation of the TAB. In summary, the TAB uses a master-slave communication protocol, using EIA-485 point-to-point serial communication. When the TAB is connected, the ALS Service Unit (ASU) becomes the master of the TAB and initiates transactions with individual boards, including the ALS-102. The TAB does not allow simultaneous data transmission and reception. The TAB employs standard cyclical redundancy check protection to ensure the integrity of the information communicated. The TAB communication protocol supports the transmission of adjustable parameter data, calibration data, operational mode data, sensor data, health, status, and calculated parameter data.

The TAB will communicate with the ASU application that resides on the maintenance work station. The TAB allows access to the ALS-102 non-volatile memory. The non-volatile memory stores setpoints, deadbands, filter coefficients, and configuration parameters unique to the DCPP ALS PPS. Consequently, the non-volatile memory holds the parameters necessary for the core logic board to perform its required functions. Each memory location in non-volatile memory is required to have a cyclical redundancy check. Failed cyclical redundancy checks within the calibration segment of non-volatile memory are reported to the ASU when a TAB transaction accesses the failed memory location.

The TxBs use a serial EIA-422 communication. They are configured to only transmit data to the Packet Data Network (PDN) gateway switch and the ALS maintenance work station. Communications for the TxB ports is unidirectional and does not require the use of handshaking signals, or instructions from the ALS maintenance work station or the PDN gateway switch. As stated in the licensee's letters dated May 9, 2013 (Reference 13), and June 22, 2015 (Reference 19), and the Advanced Logic System Topical Report, both TxB1 and TxB2 are EIA-422 communication links in which the receive capability is physically disabled by hardware (the termination resistor is not used, and are instead terminated in such a way that the transmit data are looped back to the ALS-102 FPGA for integrity testing). The ALS-102 is physically and electrically incapable of receiving information from outside the ALS-102 via the transmit busses TxB1 and TxB2. Unidirectionality of the TxBs provide functional isolation of the ALS chassis. The TxB1 and TxB2 channels are individually isolated from each other.

The ALS-102 transmits application data to the maintenance work station via the TxB2 communication channel. The TxB1 communication channel transmits application data to the PDN gateway switch that connects to the PDN gateway computer.

The communication logic for the TxBs is included in the ALS-102 control logic board. This logic is independent from the safety functions implemented in the ALS-102 (Reference 30).
The "ALS-ASU Communication Protocol," document 6116-00100, Revision A (Reference 100)

describes the configuration of the TxB communication protocol, including data streams and data content and format. The contents of the two data streams are identical in size, content, and transmission rate.

The data to be transmitted via the TxBs are gathered and grouped in ALS-102. This gathering process is performed in the virtual channels of the control logic board in the ALS-102. By letter dated April 30, 2014 (Reference 17), and the ALS-102 FPGA Requirements Specification (Reference 163), the licensee and the ALS vendor describe configuration and operation of the virtual channels, and collection of data information, and subsequent transfer of data through the TxB1/TxB2 data steam. Specifically, a virtual channel is an arrangement of hardware logic that generates a single protection action signal necessary to perform the control or safety function in the ALS-102. The virtual channel is configured in a separated finite state machine in the core logic board. Each virtual channel functions independently, and provides a single protection action signal without affecting any of the other channels. Also, each virtual channel has its own sets of configuration parameters and data registers, and supports a different set of input/output configurations. The ALS-102 FPGA Requirements Specification and IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management" (Reference 78) define the virtual channels for the DCPP PPS. The virtual channel has four distinct operating modes:

- Normal - the virtual channel processes its associated functional logic.
- Bypass - in this mode the channel is out-of-service-alarmed and the filtered/scaled value in the instrument data register is held at its last state (effectively as-is).
- Override - the channel is in ALS bypass (out-of-service) and allows the maintenance work station (via the TAB/ASU interface) to inject digital values and control the channel for testing and calibration. Virtual channel comparators and/or analog output values will process the injected values. This is specific to the ALS-102 board; it does not override the slave board modes of operation.
- Calibrate - the channel is in ALS bypass (out-of-service) and it allows updates to the tunable parameters in the non-volatile memory.

For modification of configurable parameters in the non-volatile memory, the channel should be in the CALIBRATE mode. In addition, each virtual channel includes an enable block to enable/disable the logic (Reference 163). The register to enable this block is part of the non-volatile memory. If a channel is not enabled, it will not process data. Based on the Westinghouse letter dated January 5, 2016 (Reference 198), in response to an NRC request for additional information dated December 23, 2015 (Reference 237), if the contents of the non-volatile memory are corrupted, the board will enter the halt state. In this case, the output board in the system will enter into a fail-safe state, which is pre-determined based on the configuration information in the non-volatile memory.

The data transmitted in the TxBs originate in the data registers used in the virtual channels. These data are marshaled by a specific finite state machine for the TxB communication, where it is then transmitted to the physical bus. The register transfer level that implements the communication channels is part of the platform and is common across all applications of the ALS-102 that use the TxB communications interface. The project specific data set, as defined in the "ALS-ASU Communication Protocol" (Reference 100) is gathered by and written from the ALS-102's core logic board into the communication channel interface module's register interface. This is a one way interface. The licensee's letter dated April 30, 2014 (Reference 17), describes how the data are gathered and transferred in each core.

The maintenance work station validates the data received via TxB2 by checking the information contained in the data package (e.g., cyclical redundancy check). If the data are invalid or erroneous, the maintenance work station will indicate this via the TxB2 status indicator. If the data are valid, the application in the maintenance work station will record the data for information to be displayed in the ALS system status. The ASU software application includes status displays containing read-only indication of connection status for each TxB communication channel.

As described in letters dated September 11, 2012 (Reference 7), April 30, 2014 (Reference 17), and June 22, 2015 (Reference 19), under administrative control, the licensee could make modifications while the system is in operation by placing a channel in bypass mode test-in-bypass, test-in-trip, or manual trip. To make any changes to the channel, it is necessary to place the instrument channel in out-of-service (which requires test-in-trip or test-in-bypass on the ALS), whether operating or shutdown during any of these states. The "ALS Subsystem, System Design Specification" (Reference 127), describes these modes to perform maintenance activities of the ALS-102.

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 input/output (input/output) without affecting adjacent non bypassed safety channels. The Advanced Logic System Topical Report (Reference 30) describes calibration of an analog input/output channel using the ASU. In particular, each virtual channel may be placed out of service by putting it into the ALS bypass, override, or calibrate mode. Override or calibrate will place the virtual channel is out of service. The ASU software application includes status displays containing read-only indication of the out of service condition for each virtual channel or bypass status for each instrument channel. Placing a channel in bypass will not affect operation of the other ALS safety channels in an ALS core. Furthermore, placing a channel in bypass mode in an ALS core (Core A or Core B) for maintenance will not affect the safety functions in the other core.

If a channel is placed in ALS bypass mode, the instrument data register will hold the current value and not populate until the channel has been taken out of ALS bypass or controlled via ALS override mode. During normal operation, the channel operating mode can be changed, but it must first be changed to ALS bypass (out of service) before being changed to calibrate or override.

Based on the ALS-102 FPGA Requirements Specification (Reference 163), the virtual channel operating mode is stored in the non-volatile memory and available for display. When a modification in operating mode is required, the ASU writes to the register directly through the TAB. To modify a channel's calibration coefficients or setpoint values, the channel must first be placed in ALS bypass (out of service) mode and then be placed into calibrate mode.

3.7.3 DI&C-ISG-04 Compliance

The Digital Instrumentation and Controls, DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance," Revision 1, dated March 6, 2009 (Reference 34), developed interim NRC staff guidance on the review of communications issues applicable to digital safety systems. DI&C-ISG-04 contains NRC staff positions on three areas of interest: (1) Interdivisional Communications, (2) Command Prioritization, and (3) Multidivisional Control and Display Stations. Section 3.7, "Communications," of this safety evaluation describes the communication process for the Tricon and Advanced Logic System (ALS).

The licensee described compliance with DI&C-ISG-04 in Section 4.8 of the enclosure to its letter dated April 30, 2013 (Reference 12). In this section, the licensee stated Section 2, Command Prioritization, and Section 3, Multidivisional Control and Display Stations of DI&C-ISG-04 do not apply to the DCPP PPS replacement. The NRC staff agreed with this statement. Therefore, these sections were not evaluated for compliance.

In addition to the information provided in the license amendment request, the licensee submitted "DI&C-ISG-04 Conformance Report," Document No. 993754-1-912, Revision 0, dated September 6, 2011 (Reference 199), and the ALS "Diablo Canyon PPS ISG-04 Matrix," 6116-00054, Revision 0, dated November 9, 2012 (Reference 200). This section summarizes how the Tricon and ALS comply with DI&C-ISG-04 for interdivisional communications.

3.7.3.1 DI&C-ISG-04, Section 1 – Interdivisional Communications

Staff Position 1 of DI&C-ISG-04 provides guidance on the review of communications, which includes transmission of data and information among components in different electrical safety divisions (or channels) and communications between a safety division and equipment that is not safety related. This ISG does not apply to communications within a single division or channel. This NRC staff position states that bidirectional communications among safety divisions and between safety and non-safety equipment may be acceptable provided certain restrictions are enforced to ensure there will be no adverse impact on safety systems. It also states that systems which include communications among safety divisions and/or bidirectional communications between a safety division and non-safety equipment should adhere to the 20 points described below.

The methods by which the DCPP PPS replacement system either meets these points or provides an acceptable alternative method of complying with NRC regulations are discussed below.

3.7.3.1.1 Staff Position 1, Point 1

Staff Position 1, Point 1, states that 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 Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32). It is recognized that division voting logic must receive inputs from multiple safety divisions.

The PPS does not use any means of interdivisional data communications. The licensee is maintaining divisional independence by not including any cross-divisional communication links between protection sets. In addition, data communication does not occur between the Tricon and the ALS systems within a division, and each system has its independent maintenance work station. Thus, there is no communication between controllers in redundant safety divisions. In addition, all voting logic for engineered safety function actuation system and reactor trip functions would be performed by the solid state protection system. The solid state protection system is not modified by this license amendment request.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

<u>Tricon</u>

The Tricon portion of the PPS replacement does not communicate data between redundant safety divisions, and furthermore it does not communicate with the ALS in the same division. Thus, the Tricon does not require information originating outside its own safety division to perform its safety functions.

The sensors connected to the Tricon are dedicated sensors and operate completely independent of other Tricon protection sets. However, in a division, the ALS system converts temperature resistance temperature detector signals, representing the reactor hot-leg and cold-leg temperatures, and transmit them to the Tricon system as 4-20 milliampere analog inputs signals. The Tricon uses these signals to perform the safety function calculations and actuation bistable functions.

Within each protection set, the Tricon incorporates safety-to-non-safety communications with the plant computer system, its maintenance work station (maintenance work station) computers, and its remote RXM [remote extender module] non-safety chassis. The Tricon Communication Modules (TCMs) allow the Tricon to communicate with the maintenance work station and plant computer system through the dedicated port aggregator network tap. The NetOptics port aggregator tap is a hardware device that provides a bidirectional communication path to the

Tricon maintenance work station and a one-way hardware enforced communication path to the plant computer system.

Bidirectional communication with the maintenance work station is only permitted when a channel is taken out of service. To take a channel out of service, the following actions should be performed: (1) activate the out-of-service switch for that channel locked in a cabinet and (2) activating a software switch on the maintenance work station, which requires password access. When an out of service is activated, an alarm is indicated in the control room.

The Tricon also incorporates a safety-related to non-safety-related communications link to a remote RXM chassis. The purpose of the remote RXM is to acquire and transfer input/output non-safety-related signals to support functions that are not safety-related PPS functions, such as signals to various main control board indicators. It represents an expansion chassis to be located away from the main chassis. There is no data exchange between RXM chassis in other protection sets. Communications with these devices are described in Section 3.7, "Communications," of this safety evaluation.

ALS

There are no communication paths between redundant safety divisions or protection sets in the ALS portion of the PPS replacement. Furthermore, the ALS system does not depend on information originating outside its own protection set to perform the safety functions.

Within each protection set, the Tricon incorporates safety-to-non-safety communications with the plant computer system and its maintenance work station (maintenance work station) computers via the Test ALS bus (TAB) data link and ALS-102 communication channels (TxB1 and TxB2).

Bidirectional communication with the ALS maintenance work station only occurs when the TAB data link is physically connected to one of the ALS core and the TAB enable digital input is active. Activation of the TAB will be alarmed in the control room.

3.7.3.1.2 Staff Position 1, Point 2

Staff Position 1, Point 2, states that 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 does not use any means of interdivisional data communications. The licensee is maintaining divisional independence by not including any cross-divisional communication links between protection sets. In addition, data communication does not occur between the Tricon and the ALS systems within a division. Thus, there is no communication between controllers in redundant safety divisions.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

All Tricon communication with external devices is via the TCMs, NetOptics port aggregator tap, and the remote RXMs. As mentioned in Point 1, the Tricon does not share data between redundant safety divisions.

The TCM provides functional isolation by handling all communication with external devices. The communication paths have cyclical redundancy check and Internet Protocol (IP) address discrimination. Based on the Triconex Approved Topical Report (Reference 29), upon total loss of the TCMs, the main processors will continue to function and execute the Test System Application Program (TSAP). Electrical isolation is provided by multi-mode fiber optic cable connections on the TCM, and isolation tests of the TCM serial communication ports demonstrate adequate electrical isolation between the safety-related portions of the Tricon V10 and connected non-safety-related communication circuits.

Access to the Tricon is governed by the Tricon keyswitch. The keyswitch must be in the PROGRAM position to accept commands from TriStation that can modify the application running in the controller. In addition, to modify the program, the programmer must have access to the current program version loaded on the programming terminal, TriStation 1131. To access the program, the programmer must enter the correct password.

To modify parameters, the keyswitch should be in the REMOTE position. The Tricon allows modifications of certain parameters when in RUN position, if (1) the function has been taken out of service by the out-of-service switch, and (2) that removal has been confirmed by the maintenance work station (maintenance work station). Whenever the out-of-service switch is activated, and alarm will be annunciated in the control room. Furthermore, the Tricon system will activate an alarm whenever the keyswitch is not in RUN position.

The remote extender module (RXM) only acquires and transfers input/output non-safety-related signals to support functions that are not safety-related PPS functions. The primary RXM module set is connected to the remote RXM module set housed in a remote chassis. There is no data exchange between RXM chassis in other protection sets. The RXM modules are connected by fiber optic cables and therefore can be used as 1E to non-1E isolators between safety and non-safety-related. The use of RXM communications in this manner was described in the Triconex Approved Topical Report and was evaluated by the NRC in the associated safety evaluation (Reference 29).

ALS

The ALS communicates with external devices via the Test ALS bus (TAB) data link and ALS-102 communication channels (TxB1 and TxB2).

The TxB communication is unidirectional and it does not require instructions from the maintenance work station. Furthermore, the TxB communication link is physically and electrically disable to receive data.

Use of the TAB data link will be controlled by plant administrative procedures. Furthermore, to establish bidirectional communication between the ALS maintenance work station and the ALS chassis, the TAB data link should be physically connected and the TAB enable digital input is active. Activation of the TAB will be alarmed in the control room.

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 input/output without affecting adjacent non-bypassed safety channels via the ASU and TAB. The maintenance of an instrument channel affects only the specific channel being maintained; the remaining channels within the ALS chassis are operable and continue to perform their safety function, unaffected by the bypass or maintenance status of adjacent channel(s).

3.7.3.1.3 Staff Position 1, Point 3

Staff Position 1, Point 3, states that 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 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, but could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and thus 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 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 system does not use any means of interdivisional data communications. Furthermore, the ALS and Tricon in one division do not share information between them and they do not receive communication from outside its safety division to perform its safety functions.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this Staff Position 1, Point 3.

3.7.3.1.4 Staff Position 1, Point 4

Staff Position 1, Point 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 communications 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 CFR Part 50, Appendices 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 communications 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 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 NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

<u>Tricon</u>

All Tricon communication with external devices is via the TCM sand the remote RXMs.

The TCM is a communication device that transfers data between the main processors and external devices through the port aggregator tap. The TCMs allow the Tricon to communicate with the maintenance work station through the dedicated one-way port in the port aggregator tap.

The TCM uses cyclic redundancy checks, handshaking, and other protocol-based functions to ensure data communication integrity. In addition, the Tricon uses dedicated memory locations for communications (dual-port random access memory or DPRAM). The DPRAM provides separate memory areas and queues for communication messages and input/output data. These "bins" are separated according to input, output, read-only, read-write, and data type (i.e., Boolean, Reals, Integers). The DPRAM includes extensive memory protection via parity checks, cyclic redundancy checks, checksum, and other mechanisms. In this manner, there is no direct communication between the Tricon application processor and the TCM interface with the maintenance work station. Instead, communication between the TCM and application processor is bridged through the DPRAM. Therefore, the TCM provides functional isolation by handling all communication with the plant computer system and the Tricon maintenance work station. Upon total loss of the TCM, the main processors continue to function.

The Tricon also incorporates a safety-related to non-safety-related communications link to a remote RXM chassis. Both RXMs include processors to control data transmission. The safety-related primary RXM monitors all message originating in the Tricon main processor. The primary RXM's processor control access to the input/output data in the secondary RXM. Specifically, the Tricon main processor will send a request to the primary RXM using the input/output bus, which is a master/slave bus, with the primary RXM as the slave. The primary RXM will process this request and send a message to the secondary RXM requesting specific data. The secondary RXM cannot transmit data until a request from the primary RXM is received, since this request enable data transfer. The request message is sent via a separate channel than the channel to send the data.

The Triconex Approved Topical Report and the NRC's associated safety evaluation (Reference 29) describe the internal communication path for external devices to and from the Tricon V10 platform.

ALS

The ALS does not use processors. Instead, the ALS portion of the PPS replacement platform uses field programmable gate array (FPGA) hardware logic technology. Therefore, the ALS does not include a communications processor. The ALS-102 core logic board contains the application-specific logic circuits which define and control the operation of the PPS subsystem.

The data transmitted for communication via the TxBs is gathered in the ALS-102 core logic board, but this logic is independent of the safety functions implemented in the ALS-102. This prevents communication errors and malfunctions from interfering with the execution of the safety functions. Furthermore, the ALS uses different registers (i.e., not shared) for separating communication functions in the virtual channel. In addition, the TxB1/TxB2 are transmit only (unidirectional) and incapable of receiving data.

The Test ALS bus (TAB) is bidirectional and used for diagnostics, calibration, and system information gathering. The TAB is only connected and enabled during surveillance, testing, and maintenance periods via the maintenance work station. For bidirectional communication to occur, the TAB data link should be physically connected to the ALS core and the TAB enable digital input is active. Activation of the TAB will be alarmed in the control room.

3.7.3.1.5 Staff Position 1, Point 5

Staff Position 1, Point 5, states that 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 NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with Staff Position 1, Point 5.

A description on how each system meets this criterion is provided below.

Tricon

The Tricon Communication Module (TCM) and the main processor exchange data asynchronously via the Communications Bus (COMBUS). The two microprocessors exchange data through the dual-port random access memory (DPRAM). The safety evaluation of the Triconex Approved Topical Report (Reference 29), evaluated asynchronous operation of the TCM and main processor. In particular, the combined input/output communications and communications processor (IOCCOM) retrieves data from the DPRAM to send to either the input/output modules or the TCM, or deposits input/output data or communications messages into the DPRAM for use by the embedded application processor. The main processor has higher priority for accessing the DPRAM. In addition, separate queues are provided in the IOCCOM for input/output bus and communication messages. To ensure adequate execution time for safety-related input/output, the IOCCOM executes communications messages with the TCM only while waiting for input/output responses. The IOCCOM checks the link-level format and the cyclical redundancy check of all messages from the TCM. If the IOCCOM determines that the message is valid and correct, the data are placed into DPRAM.

Invensys performed operational testing to determine the longest scan-time duration. The results of these tests are in the "System Time Response Confirmation Reports," 993754-11-818-P, Revision 0, dated July 1, 2014 (Reference 201), 993754-12-818-P, Revision 0, dated

December 1, 2014 (Reference 202), 993754-13-818-P, Revision 0, dated December 1, 2014 (Reference 203), and 993754-14-818-P, Revision 0, dated December 1, 2014 (Reference 204). Section 3.15, "Response Time Characteristics," of this safety evaluation describes the result of the NRC safety evaluation.

ALS

The ALS does not include a communications processor.

Westinghouse performed testing to determine the time base frame rates for the ALS-102 boards during the factory acceptance testing (FAT). The results of these tests are in the ALS "Factory Acceptance Rest Reports," for Protection Set I, 6116-70033, Revision 0, Protection Set II, 6116-70034, Revision 0, Protection Set III, 6116-70035, Revision 0, and Protection Set IV, 6116-70036, Revision 0, August 2015 (Reference 162). The NRC staff also reviewed the FAT reports to confirm satisfactory measured frame rates of the ALS-102 boards. Section 3.15, "Response Time Characteristics," of this safety evaluation describes the results of the NRC evaluation.

3.7.3.1.6 Staff Position 1, Point 6

Staff Position 1, Point 6, states the safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes that the Tricon and ALS for the DCPP PPS complies with Staff Position 1, Point 6.

A description on how each system meets this criterion is provided below.

Tricon

The Tricon portion of the PPS replacement does not receive communication from outside its safety division to perform its safety functions. The Tricon system does not use interrupts from external devices.

The Tricon has one microprocessor to execute the safety program and another microprocessor (IOCCOM) to handle all data transfer with input/output modules and the TCM. The two microprocessors exchange data through the DPRAM. The IOCCOM interfaces with the input/output modules via the input/output bus. The IOCCOM interfaces with the TCMs via the Communications Bus (COMBUS).

ALS

The ALS does not include a communications processor. In addition, the ALS portion of the PPS replacement does not receive communication from outside its safety division to perform its safety functions. The ALS system does not perform communication handshaking or use interrupts from external devices.

3.7.3.1.7 Staff Position 1, Point 7

Staff Position 1, Point 7, states that 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 predetermined. 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 NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes that the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

The Tricon uses Tricon-compatible protocols for communicating with external devices, including remote RXMs (remote extender modules). These data are set every scan cycle, and at regular intervals, whether the data in the set have changed or not. These protocols were described and evaluated in the safety evaluation for the Triconex Approved Topical Report (Reference 29). The IOCCOM processor will perform a validity check before processing any message. Furthermore, the DPRAM includes memory protection via parity checks, cyclic redundancy checks and checksum, and other mechanisms. Therefore, corrupted or invalid messages will be discarded.

The design characteristics of the Tricon ensure the input/output messages between the main processor and non-safety input/output modules (via the safety-related primary RXM and non-safety remote RXM) are processed in a deterministic manner, with the characteristics of predictability, repeatability, bounded in time, and robustness. The inherent design characteristics as well as the built-in diagnostics ensure that any failures of the non-safety remote RXM chassis, whether the remote RXM modules or non-safety input/output modules, do not adversely impact the safety function of the safety-related main and primary RXM chassis.

ALS

When bidirectional communication is established between the maintenance work station (maintenance work station) and the ALS, the Test ALS Bus (TAB) uses standard cyclical redundancy check protection to ensure data integrity. With this validation, unrecognized messages are not accepted or used.

The ALS-102 core logic board TxB1/TxB2 communication functions are one-way, transmit only. Westinghouse defined the communication protocol for them in the "ALS-ASU Communication Protocol," 6116-00100, Revision A (Reference 100). The ALS Service Unit (ASU) in the maintenance work station validates the data received before using it.

3.7.3.1.8 Staff Position 1, Point 8

Staff Position 1, Point 8, states that 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 system does not use any means of interdivisional data communications. Furthermore, the ALS and Tricon in one division do not share information. The discussion in these points also explained how communication with non-safety devices is implemented.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

3.7.3.1.9 Staff Position 1, Point 9

Staff Position 1, Point 9, states that 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 NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

All Tricon communication with external devices is via the Tricon Communication Modules (TCMs) and remote extender modules (RXMs). The combined input/output communications (IOCCOM) processor in the main processor uses dedicated memory locations for communications with the TCMs. Specifically, data received by the Tricon is stored in fixed and dedicated memory locations. All communications between the safety processor and the

IOCCOM and RXMs are via dual-port random access memory (DPRAM). The DPRAM provides separate memory areas and queues for communication messages and input/output data. In addition, input data are separated from output data via the DPRAM. Input/output data processing takes priority over communication messages to/from the TCMs. Data are exchanged with the applications software at the end of each program scan.

For communications with the RXMs, the Tricon uses the input/output bus to transmit data to the IOCCOM processor. Commands requesting information from the main processor are sent to the RXM via separate path than the responses from the input/output modules. In addition, the IOCCOM processor verifies the data before processing data and forward it to the DPRAM, and from the DPRAM the main processor can retrieve this data.

ALS

The ALS does not include a communications processor. In the ALS, the communication processing logic circuits are separated from safety processing logic circuits but resides in the ALS-102 core logic board. Data registers created in the virtual channels to be transmitted is marshaled via a specific finite state machine (see the licensee's letter dated June 22, 2015 (Reference 19), for detailed information on data gathering for each core). The communication protocol and packet contents for the DCPP PPS project were defined in the "ALS-ASU Communication Protocol," 6116-00100, Revision A (Reference 100).

3.7.3.1.10 Staff Position 1, Point 10

Staff Position 1, Point 10, states that safety division software should be protected from alteration while the safety division is in operation. Online changes to safety system software should be prevented by hard-wired interlocks or by physical disconnection of maintenance and monitoring equipment. A work station (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 work station 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 hard-wired 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 work station to accommodate the effects of the open circuit or for status logging or other purposes.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

The Tricon system does not fully meet Staff Position 1, Point 10. The licensee provided justification to an alternative mean to meet Point 10. Specifically, the licensee used a combination administrative controls and system design to meet this Point.

The Tricon's maintenance work station (maintenance work station) computers communicate only with the safety-related Tricon controller within that division. The maintenance work station within a given protection set cannot communicate with or modify a maintenance work station from another protection set. The data are transmitted through the TCMs. In addition, this communication is through the NetOptics port aggregator tap, providing another level of protection.

Modifications to the Tricon software require a personal computer with TriStation 1131 software. Furthermore, the Tricon has a keyswitch to prevent the TCM for accepting "write" messages. Access to the key will be site-controlled by administrative procedures. The keyswitch relies on software to allow connection with the TriStation 1131. Section 4.8.10 of the enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the logic implementation of the keyswitch. The keyswitch position is monitored by the Tricon and whenever the keyswitch is not in the RUN position, an alarm will be activated in the control room.

The Tricon keyswitch must be in the PROGRAM position to allow modifications to the application program executing in the Tricon. To allow modification of parameters, the keyswitch must be in either PROGRAM or REMOTE position. When the Tricon is in RUN, the system won't accept parameters modifications, except for certain defined variables. In this case, the Tricon will only allow modification of any parameters if (1) the function has been taken out of service by the out-of-service switch, and (2) that removal has been confirmed by the maintenance work station. After these two actions are performed, the Tricon will enable the limited access functions gate enable and gate disable. The Tricon will generate an alarm upon actuation of any channel out-of-service switch in a protection set.

The RXM cannot be modified during run time. Furthermore, there is no interface with the TriStation 1131 running in the plant's personal computer that would allow modification of the RXM module firmware during run time.

ALS

The Test ALS Bus (TAB) data link is the only mechanism to adjust addressable constants, setpoints, or parameters. To enable this communication the ALS data link should be physically connected and the TAB enable digital input active. Activation of the TAB will be indicated in the control room.

By letters dated April 30, 2014 (Reference 17), and June 22, 2015 (Reference 19), the licensee explained how certain ALS parameters can be modified during plant operation, when the instrument channel is out of service. Furthermore, enabling the TAB data link to the maintenance work station 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. PG&E will establish administrative controls to require restoration of the affected ALS core chassis within 30 days for the condition in which a single ALS core chassis is out of service, except for maintenance of the of the narrow-range resistance temperature detector (RTD) temperature channels. In its letter dated April 30, 2014, the licensee explained the reasons for this exception and provided justification for this exception.

The TAB communication cannot be used to modify the safety logic in the ALS. Changes to the safety logic will require the use of special tools and board removal. By letter dated June 22, 2015, the licensee explained that if one of the ALS-102 board needs to be replaced, the licensee would require the use of a spare board. In this case, the licensee would need to configure the parameters in the non-volatile memory. The licensee would use the ALS test and configuration tool to load the associated non-volatile memory image to the spare board. The licensee confirmed this tool cannot be used to modify or download field programmable gate array (FPGA) logic.

3.7.3.1.11 Staff Position 1, Point 11

Staff Position 1, Point 11, states that 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 does not utilize any means of interdivisional safety-to-safety data communications. The licensee is maintaining divisional independence by not including any cross-divisional communication links between protection sets. Specifically, the Tricon portion of the PPS replacement does not communicate data between redundant safety divisions. In the same manner, the ALS portion of the PPS replacement does not communicate data between redundant safety divisions.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

3.7.1.1.12 Staff Position 1, Point 12

Staff Position 1, Point 12, states that communication faults should not adversely affect the performance of required safety functions in anyway. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 CFR Part 50, Appendix A. This section provides 12 examples of credible communication faults, but cautions that the possible communication faults are not limited to the list of 12.

As previously noted in Points 2 and 4, the Tricon and ALS do not receive information from external devices, and these systems do not use any means of interdivisional data communications.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

All communication with external devices is through either the TCMs or the RXMs. Furthermore, as described in Point 5, the Tricon has one microprocessor to execute the safety program, and another microprocessor (IOCCOM) to handle all data transfer with input/output modules and the TCM. The two microprocessors exchange data through the dual-port random access memory. As stated in Point 7, the Tricon system includes the means to detect and reject invalid messages. Therefore, if a failure of the TCM or RXM occur, the main processor will continue to perform its safety functions.

ALS

ALS communicates with external devices via the TAB or TxB communications. The TAB data link will only be used during surveillance, testing, and maintenance periods via the maintenance work station. When bidirectional communication is established between the maintenance work station and the ALS, the TAB uses standard cyclical redundancy check protection to ensure data integrity. With this validation, unrecognized messages are not accepted or used. In the case of the TxB communication, the faults described in this DI&C-ISG-04 position do not apply because the ALS is not receiving any messages or acknowledgements by way of the TxB lines. As described in Section 3.7.2, the TxB channels are physically disabled by hardware.

3.7.3.1.13 Staff Position 1, Point 13

Staff Position 1, Point 13, states that 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 system does not use any means of interdivisional data communications. Furthermore, the ALS and Tricon in one division do not share information.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

3.7.3.1.14 Staff Position 1, Point 14

Staff Position 1, Point 14, states that 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 system does not use any means of interdivisional data communications. Furthermore, the ALS and Tricon in one division do not share information.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

3.7.3.1.15 Staff Position 1, Point 15

Staff Position 1, Point 15, states that communications 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 evaluation of the DCPP PPS replacement system against Staff Position 1, Point 7, determined that a fixed data format of the data sets used by the station was established. As a result, these data sets are predefined and their format and sequence are predetermined.

A description on how each system meets this criterion is provided below.

Tricon

The Tricon uses Tricon-compatible protocols for communicating with external devices, including remote RXMs. These protocols were described and evaluated in the safety evaluation of the Triconex Approved Topical Report (Reference 29).

ALS

After bidirectional communication is established between the maintenance work station and the ALS, the TAB will use standard cyclical redundancy check protection to ensure data integrity. With this validation, unrecognized messages will not be accepted or used.

The ALS-102 core logic board TxB1/TxB2 communication functions are one-way, transmit only.

3.7.3.1.16 Staff Position 1, Point 16

Staff Position 1, Point 16, states that "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 a reactor protection system/engineered safety features actuation system communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criterion of: (1) 10 CFR Part 50, Appendix A, GDC 24, which states, in part, that "[i]nterconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired," and (2) IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" and the correction sheet dated January 30, 1995 (Reference 32) (Source: Section 3.4.3 of NUREG/CR-6082, "Data Communications," August 1993; Reference 205).

The PPS replacement system does not use any means of interdivisional data communications. Furthermore, the ALS and Tricon in one division do not share information.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

3.7.3.1.17 Staff Position 1, Point 17

Staff Position 1, Point 17, states that pursuant to 10 CFR 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 electromagnetic interference/radio frequency interference and power surges, if the environments are significant to the equipment being qualified.

Section 3.5, “Equipment Environmental Qualification,” of this safety evaluation describes equipment qualification testing performed on the ALS and Tricon systems to support DCPP PPS replacement.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

The qualification of the Tricon platform did not include the fiber optic cable. In the “Software Configuration Management Plan (SCMP),” Revision 1, 993754-1-909-P, dated December 18, 2012 (Reference 116), the licensee noted that since the TCM and the remote RXM link do not constitute vital or safety links, the gradual degradation requirement does not apply. However, it has been established that the fiber optic cable meets electrical isolation requirements. In addition, the RXMs were qualified electrical isolation devices, meeting the electrical isolation requirements of IEEE 384-1981, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits” (Reference 206).

ALS

The ALS does not rely on data communications outside the ALS chassis for any safety function. Within the chassis, the communications media is provided by circuit traces on the backplane and the ALS cards. Section 3.5 describes equipment qualification testing.

3.7.3.1.18 Staff Position 1, Point 18

Staff Position 1, Point 18, states that provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

A description on how each system meets this criterion is provided below.

Tricon

The Tricon Communication Module (TCM) handles all protocol, start/stop bits, handshaking, etc., tasks. The main processor is neither burdened nor interrupted. Communication errors and malfunctions do not interfere with the execution of the safety function. Exchange of data between the communications processors and main processor occur in every scan cycle.

Because all the communication with external devices, systems, and hosts is performed by and localized in the TCM, the main processors are alleviated of unneeded communications functionality and attendant complications due to complexity. Also, as discussed in Invensys response to Point 10, the Tricon architecture ensures that the keyswitch, out-of-service switches, and programmed features in the PPS application program prevent changes to the application program and setpoints. This mitigates any deficiencies in the TCM with regard to performance deficits posed by unneeded functionality.

A failure modes and effects analysis (FMEA) was performed on the Tricon system, which documented evaluation of postulated failures on the operation of the main processors, TCMs, and RXMs. Evaluation of this FMEA is provided in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation.

ALS

The ALS uses virtual channels, which are assigned individual logic paths within the core logic board. In this manner, the safety logic is separated and independent of the communication finite state machine. The data gathered and transmitted in the communication channels (TxBs) originate in the data registers used in the virtual channels. Specifically, transmit channels pass data from their channel data register to the channel's communication interface outputs through buffers, providing channel integrity verification.

3.7.3.1.19 Staff Position 1, Point 19

Staff Position 1, Point 19, states that the communications data rates be such that they will not exceed the capacity of a communications link or the ability of nodes to handle traffic, and that all links and nodes have sufficient capacity to support all functions. To do this, 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 and that communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.

The "DI&C-ISG-04 Conformance Report," 993754-1-912, Revision 0 (Reference 199), and the ALS "Diablo Canyon PPS ISG-04 Matrix," 6116-00054, Revision 0 (Reference 200) describe how each vendor showed compliance with Point 19. A brief description on how each system meets this criterion is provided below.

The NRC staff has reviewed the design and functionality of the communications process, has examined the hardware and software used to implement this process, and concludes the Tricon and ALS for the DCPP PPS complies with this item.

Tricon

Communication within the Tricon is cyclic, with data being refreshed in every scan. Factors that affect Tricon communications performance include: COMBUS speed, amount of aliased data and scan time, network speed and loading, and the communication protocol selected. The "Software Configuration Management Plan (SCMP)," Revision 1, 993754-1-909-P, dated December 18, 2012 (Reference 116), defines the scan time and communication speed for each factor. This information showed the data rate capacity in the Tricon system exceeds the capacity of the communication through the TCM. But in the event the main processors are excessively burdened with data requests, the Tricon continuously monitors system health and performance, activating an alarm should scan time exceed the predicted performance.

For the RXMs, congestion is not a concern, because the input/output bus is a closed system utilizing a single-threaded master-slave serial protocol based on RS-485.

Section 3.15, "Response Time Characteristics," of this safety evaluation describes the system response time characteristics for the Tricon system.

ALS

Internal communication in the ALS is performed via the Reliable ALS Bus (RAB), which was evaluated with the Advanced Logic System Topical Report (Reference 30). The RAB uses point-to-point safety communication. TxB communications are all point-to-point serial. The TxB1/TxB2 are used for sending ALS status information. The TxB1/TxB2 are transmit only (unidirectional).

Bidirectional communication is only permitted through the Test ALS Bus (TAB). When bidirectional communication is established, the TAB uses a master-slave protocol, with the ALS Service Unit (ASU) acting as the master. In this manner, the TAB does not allow simultaneous data transmission and reception.

Westinghouse defined the data scan rates during the system design. Section 3.15, "Response Time Characteristics," of this safety evaluation describes the system response time characteristics for the ALS system.

3.7.3.1.20 Staff Position 1, Point 20

Staff Position 1, Point 20, states that 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.

Section 3.15, "Response Time Characteristics," of this safety evaluation describes the system response time characteristics for the ALS and Tricon systems. This section also provides the NRC staff evaluation on this subject.

3.7.3.2 DI&C-ISG-04, Section 2 – Command Prioritization

Section 2 of DI&C-ISG-04 provides guidance applicable to a prioritization device or software function block, which receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device.

This section was not evaluated for the DCPP PPS replacement.

3.7.3.3 DI&C-ISG-04, Section 3 – Multidivisional Control and Display Stations

Section 3 of DI&C-ISG-04 provides guidance concerning operator work stations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division, and applies to work stations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the work station.

This section was not evaluated for the DCPP PPS replacement.

3.8 Tricon V10 Platform Reference Design Changes

By letter dated August 2, 2012 (Reference 6), Pacific Gas and Electric Company (PG&E) notified the NRC staff of Tricon V10 platform changes associated with its PPS replacement license amendment request. Attachment 4 to the August 2, 2012, letter, "V10 Tricon Reference Design Change Analysis," 993754-1-916, Revision 0, dated March 19, 2012, (Reference 207), provided the scope and extent of changes to the previously approved Tricon V10 platform topical report referenced within the DCPP PPS LAR.

The Triconex Approved Topical Report (Reference 29) and other Tricon platform documents submitted with the PPS replacement license amendment request letter dated October 26, 2011 (Reference 1), describe use of the Tricon V10.5.1 platform and the TriStation 1131 V4.7.0. This is also the platform version for which the NRC provided the baseline Tricon V10 safety evaluation for generic nuclear industry approval.

Since approval of the Tricon V10 platform, the Tricon platform has undergone changes for various reasons and version V10.5.3 is the most current nuclear qualified product, subsequent to maintenance releases V10.5.2 and V10.5.3. The TriStation 1131 has also been changed to resolve various performance issues and version V4.9.0 is the most current nuclear qualified product. These are the versions used for the development of the DCPP PPS replacement.

During a regulatory audit of the Invensys facility conducted on November 13-16, 2012, the NRC staff reviewed proposed deviations from the approved Tricon V10 topical report and verified these changes were implemented pursuant to regulatory criteria identified in the Tricon V10 safety evaluation. Details of this audit are contained in the associated audit report (Reference 36). The results of this audit are summarized below.

3.8.1 System Level Differences Between V10.5.1 and V10.5.3

Implementation of V10.5.3 changes did not require any changes to the architecture of the Tricon V10 system.

3.8.2 Hardware Changes

Tricon V10 system hardware is unchanged between V10.5.1 and V10.5.3. No new hardware or components were added, and existing hardware components described in Section 3.1.6, "Process Protection System Hardware Components," of this safety evaluation have not been modified in either maintenance releases V10.5.2 or V10.5.3.

3.8.3 Software Changes

No new software modules were added to the Tricon system in maintenance releases V10.5.2 or V10.5.3; however, three existing software modules in Tricon V10.5.1 were revised. They are:

1. Analog input firmware used in the Next Generation Analog Input (NGAI) Module (3721N). This module is used for processing safety-related analog inputs.
2. Digital output firmware used in the Next Generation Digital Output (NGDO) Module (3625N). This module is used for processing safety-related digital outputs.
3. TriStation 1131 Programming Software. This software is the engineering tool for developing the safety-related application program.

All other software remained unchanged.

The NRC staff reviewed documentation associated with these software changes during the Invensys regulatory audit and a summary of these changes is provided as follows.

Maintenance Release V10.5.2

The NRC staff reviewed the "Tricon V10.5.2 Release, Software Release Definition," 6200003-226, Revision 1.0, dated December 10, 2010 (Reference 208); "Tricon V10.5.2, Engineering Project Plan," Revision 1.4, 9100346-001, dated December 2, 2010 (Reference 209); and the "Tricon V10.5.2, V&V Test Report," Revision 1.1, dated January 14, 2011 (Reference 137), for this release. The V10.5.2 upgrade was initiated by Invensys Operations Management (IOM) to resolve an internal diagnostic anomaly on input/output modules 3625/N (Digital Output 6255), 3720 and 3721/N (Analog Input 6256). This anomaly was discovered in the field (from non-nuclear sources) and caused random indication of a fault condition in the affected module. This condition was documented in a product discrepancy report. IOM made a determination this anomaly did not affect the safety function of the modules, but was a source of nuisance alarms.

The IOM "Technical Advisory Bulletin #183, Intermittent Inter-Leg Register Faults on Specified Tricon I/O Modules," Revision 1, 9791006-183, dated February 21, 2011 (Reference 210), was issued to users of these modules to communicate operational restrictions and recommended actions to address the problem with installed modules by resetting faults. This Technical Advisory Bulletin also states the problem has been resolved. The anomaly was determined not to be reportable per 10 CFR Part 21 because this problem did not affect execution of the safety function within affected modules.

The "Tricon V10.5.2, Engineering Project Plan," Revision 1.4 (Reference 209) delineates the engineering actions, deliverables, and responsible individuals associated with the Tricon V10.5.2 project. It prescribes the detailed engineering development, verification, validation, certification, and documentation activities required to correct the problem and revise the software for the affected modules (3625N, 3720, and 3721N). The NRC staff reviewed the Engineering Project Plan and concludes that it prescribes a process consistent with the NRC approved Triconex development procedures. The NRC staff also reviewed the "Software Requirements Specification (SRS)," Revision 4, 993754-11-809-P, dated January 21, 2014 (Reference 166), and verified the resultant changes had been included in the SRS for the modules affected by revision V10.5.2. The NRC staff observed that verification and validation (V&V) of V10.5.2 software changes is documented in the Tricon V10.5.2, V&V Test Report, which includes the test results. All prescribed V&V tests were conducted with acceptable results.

All Tricon configurations undergo an external, independent review and testing by TÜV Rheinland. As part of the independent review, TÜV Rheinland assesses process changes and performs full V&V, including source code reviews in accordance with International Electrotechnical Commission (IEC) 61508.

The NRC staff's review of the Tricon V10.5.2 V&V Test Report determined IOM used independent, external reviews of the design and testing activities for this change. TÜV Rheinland reviewed all Tricon V10.5.2 project documents and issued a confirmation letter, which states that Tricon 10.5.2 is certified against IEC 61508. An additional external, independent review was performed by Wurldtech. Wurldtech performed a review of the Tricon V10.5.2 project documents and issued its certification.

The NRC staff verified the proper module versions of the V10.5.2 software were released in January 2011 with "Tricon V10.5.2 Release, Software Release Definition" (Reference 208). The NRC staff further verified Tricon V10.5.2 was added to the Nuclear Qualified Equipment List.

Maintenance Release V10.5.3

The NRC staff reviewed the "Tricon PAN 25 Fix, Engineering Project Plan," Revision 1.2, 9100428-001, dated October 12, 2011 (Reference 211); the "Tricon PAN25 Master Test Report," Revision 1.0, dated October 12, 2011 (Reference 212); and "Tricon V10.5.3, Software Release Definition," Revision 1.0, 6200003-230, dated September 28, 2011 (Reference 213), for this release. The V10.5.3 upgrade was initiated by IOM to resolve a potential safety issue, which was discovered in Tricon digital output modules (3625N). A condition of spurious output transitions in the 3625 series digital output modules under certain circumstances was reported. The nuclear qualified digital output module 3625N was one of the affected modules. The condition was documented in a product discrepancy report (IRTX#22481) and was assigned as Criticality 1, which means this condition can "Impact System Safety."

As required by the Triconex quality assurance program, "Product Alert Notice #25—Potential Safety Issue," Revision 2, 9791010-025, dated October 12, 2011 (Reference 214), was issued to alert customers of this condition and proposed appropriate compensatory actions. Product Alert Notice (PAN) 25 lists system versions for which the problem has been resolved. A revision to the digital output module firmware was required to eliminate the cause of the potential spurious transitions. As documented in the Tricon PAN 25 Fix, Engineering Project Plan, this anomaly was determined not to be reportable per 10 CFR Part 21 because this condition could not cause substantial safety hazard given the limited conditions for which the anomaly would manifest itself and the effectiveness of the prescribed measures in PAN 25. This issue does not affect the DCPP PPS because the system uses V10.5.3.

The Tricon PAN 25 Fix, Engineering Project Plan delineates the engineering actions, deliverables, and responsible individuals associated with the Tricon V10.5.3 project. It prescribes the detailed engineering development, verification, validation, certification, and documentation activities required to correct the problem and revise the software for the 3625 series digital output module, including the 3625N. The NRC staff reviewed the Engineering Project Plan and concludes that it prescribes a process consistent with the NRC-approved Triconex development process procedures. The NRC staff reviewed the "Software Requirements Specification (SRS)" (Reference 166), and verified changes had been included in the SRS for the modules affected by revision V10.5.3. The NRC staff observed verification and validation of V10.5.3 software changes was appropriately documented in the Tricon PAN 25 Master Test Report, Revision 1.0. This test report documents the test results for tests performed during the Verification and Validation of the PAN 25 resolution as delineated in the Tricon PAN 25 Fix, Master Test Plan, and provides a recommendation to release the software module. All specified V&V tests were conducted with acceptable results.

The NRC staff's review of the Tricon PAN 25 Master Test Reports also determined IOM used an independent, external review resource for the design and testing activities associated with this change. TÜV Rheinland reviewed all Tricon PAN 25 project documents and issued a confirmation letter, which states Tricon 10.5.3 is certified against IEC 61508.

The NRC staff verified the proper module versions of the V10.5.3 software were released with the Tricon V10.5.3, Software Release Definition. The NRC staff further verified Tricon V10.5.3 was added to the Nuclear Qualified Equipment List.

TriStation 1131 Application Software Change V4.9.0

Tricon V10.5.3 includes an updated version of the TriStation 1131 programming software. The Tricon V10.5.1 system was originally released with TriStation 1131 V4.7.0. This programming software suite has since been upgraded to correct performance issues and has been made available as TriStation 1131 V4.9.0 for use in Tricon V10.5.3 systems.

The TriStation 1131 V4.9.0 upgrade project was initiated to resolve accumulated product discrepancy reports and to add minor functional improvements to the TriStation and Safety Suite Applications product. The TriStation 1131 V4.9.0 change did not add any new features, but provided enhancements to existing features. Therefore, the TriStation 1131 V4.9.0 maintains the features described in the Tricon V10 safety evaluation for the Triconex Approved Topical Report (Reference 29).

The "TriStation V4.9.0 and Safety Suite Apps, Engineering Project Plan," Revision 1.3, 9100359-001, dated June 13, 2011 (Reference 215), identifies the engineering actions, deliverables, and responsible individuals associated with the TriStation 1131 V4.9.0 project. It prescribes the detailed engineering development, verification, validation, certification, and documentation activities required to correct the problems documented in product alert notices, and to revise the TriStation 1131 software. The NRC staff reviewed the Engineering Project Plan and it prescribes a process consistent with the NRC-approved Triconex development process procedures, and contains a complete list of deliverables for the project with regard to the software changes and enhancements.

The NRC staff observed verification and validation (V&V) of TriStation V4.9.0 software changes were appropriately documented in the "TriStation 1131 V4.9.0 Test Report," Revision 0.4, dated May 16, 2011 (Reference 216). This test report documents the successful test results of all tests performed during verification and validation of the problems documented in product alert notices, as delineated in the TriStation 1131 V4.9.0 V&V Test Plan, and provides a recommendation to release the software module. All specified V&V tests were conducted with acceptable results.

The NRC staff verified proper versions of the TriStation V4.9.0 software were released with the "TriStation 1131 v4.9.0.117 SRD Software Release Definition," Revision 1.2, 6200097-038, dated August 23, 2011 (Reference 217). The NRC staff further verified TriStation V4.9.0 was subsequently added to the Nuclear Qualified Equipment List.

3.8.4 Development Process Changes

The regulations in 10 CFR 50.55(i) require, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. Standard Review Plan (SRP) Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems" (Reference 218), Section 3.H, "Review of the Acceptance of Commercial-Grade Digital Equipment," states, in part, that "All software, including operating systems, that is resident on safety system computers at run time must be qualified for the intended applications. Qualification may be established either by producing the [predeveloped software (PDS)] items under a 10 CFR Appendix B quality assurance program or by dedicating the item for use in the safety system as defined in 10 CFR 21."

The NRC staff approved the Tricon V10 system developmental processes in its safety evaluation for the Triconex Approved Topical Report (Reference 29), which included process changes from those approved in the V9 Tricon safety evaluation dated December 11, 2011 (Reference 219). The IOM development process is contained in three IOM documents governing Invensys Operations Management (IOM) internal development; the Quality Assurance Manual (QAM), Quality Procedure Manual (QPM), and the Engineering Department Manual (EDM).

In developing the Tricon V10.5.3 system, several changes, additions, and deletions were made to the development process. Changes to these IOM developmental process documents governing IOM internal development processes are described below.

<u>V10.5.2 and V10.5.3 Software Development Process Changes</u>

The NRC staff reviewed each of the IOM development process procedure changes and determined these changes were either editorial, clarified/strengthened existing development processes, or reflect stronger conformance to industry and International Electrotechnical Commission (IEC) standards.

The NRC staff identified no reduction in previous commitments in these changes. No other IOM development process procedures applicable to the V10.5.2 and 10.5.3 software upgrades were changed or discussed.

The Tricon V10.5.2 and V10.5.3 platform software changes were developed using the same high quality design and development process used to develop the original Tricon V10.5.1 software components. The development process was approved in the NRC staff's December 11, 2001, safety evaluation on the original Tricon V9 topical report (Reference 219) and updated as appropriate in the Tricon V10.5.1 topical report safety evaluation for the Triconex Approved Topical Report (Reference 29). Based on the information reviewed by the NRC staff, the Tricon V10.5.2 and V10.5.3 platform software changes meet the operational and safety requirements for the DCPP PPS application and are acceptable for use in safety-related applications at nuclear power plants.

3.9 <u>Conformance with IEEE Std. 603-1991, "IEEE Standard Criteria For Safety Systems for Nuclear Power Generating Stations"</u>

3.9.1 IEEE 603-1991, Clause 4, Design Basis

Because the Tricon and Advanced Logic System (ALS)-based process protection system (PPS) is replacing the existing Eagle 21 PPS, its established specific basis is the same basis which was credited for the existing system approved in NRC staff letter dated October 7, 1993 (Reference 23). This basis consists of the plant accident analysis and technical specifications. The licensee performed an evaluation of the revised PPS design and determined that the replacement system continues to meet the requirements set forth in the Final Safety Analysis Report Update (FSARU) Chapter 15, "Accident Analyses" (Reference 52).

The NRC staff was able to access the design basis documents for the plant in order to determine the adequacy of the replacement PPS. The NRC staff determined the established basis for the replacement PPS remains consistent with the plant's design basis.

3.9.1.1 IEEE 603-1991, Clause 4.1, Identification of the Design Basis Events

This item requires that the design basis documentation include the safety functions and corresponding protective actions of the execute features for each design basis event.

The DCPP safety functions and corresponding protective actions of the execute features for each design basis event for the PPS are unchanged as a result of the system upgrade; therefore, no evaluation was performed with respect to the documentation of the safety functions and protective actions.

3.9.1.2 IEEE 603-1991, Clause 4.2, Identification of Safety Functions and Protective Actions

This item requires that the design basis documentation include the safety functions and corresponding protective actions of the execute features for each design basis event.

The DCPP safety functions and corresponding protective actions of the execute features for each design basis event for the PPS are unchanged as a result of the system upgrade; therefore, no evaluation was performed with respect to the documentation of the safety functions and protective actions.

3.9.1.3 IEEE 603-1991, Clause 4.3, Permissive Conditions for Operating Bypasses

This item requires that the design basis documentation include the permissive conditions for each operating bypass capability that is to be provided.

The modifications being made to the PPS do not change the bypass designs as described in the DCPP FSARU; therefore, no evaluation was performed with respect to the documentation of the permissive conditions for operating bypass. The permissive conditions for operating bypasses are defined in the PPS replacement project specifications. The NRC staff therefore determined that the requirements of Clause 4.3 are satisfied.

3.9.1.4 IEEE 603-1991, Clause 4.4, Identification of Variables Monitored

This item requires that the design basis documentation include 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 assured.

The safety variables and analytical limits that are to be monitored have not been changed as a result of the PPS upgrade; therefore, no evaluation was performed with respect to the documentation of the variables monitored and the analytical limits. System response times, accuracies, and setpoints did, however, require evaluation to determine if changes resulting from the PPS modification would impact proper completion of the PPS-required protective actions.

The setpoint calculations for the PPS replacement are contained in the "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," WCAP-17696-P, Revision 0, January 2013 (Reference 220), using the setpoint methodology contained in the "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," Revision 0, WCAP-17706-P, January 2013 (Reference 221). The setpoint calculations show a margin between all trip setpoints and the respective analytical limits. This is intended to assure acceptable completion criteria for all of the affected protective functions.

The PPS functional requirements specification provides additional details regarding setpoint calculations including response time requirements for all PPS safety input functions. The NRC staff determined that the requirements of Clause 4.4 are satisfied.

3.9.1.5 IEEE 603-1991, Clause 4.5, Minimum Criteria for Manual Protective Actions

This item requires that the design basis documentation include the minimum criteria for each protective action in Clause 4.2 whose operation may be controlled by manual means initially or subsequent to initiation.

The DCPP reactor protection system and engineered safety features actuation system include manual controls for the system-level reactor trip actuation and the channel and component level actuations of the engineering safeguards equipment. The PPS replacement project does not alter the system-level manual actuation configuration performed by the solid state protection system.

None of the following will be impacted by the PPS replacement:

- System environmental criteria,
- Information available to the operator,
- Justification for allowing manual control, and
- Time responses discussed in the safety analysis.

The NRC staff determined that the replacement PPS design meets the requirements of Clause 4.5.

3.9.1.6 IEEE 603-1991, Clause 4.6, Identification of the Minimum Number and Location of Sensors

This item requires that the design basis documentation include, for those sensors in Clause 4.4, that have spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and location of sensors required for protective purposes.

With the exception of activation of previously spare resistance temperature detector sensors, the existing sensors required for protective purposes have not changed in number or location. Therefore, the spatial dependence of the system sensors has not been affected by the PPS replacement. The NRC staff determined that the replacement PPS complies with the requirements in Clause 4.6 for the minimum number and location of sensors.

3.9.1.7 IEEE 603-1991, Clause 4.7, Range of Transient and Steady-State Conditions

This item requires that the design basis documentation include the range and steady-state transient 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.

Both of the replacement digital platforms, Tricon and ALS, are located in the same cabinets that house the existing Eagle 21 PPS. Therefore, the environmental conditions experienced by the modified PPS will remain the same.

The range of transient and steady-state conditions during normal, abnormal, and accident conditions will not be affected as a result of the PPS modification. Therefore, no evaluation was performed with respect to the documentation of the range of transient and steady state conditions. The PPS replacement equipment is qualified to operate in the existing plant environmental conditions.

3.9.1.8 IEEE 603-1991, Clause 4.8, Conditions Causing Functional

This item requires that the design basis documentation include 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.

The replacement PPS equipment will be located in the same room as the existing Eagle 21 PPS. The installation of the replacement PPS will not change any of the provisions, or associated conditions, that are documented as part of the plant design basis. Since the location of the new system is the same as the old system, no new conditions having the potential for causing degradation are being introduced.

The replacement PPS is also qualified to operate within the environmental conditions that may exist during any accident or transient that requires the PPS to perform a safety function. The NRC staff therefore, determined that the modified PPS complies with the requirements of Clause 4.8.

3.9.1.9 IEEE 603-1991, Clause 4.9, Methods Used to Determine Adequate Reliability of the Safety System

This item requires that the design basis documentation include the methods used to determine that the reliability of the safety system design is appropriate for the safety systems design and any qualitative or quantitative goals that may be imposed on the system design.

The methods used to determine reliability for each of the DCPP PPS platforms is described as follows:

Tricon

In Section 2.2.12, "Reliability and Availability Analysis," of the Triconex Approved Topical Report (Reference 29), 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.

ALS

The reliability numbers in the Advanced Logic System Topical Report (Reference 30) were calculated for each of the platform's seven different types of modules.

The methods used for determining reliability of each of these platforms was based on the establishment of quantitative goals that were specified by the licensee. The licensee has specified that high reliability will be achieved in the PPS by using high-quality components arranged in independent redundant channels. The NRC staff concludes that the reliability goals and the methods employed by the platform vendors to meet these goals were appropriate and were determined to provide an adequate means of meeting the performance requirements of the PPS. Based on the above, the NRC staff determined that the modified PPS complies with the requirements of Clause 4.9.

3.9.1.10 IEEE 603-1991, Clause 4.10, Control after Protective Actions

This item requires that the design basis documentation include the critical points in time or plant conditions, after the onset of the design basis event, including the point in time or plant conditions (1) for which the protective actions of the safety system shall be initiated, (2) that define the proper completion of the safety function, (3) that require automatic control of protective actions, and (4) that allow returning the safety system to normal.

The replacement PPS does not modify the existing design basis critical points in time or plant conditions where the protective actions of the safety system are required to be initiated.

The point in time where the protective action is required is determined by the setpoint for that protective action. The completion of the protective action is determined by the response time, and this is specified in the PPS functional requirements specification. The definition of proper completion of the safety function, the required automatic control of protective actions, and the determination of when the safety system may be returned to normal will not change as a result of this modification. The NRC staff therefore determined that the replacement PPS complies with the requirements of Clause 4.10.

3.9.1.11 IEEE 603-1991, Clause 4.11, Equipment Protective Provisions

This item requires that the design basis documentation include 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 system that would prevent the safety systems from accomplishing their safety functions. Several new features are being introduced to the design of the replacement PPS to ensure that safety functionality of the PPS will be maintained.

Signal validation is required for the over power delta temperature and over temperature delta temperature channels. Input range checking is performed for all PPS input channels. This includes out of range high and low setpoints. Both 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. The NRC staff therefore determined that the replacement PPS complies with the requirements of Clause 4.11.

3.9.1.12 IEEE 603-1991, Clause 4.12, Special Design Bases

This item requires that the design basis documentation include any other special design basis provisions that prevent the safety systems from accomplishing their safety functions.

The only special design basis item that has been implemented with the replacement PPS concerns the inclusion of a new diversity and defense-in-depth (D3) evaluation. The licensee chose to eliminate the need for certain diverse manual actuations for the events where an operator's timed response was determined to be too short. Automatic mitigation functions will be initiated by the independent, diverse ALS portion of the PPS replacement for events that previously required manual operator action for mitigation of a design basis event concurrent postulated common-cause failure of the PPS. Since the DCPP PPS relies upon this ALS diversity feature to perform its safety function in conjunction with a software common-cause failure, the DCPP FSARU will be updated to reflect this revised PPS design basis which will meet the requirements of Clause 4.12, Item 1.

The updated PPS D3 evaluation has been approved by the NRC and is included in the design basis for the replacement PPS. The NRC staff therefore determined that the replacement PPS complies with the requirements of Clause 4.12.

3.9.2 IEEE 603-1991, Clause 5, System

This clause requires that safety systems, 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 are required to be comprised of more than one safety group of which any one safety group can accomplish the safety function.

The precision aspects of the PPS for safety-related functions are addressed by the signal processing of input signals associated with the initiation of safety functions. Signal processing requirements are specified in the system functional requirements specification and once implemented, are verified during the system validation and factory acceptance testing activities.

The PPS consists of multiple redundant protection sets. Electric power to these protection sets is also supplied by redundant sources. Each protection set is capable of providing the initiation signals needed to accomplish safety functions required by the plant accident analysis. The PPS is therefore considered to be comprised of more than one safety group and each of these safety groups are capable of providing the necessary actuation signals to the solid state protection system to accomplish the required safety functions.

3.9.2.1 IEEE 603-1991, Clause 5.1, Single-Failure Criterion

This clause requires that the safety system be able to perform its safety function 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.

In Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.1, "Single Failure Criterion" (Reference 41), provides acceptance criteria for the single-failure criterion, including Regulatory Guide (RG) 1.53, Revision 2, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," November 2003 (Reference 60), which endorses IEEE Std. 379-2000, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 61).

A system-level failure modes and effects analysis (FMEA) was performed to provide a basis for conformance to the single-failure criterion. The FMEA is described and evaluated in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation. The NRC staff determined that the PPS FMEA adequately demonstrates that the PPS will remain capable of performing its required safety functions when postulated single failures of the system occur. The NRC staff also reviewed the diversity and defense-in-depth (D3) analysis in Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation and determined that D3 analysis provides reasonable assurance that the modified PPS will meet single-failure criterion. Based on the evaluations referenced above, the NRC staff determined that the replacement PPS complies with the requirements of Clause 5.1.

3.9.2.2 IEEE 603-1991, Clause 5.2, Completion of Protective Action

This clause states 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. In SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.2, "Completion of Protective Action," provides acceptance criteria for this requirement.

In request for additional information (RAI) 56 dated March 31, 2014 (Reference 190), the NRC requested that the licensee provide information to support the compliance of the PPS safety systems with these criteria. By letter dated April 30, 2014 (Reference 17), the licensee provided information for functions which use the solid state protection system for actuation. The PPS compares plant parameters against protective setpoints and provides discrete actuation signals to the solid state protection system, whose logic is not affected by the PPS replacement. For these safety functions, it is the solid state protection system logic which ensures completion of protection action upon receipt of actuation signal.

The NRC staff reviewed the functional requirements of the replacement PPS and concludes that completion of protective action functions are not being implemented in the PPS portion of the safety systems. Instead, functions to ensure that automatic protective action signals remain active when the conditions for safety function initiation subsequently clear are performed by systems that are not being modified as part of the PPS replacement.

Tricon

The Tricon portion of the PPS uses a scan-based architecture designed so that, once initiated, the protective action proceeds to completion. Interrupts are not used and return to normal operation requires deliberate operator action.

ALS

The ALS portion of the PPS does not require manual intervention or acknowledgment of actuation commands to complete a protective action.

Manual initiation of safety functions is accomplished by the downstream solid state protection system which is not being modified by the PPS modification; however, the NRC staff confirmed that these functions do meet the completion of the protective function criteria.

The NRC staff confirmed that the reactor trip system and engineered safety feature actuation system design with incorporation of the replacement PPS requires deliberate operator action to return safety system components to a non-actuated state. The NRC staff therefore determined that the replacement PPS complies with the requirements of Clause 5.2.

3.9.2.3 IEEE 603-1991, Clause 5.3, Quality

This clause states that the components and modules within the safety system 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 plan. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.3, "Quality," provides acceptance criteria for the quality requirement. This acceptance criteria states that the quality assurance provisions of 10 CFR 50, Appendix B, apply to a safety system.

Criterion 1, 1967, "Quality Standards" of the DCPP FSARU states that "(t)hose systems and components of reactor facilities that are essential to the prevention of accidents which could affect the public health and safety, or mitigation of their consequences, shall be identified and then designed, fabricated, and erected to quality standards that reflect the importance of the safety function to be performed. Where generally recognized codes or standards on design, materials, fabrication, and inspection are used, they shall be identified. Where adherence to such codes or standards does not suffice to ensure a quality product in keeping with the safety functions, they shall be supplemented or modified as necessary. Quality assurance programs, test procedures, and inspection acceptance levels to be used shall be identified. A showing of sufficiency and applicability of codes, standards, quality assurance programs, test procedures, and inspection acceptance levels used is required."

The licensee has an NRC-approved 10 CFR Part 50, Appendix B, Quality Assurance Program. The licensee has audited each of the platform vendors and maintains Invensys and Westinghouse on its approved Appendix B suppliers list. During the design, development, and testing of the replacement PPS, the licensee has conducted oversight activities. The approval of the Tricon and ALS platform topical reports confirmed that the platform components are of adequate quality and meet the acceptance criteria of SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality." These determinations meet the guidance acceptance criteria in SRP Chapter 7, Appendix 7.1-C, Section 5.3, "Quality"; therefore, the replacement PPS conforms to the requirements of Clause 5.3, as explained in the subsections below.

3.9.2.4 IEEE 603-1991, Clause 5.4, Equipment Qualification

This clause states that safety system equipment 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. Acceptance criteria for IEEE Std. 603-1991, Clause 5.4 are provided in SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.4, "Equipment Qualification." This acceptance criteria states that the applicant/ licensee should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. Regulatory Guide 1.89, Revision 1, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Revision 1, June 1984 (Reference 65), endorses and provides guidance for compliance with IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations" (Reference 66).

Tricon

Seismic qualification of the Tricon equipment involved type tests that were performed and evaluated during the NRC's platform evaluation. These tests included a resonance search followed by five simulated Operating Basis Earthquakes and one simulated Safe Shutdown Earthquake at 9.75 g and 14 g, respectively. These tests were based on a damping factor of 5 percent. The simulation vibrations were applied triaxially and included a random frequency content. Several additional test requirements were applied and these are listed in the Section 2.2.4, "Seismic Qualification," of the Triconex Approved Topical Report (Reference 29). The representative test Tricon system remained operational throughout these tests and was capable of meeting its performance requirements during and following the application of the simulated Operating Basis Earthquakes and the Safe Shutdown Earthquake.

The test system alarm relay contacts were not monitored in a manner to ensure that contact chatter did not occur during the tests; therefore, the chassis alarm relays are not considered to be seismically qualified. The NRC verified that the alarm relays used in the PPS are not relied upon for the performance of any PPS safety function.

ALS

The physical requirements for the DCPP PPS replacement equipment are specified to the vendors in the DCPP Functional Requirements Specification, Revision 7 (Reference 126). Physical requirements specified include temperature, relative humidity, pressure, radiation, seismic, electromagnetic capability, and emissions. The vendor requirements traceability matrix documents contain the basis for how the equipment meets the physical requirements of the DCPP Functional Requirements Specification.

An evaluation of the PPS replacement system equipment qualification is provided in Section 3.5, "Equipment Environmental Qualification," of this safety evaluation. The NRC staff has determined that the PPS equipment qualifications adequately demonstrate that the replacement PPS is capable of meeting its functional performance requirements over the range of normal and worst-case accident environmental conditions to be expected in the DCPP cable spreading room. Based on the above, the replacement PPS meets the requirements of Clause 5.4.

3.9.2.5 IEEE 603-1991, Clause 5.5, System Integrity

This clause states that the safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.5, "System Integrity," provides acceptance criteria for system integrity. This acceptance criteria states that the NRC staff should confirm that tests have been conducted on safety system equipment components and the system racks and panels as a whole to demonstrate that the safety system performance is adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment. Ensure that test shows that if the system does fail, it fails in a safe state, and that failures detected by self-diagnostics should also place a protective function into a safe state.

The replacement PPS will be installed inside the DCPP cable spreading room. The review discussed in Section 3.5, "Equipment Environmental Qualification," of this safety evaluation has determined that the replacement PPS is qualified for that environment. The cable spreading room envelope is maintained in an ambient mild environment during normal and accident conditions. The installation of the replacement PPS will not change any of the provisions, and associated conditions, that are documented as required by IEEE Std. 603, Clause 4. The equipment qualification, evaluated in Section 3.5 of this safety evaluation, provides reasonable assurance that the replacement PPS is capable of performing its safety functions over the full range of environmental conditions that may exist during the worst-case design basis event during which the safety functions are required.

The NRC staff review confirmed that the failure modes and effects analysis provide reasonable assurance that an input signal or system failure, including power supply or input power failure, will cause the PPS to fail in the predefined safe state and annunciate that failure to the operators. Further, the NRC staff review confirmed the self-diagnostic features and tests performed by the ALS and Tricon platforms will place the PPS into a safe state and will annunciate failure status to the operators. The NRC staff has, therefore, determined that there is reasonable assurance that the replacement PPS meets the criteria of Clause 5.5.

3.9.2.6 IEEE 603-1991, Clause 5.6, Independence

3.9.2.6.1 IEEE 603-1991, Clause 5.6.1, Between Redundant Portions of a Safety System

This clause states that the safety systems be designed such that there is sufficient independence between redundant portions of a safety system such that the redundant portions are independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.

The replacement PPS design consists of four independent protection sets. Each of these protection sets is physically separated and electrically isolated from the other protection sets. The replacement PPS does not incorporate any communications links or data sharing features between redundant protection sets.

Each PPS protection set has dedicated sensors that provide analog input signals needed to accomplish safety functions. Electrical independence between redundant portions of the PPS is provided for by using diverse power supplies and separation of cabling. Each PPS protection set is powered from a separate vital 120 Volts alternating current (VAC) bus. Cables associated with the four PPS protection sets are routed in separate cable trays. The requirement for physical isolation, between redundant portions of the PPS, is met by the physical arrangement of each protection set within separate cabinets.

The NRC staff determined that there is sufficient independence between redundant portions of the replacement PPS and, therefore, the replacement PPS meets the requirements of Clause 5.6.1.

3.9.2.6.2 IEEE 603-1991, Clause 5.6.2, Between Safety Systems and the Effects of Design Basis Event

This clause states that the safety system equipment required to mitigate the consequences of a specific design basis event be independent of, and physically separated from, the effects of a specific design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Clause 5.6.2 further states that equipment qualification in accordance with Clause 5.4 is one method that can be used to meet this requirement.

Criterion 20, 1967, "Protection systems redundancy and independence," of the DCPP FSARU requires that "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."

The NRC staff reviewed the equipment qualifications of the replacement PPS and determined this qualification demonstrates sufficient independence between the replacement PPS and effects of design basis events. The digital PPS is capable of mitigating the consequences of design basis events, and is sufficiently physically separated from the effects of the design basis events. The NRC staff therefore determined the replacement PPS meets the requirements of Clause 5.6.2.

3.9.2.6.3 IEEE 603-1991, Clause 5.6.3, Between Safety Systems and Other Systems

This clause states that the safety systems be designed such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of this standard. This requirement is subdivided into requirements for interconnected equipment, equipment in proximity, and the effects of a single random failure. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, does not provide any additional acceptance criteria beyond that in Clause 5.6.3.

The three subsections below document the evaluation of interconnected equipment, equipment in proximity, and the effects of a single random failure separately. The NRC staff evaluated the communication independence between the replacement PPS and other systems (see Section 3.7, "Communications," of this safety evaluation). Security aspects of the Clause 5.6.3 were evaluated by the NRC staff (see Section 3.12, "Secure Development and Operational Environment," of this safety evaluation). Based on these evaluations, the NRC staff determined that the replacement PPS meets the requirements of Clause 5.6.3.

3.9.2.6.3.1 IEEE 603-1991, Clause 5.6.3.1, Interconnected Equipment

This clause states that equipment that is used for both safety and non-safety functions, as well as the isolation devices used to affect a safety system boundary, shall be classified as part of the safety systems. This clause further states 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, and that a failure in an isolation device will be evaluated in the same manner as a failure of other equipment in a safety system.

Some components of the replacement PPS such as the maintenance work station (maintenance work station) are classified as non-safety-related. The NRC staff confirmed that none of these devices are used for the accomplishment of any of the PPS safety functions. Since all other components of the PPS are classified as safety-related, the replacement PPS meets the requirements of Clause 5.6.3.1.

The effect of isolation device failures is considered in the system level failure modes and effects analysis (FMEA) for the PPS (see Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation). The PPS Tricon and ALS subsystems are protected from high current in the interfacing non-safety systems. Because isolation devices used in the PPS are classified as safety-related, they are evaluated for failures in the same manner as the other safety-related components of the PPS.

3.9.2.6.3.2 IEEE 603-1991, Clause 5.6.3.2, Equipment in Proximity

This clause states 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. This clause further states that the physical barriers used to effect a safety system boundary shall meet the requirements of Clauses 5.3, "Quality," 5.4, "Equipment Qualification," and 5.5, "System Integrity," for the applicable conditions specified in Clauses 4.7 and 4.8 of the design basis.

The existing 16 cabinets housing the Eagle 21 PPS will be retained and the replacement PPS components will be installed into them. The need for physical isolation is met by the physical arrangement of each PPS protection set within separate sets of cabinets. Each of the four PPS protection sets (A, B, C, and D) will occupy a single set of cabinets (five cabinets each for protection sets A and B, and three cabinets each for protection sets C and D). Physical separation is maintained between redundant PPS protection sets by the cabinet and cable layouts.

Outside the PPS cabinets, vital signals and wiring are separated and physically protected to preserve channel independence and maintain system redundancy against physical hazards.

System sensors are physically separated from each other. The arrangement of system sensors and field wiring is not changed by the proposed design change.

The replacement PPS protection sets are installed in separate safety-related cabinets within the cable spreading room. There is no change in the physical proximity or separation of these cabinets. These cabinets and their location ensure that there is no equipment in other systems that are in physical proximity to the PPS equipment that performs the safety functions.

3.9.2.6.3.3 IEEE 603-1991, Clause 5.6.3.3, Effects of a Single Random Failure

This clause states that where a single random failure in a non-safety system can result in a design basis event, and 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.

Sections 3.5, "Equipment Environmental Qualifications," and 3.9.2.4, "IEEE 603-1991, Clause 5.4, Equipment Qualification," of this safety evaluation evaluate the ability of the replacement PPS to function in all anticipated operating environments, including those present during design basis events. Section 3.9.2.6.1, "IEEE 603-1991, Clause 5.6.1, Between Redundant Portions of a Safety System," and 3.9.2.6.2, "IEEE 603-1991, Clause 5.6.2, Between Safety Systems and the Effects of Design Basis Event," of this safety evaluation document the evaluations that the replacement PPS will function independently of credible failures in interconnected equipment and equipment in proximity to the PPS.

There are no single random failures of non-safety systems that can result in a design basis event, and also prevent proper action of the DCPP safety systems designed to protect against that event; therefore, the replacement PPS complies with the criteria of Clause 5.6.3.

3.9.2.7 IEEE 603-1991, Clause 5.7, Capability for Test and Calibration

This clause states that the safety system shall have the capability for test and calibration while retaining the capability to accomplish its safety function, and that this capability be provided during power operation, and shall duplicate, as closely as practicable, performance of the safety function. 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; however, appropriate justification shall be provided, acceptable reliability of equipment operation shall demonstrated, and the capability shall be provided while the generating station is shut down.

In SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.7, "Capability for Test and Calibration" (Reference 41), provides acceptance criteria for IEEE Std. 603-1991, Clause 5.7. It states that guidance on periodic testing of the safety system is provided in Regulatory Guide (RG) 1.22, Revision 0, "Periodic Testing of Protection System Actuation Functions," February 1972 (Reference 58), and in RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," April 1995 (Reference 69), that endorses IEEE Std. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems" (Reference 70). Clause 5.7 acceptance criteria states that periodic testing should duplicate, as closely as practical, the overall performance required of the safety system, and that the test should confirm operability of both the automatic and manual circuitry. This capability should be provided to permit testing during power operation and that when this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Clause 5.7 further states that test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. Clause 5.7 further states that for digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and computer lockup.

Standard Review Plan (SRP) Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions," March 2007 (Reference 47), describes additional considerations in the evaluation of test provisions in digital computer-based systems. The self-test features associated with the replacement PPS are evaluated in Section 3.10, "Conformance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," of this safety evaluation.

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. The Tricon and ALS platform self-tests and the application-specific test and calibration functions are performed during the system factory acceptance testing to verify the safety function is not adversely affected by performance of built-in or application-specific test and calibration functions.

Process protection system (PPS) periodic testing includes channel calibrations. The channel calibrations can be performed online using the bypass capability of the channel or during refueling outages when the PPS is not required to be operable.

When on-line testing is required for system maintenance, the PPS replacement design allows for testing without disconnecting wires, installing jumpers, or otherwise modifying the installed equipment. Simulated signal inputs into a protection channel can be applied using measuring and test equipment. During performance of testing or maintenance of the PPS replacement, affected channels may be placed into the bypass mode.

Considering the system testing and calibration features described above, the NRC staff determined that replacement PPS design has sufficient capability for performance of testing and calibration during power operation. The NRC staff also determined that the test methods described in the license amendment request adequately duplicate the performance of the system safety functions to provide reasonable assurance these functions can be maintained in an operable state during plant power operations.

3.9.2.8 IEEE 603-1991, Clause 5.8, Information Displays

This clause contains no requirements, but has four subclauses that do contain requirements that were used to evaluate the replacement PPS in the subsections below. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, Section 5.8, "Information Displays" (Reference 41), provides further review guidance for Clause 5.8.

3.9.2.8.1 IEEE 603-1991, Clause 5.8.1, Displays for Manually Controlled Actions

This clause states that 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 will be part of the safety systems. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.

The replacement PPS supplies signals to several display instruments used to support manual control actions. These functions are being implemented in a manner which duplicates the display functions that are currently being performed by the Eagle 21 PPS. As such, no change to existing display functionality or introduction of new display functionality is being implemented with this modification.

The display instruments 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 included as part of the DCPP safety systems.

The NRC staff reviewed the indications provided by PPS functions and determined that safety system manual control actions are adequately supported by these indications. The NRC staff also determined that PPS-supported indications provide information to plant operators in an unambiguous format which supports successful completion of all required safety functions. The replacement PPS therefore complies with the criteria of Clause 5.8.1.

3.9.2.8.2 IEEE 603-1991, Clause 5.8.2, System Status Indication

This clause states that display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. It also states that this information shall include indication and identification of protective actions of the sense and command features and execute features. Clause 5.8.2 further states that the design minimize the possibility of ambiguous indications that could be confusing to the operator; however, the display instrumentation provided for safety system status indication need not be part of the safety systems.

The display instruments used for indicating protective actions of the sense and command features and execute features associated with the PPS are primarily associated with inputs and outputs of the solid state protection system (SSPS), which are not being modified by the PPS replacement. The status of all actuated components is indicated on the control boards together with the control switches that are provided for the individual safety system components.

The NRC staff determined that the replacement PPS status indications as provided by safety system components remains accurate, complete, and timely, and meets the requirements of IEEE Std. 603 Clause 5.8.2.

3.9.2.8.3 IEEE 603-1991, Clause 5.8.3, Indication of Bypasses

This clause states 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, then continued indication of this fact for each affected safety group shall be provided in the control room. Clause 5.8.3 further states that this display instrumentation need not be part of the safety systems; that this indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable; that the capability shall exist in the control room to manually activate this display indication; and that the information displays shall be located accessible to the operator. Regulatory Guide (RG) 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," February 2010 (Reference 59), describes an acceptable method of complying with the requirements of Clause 5.8.3.

The NRC staff reviewed the replacement PPS functional requirements relating to channel bypass. Only containment high-high pressure to initiate containment spray and turbine impulse pressure high for activation of P-13 signals are explicitly required to have channel bypass capability. The NRC staff confirmed that placing any of these PPS channels into bypass will automatically cause a main annunciator system annunciation to alert the operator of this condition. The staff also confirmed that this main annunciator system alarm remains in the alarm state until the associated channel is removed from bypass and restored to operation. Further review of the PPS design revealed that several other PPS safety functions were provided with similar channel bypass capabilities. The NRC staff confirmed that these additional bypass functions conformed to the criteria of this clause by providing continuous bypassed and inoperable status indication when placed in the bypass mode of operation. The main annunciator system alarm displays are always active in the main control room; therefore, no manual activation is necessary.

The NRC staff concludes that the channel bypass functions are being implemented in a manner which is consistent with the criteria of this clause. Therefore, the replacement PPS meets the requirements of Clause 5.8.3.

3.9.2.8.4 IEEE 603-1991, Clause 5.8.4, Location

This clause states that the information displays shall be located accessible to the operator and that information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.

The locations of the control board indications are not changing as a result of the PPS replacement and will remain accessible to the operators. Information displays in the control room are part of the safety systems and are unchanged from those approved for the Eagle 21 PPS. The NRC staff determined that the replacement PPS meets the requirements of Clause 5.8.4.

3.9.2.9 IEEE 603-1991, Clause 5.9, Control of Access

This clause states that the safety system shall be designed to permit administrative control of access to safety system equipment. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.9, "Control of Access" (Reference 41), provides acceptance criteria for Clause 5.9. This acceptance criteria states that administrative control is acceptable to assure that the access to the means for bypassing safety system functions is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access, and that digital computer-based systems need to consider controls over electronic access, including access via network connections and maintenance equipment, to safety system software and data. Electronic access to the replacement PPS is evaluated in Section 3.7.3, "DI&C-ISG-04 Compliance," of this safety evaluation. Security aspects of the Clause 5.9 were evaluated by the NRC staff in Section 3.12, "Secure Development and Operational Environment," of this safety evaluation.

The replacement PPS contains design features that provide means to control physical access to protection system equipment, including access to test points and the means for changing setpoints via the maintenance work stations. The PPS components including the maintenance work stations are located inside locked cabinets and the keys to these cabinets are administratively controlled by the operators. Additional access control features are considered by the licensee to be sensitive information and have been withheld from public disclosure pursuant to 10 CFR 2.390 (e.g., access to the vital area). Access control of these areas is addressed under the plant physical security and is therefore acceptable. Logical access via communication pathways is also controlled as described in Sections 3.1.6.1.7, "Tricon Communications," and 3.1.6.2.4, "ALS Communications," of this safety evaluation. Communication pathway access controls are evaluated in Section 3.7, "Communications," of this safety evaluation. The replacement PPS when controlled as described above meets the requirements of Clause 5.9.

3.9.2.10 IEEE 603-1991, Clause 5.10, Repair

This clause states that safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.10, "Repair" (Reference 41), provides acceptance criteria for Clause 5.10. This acceptance criteria states that while digital safety systems may include self-diagnostic capabilities to aid in troubleshooting, the use of self-diagnostics does not replace the need for the capability for test and calibration systems as required by Clauses 5.7 and 6.5.

The timely identification and location of malfunctioning PPS components is facilitated by platform and application-specific (hardware and software) features of the replacement PPS. The majority of equipment is modular, rack-mounted, and components are expected to be replaced rather than repaired to address failures. This facilitates timely repair of failed PPS components.

Both the Tricon and ALS portions of the PPS are designed for high reliability and have self-diagnostic features built into them. These features minimize required maintenance of these systems and simplify on-line hardware replacement activities.

The NRC staff reviewed the maintenance and repair features and capabilities of the Tricon and ALS subsystems and determined that they adequately address the timely recognition, location, replacement, repair, and adjustment of malfunctioning PPS equipment. Furthermore, the PPS design does not unduly rely upon self-diagnostic capabilities of the system to meet system test and calibration criteria. Though self-test features are being credited for operability determination purposes, both of the PPS subsystems will retain the capability for on-line testing including signal injection tests during plant operation. The NRC therefore concludes that the replacement PPS meets the criteria of Clause 5.10.

3.9.2.11 IEEE 603-1991, Clause 5.11, Identification

This clause states that safety system equipment be distinctly identified for each redundant portion of a safety system; that identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes; that identification of safety system equipment and its divisional assignment shall not require frequent use of reference material; and that the associated documentation shall be distinctly identified; however, components or 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.11, "Identification" (Reference 41), provides acceptance criteria for IEEE Std. 603-1991, Clause 5.11. This acceptance criterion also identifies Regulatory Guide (RG) 1.75, Revision 3, "Criteria for Independence of Electrical Safety Systems," dated February 2005 (Reference 63), which endorses IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 64), as guidance.

The DCPP plant-specific identification requirements provide a standardized method for identifying equipment diagrams and signal names on function diagrams. These items are adequately named for the purposes of understanding the documentation, and uniquely identifying instrumentation and controls equipment, diagrams, and signals.

All PPS equipment is identified by identification (ID) codes. The identification coding of existing field equipment is based on the original licensee ID assigned for the field devices. The PPS software engineering tools also document the hardware and software in the form of diagrams, which are identified by ID codes.

Cables associated with the four PPS protection set components are color-coded as red, white, blue, and yellow corresponding to assigned PPS protection set cabinets, respectively, and are routed in separate cable trays. PPS protection set equipment is similarly color-coded. This is in accordance with the guidance on identification provided in IEEE Std. 384-1992, Section 6.1.2, "Identification." The NRC staff determined that the identification of the replacement PPS and associated components meets the requirements of Clause 5.11.

3.9.2.12 IEEE 603-1991, Clause 5.12, Auxiliary Features

This clause states that auxiliary supporting features meet all requirements of this standard, and that auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions and are 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.12, "Auxiliary Features" (Reference 41), provides acceptance criteria for Clause 5.12. This acceptance criterion states that SRP Branch Technical Position (BTP) 7-9, Revision 5, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," March 2007 (Reference 43), provides guidance for the review of anticipatory trips that are auxiliary features of a reactor protection system.

The replacement PPS design includes a feature that transmits system data to non-safety-related plant systems. The degree of independence between the PPS and these systems is evaluated in Section 3.7.3, "DI&C-ISG-04 Compliance," of this safety evaluation. That evaluation supports the conclusion that this communications feature will not degrade the safety PPS performance below an acceptable level. All other non-safety-related features supported by the PPS are either isolated from the PPS via qualified isolation devices or are included in the safety system design. All features included in the safety system design were evaluated to the requirements of IEEE Std. 603-1991. The replacement PPS therefore meets the criteria of Clause 5.12.

3.9.2.13 IEEE 603-1991, Clause 5.13, Multi-Unit Stations

This clause states 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.13, "Multi-Unit Stations" (Reference 41), provides acceptance criteria for Clause 5.13. This acceptance criterion states that the shared user interfaces must be sufficient to support the operator needs for each of the shared units.

The PPS replacement project does not include sharing of any PPS structures, systems, or components between the two DCPP units. Because of this, the ability to simultaneously perform required safety functions in both DCPP units is maintained with the replacement PPS. The replacement PPS therefore complies with the criteria of Clause 5.13.

3.9.2.14 IEEE 603-1991, Clause 5.14, Human Factors Considerations

This clause states that human factors 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 operators and maintainers can be successfully accomplished to meet the safety system design goals. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.14, "Human Factors Considerations" (Reference 41), provides acceptance criteria for Clause 5.14, and states that safety system human factors design should be consistent with the applicant/licensee's commitments documented in Chapter 18 of the Final Safety Analysis Report Update (Reference 52).

The existing operator interfaces associated with the Eagle 21 PPS using control panel mounted switches and indicators are not being changed as part of the PPS replacement project. PPS outputs to the control room annunciation system are being revised so that they operate as dry contacts but they remain functionally equivalent to the existing Eagle 21 alarms. Additional alarm functions are also being added to the PPS.

The PPS human-system interface (HSI) design follows the guidance provided in the DCPP HSI Development Guidelines Document, which references NUREG-0700, Revision 2, "Human-System Interface Design Review Guidelines," May 2002 (Reference 55). This process is being implemented in conjunction with development of the replacement PPS design by PG&E. The NRC staff concludes the human-machine interface aspects of the replacement PPS meets the requirements of Clause 5.14.

3.9.2.15 IEEE 603-1991, Clause 5.15, Reliability

This clause states that 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.15, "Reliability" (Reference 41), provides acceptance criteria for Clause 5.15. This acceptance criterion states that the applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed and that for computer systems, both hardware and software reliability should be analyzed. The acceptance criteria in the SRP further states that software that complies with the quality criteria of Clause 5.3 and that is used in safety systems that provide measures for defense against common-cause failures, as previously described for Clause 5.1, are considered by the NRC staff to comply with the fundamental reliability requirements IEEE Std. 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations" (Reference 222), and IEEE Std. 603-1991.

Criterion 19, 1967, "Protection Systems Reliability" of the DCPP FSARU requires that Protection systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

Appendix 7.1-C, Section 5.15, further states that the assessment of reliability should consider the effect of possible hardware and software failures and the design features provided to prevent or limit the effects of these failures, and that hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures.

Failure modes and effects analyses (FMEAs) were performed to support the reliability analysis in accordance with IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems" (Reference 174), and IEEE Std. 577-1976, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations" (Reference 223). The FMEAs were evaluated by the NRC staff (see Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation). The NRC staff has determined that the replacement PPS meets the requirements of Clause 5.15.

3.9.3 IEEE 603-1991, Clause 6, Sense and Command Features

The requirements of this clause, in addition to the requirements of Clause 5, apply to the Sense and Command Features of a safety system. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6, "Sense and Command Features - Functional and Design Requirements" (Reference 41), provides acceptance criteria for Clause 6.

3.9.3.1 IEEE 603-1991, Clause 6.1, Automatic Control

This clause states that for each design basis event, all protective actions should automatically initiate without operator action, except as justified in IEEE Std. 603 Clause 4.5. In SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.1, "Automatic Controls" (Reference 41), provides acceptance criteria for Clause 6.1. The acceptance criteria states the automatic initiation should be precise and reliable, and the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis.

In SRP Chapter 7, Appendix 7.1-C, Section 6.1, states that, for digital computer-based systems, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real-time performance is deterministic and known. Standard Review Plan Branch

Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance" (Reference 50), provides guidance for this evaluation.

The replacement PPS design includes documents that describe the software and hardware requirements of the system. The NRC staff determined that the functional requirements have been appropriately allocated between hardware and software. The NRC staff determined that the replacement PPS design adequately demonstrates the deterministic behavior of the replacement PPS.

The evaluation of the replacement PPS response time against the applicable requirements is documented in Section 3.15, "Response Time Characteristics," of this safety evaluation. The evaluation of the PPS setpoint values is documented in Section 3.16, "System Setpoints Evaluation," of this safety evaluation. Based on the reviews documented in these two sections, the NRC staff determined that the replacement PPS conforms to the criteria of Clause 6.1.

3.9.3.2 IEEE 603-1991, Clause 6.2, Manual Control

This clause contains the requirements applicable to manual controls as described in the subsections below. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.2, "Manual Control" (Reference 41), provides acceptance criteria for Clause 6.2. There are three categories of manual controls as described in Clause 6.2, "Manual Control." The evaluation of the digital reactor protection system/engineered safety features actuation system against the requirements on each of these three categories is addressed in the subsections below.

3.9.3.2.1 IEEE 603-1991, Clause 6.2.1, Division Level Activation

This clause requires that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. These means must minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.2, "Manual Control" (Reference 41), states that features for manual initiation of protective action should conform to Regulatory Guide (RG) 1.62, Revision 1, "Manual Initiation of Protection Action," June 2010 (Reference 62), and will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

The means for providing manual initiation of protection actions at the division level are performed by systems that are external to the PPS. These means are provided at the solid state protection system actuation level, which is downstream of the PPS. The PPS replacement does not affect any of the division-level manual initiation features or functions in the DCPP protection system. The replacement PPS meets the requirements of Clause 6.2.1.

3.9.3.2.2 IEEE 603-1991, Clause 6.2.2, Non-Automatic Control

This clause requires 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 must meet the requirements of Clause 5.8.1.

The manual initiation and control of protective actions functions is not affected by the PPS replacement; therefore, this feature of the replacement PPS continues to meet the criteria of Clause 6.2.2.

3.9.3.2.3 IEEE 603-1991, Clause 6.2.3, Manual Control after Completion of Protective Action

This clause requires that means be provided in the control room 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 quality and location of associated displays and controls must be appropriate for the time period within which the actions must be accomplished and the number of available qualified operators. Such displays and controls must be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.

The PPS replacement does not change the information provided to the operators, the actions needed of the operators, or the quantity of the associated displays and controls available to the operators. Safety-related controls and indicators remain Class 1E and non-safety-related indicators are driven by qualified isolation devices.

Neither the manual initiation and control of protective action functions nor the information provided to the operators to support manual actions is affected by the PPS replacement. Therefore, the replacement PPS continues to meet the regulatory requirements of Clause 6.2.3.

3.9.3.3 IEEE 603-1991, Clause 6.3, Interaction with Other Systems

This cause contains two subclauses that have requirements that were used to evaluate the replacement PPS. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.3, "Interaction between the Sense and Command Features and Other Systems" (Reference 41), provides acceptance criteria for subclauses of Clause 6.3.

3.9.3.3.1 IEEE 603-1991, Clause 6.3.1, Interaction with Other Systems

This clause states that if a single credible event can both 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 an alternate channel or alternate equipment not subject to this failure will be provided, or equipment not subject to failure caused by the same single credible event shall be provided. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.3, "Interaction between the Sense and Command Features and Other Systems" (Reference 41), states that if the event of concern is a single failure of a sensing channel shared between control and protection functions, isolating the safety system from the sensing channel failure by providing additional redundancy or isolating the control system from the sensing channel failure by using data validation techniques to select a valid control input are approaches that have been previously accepted.

The PPS is designed to minimize the possibility of occurrence for events that can 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.

Each of the PPS failure modes and effects analyses (FMEAs) analyzes interconnections and means of isolation between redundant safety channels and circuits and between non-safety and safety channels and circuits to assure that no single failure can cause the loss of a safety function or spurious actuations (see Section 3.4.3.4, "Failure Modes and Effects Analysis/Reliability Analysis," of this safety evaluation). Devices used for Class 1E isolation have been qualified (by analyses and evaluation) to prevent electrical faults from propagating between redundant Class 1E circuits and between Class 1E circuits and non-Class 1E circuits (see Section 3.5, "Equipment Environmental Qualification," of this safety evaluation). The FMEA analyzes features included within the replacement PPS boundary including the maintenance work station and the gateway computer to assure that no single failure can cause the loss of a safety function or lead to spurious safety function actuations.

The PPS design does include sharing of certain signals between safety protection systems and systems that are used for non-safety control purposes; however, these system interactions are not being changed as part of this PPS replacement project.

To assure that compliance is maintained and that no additional control to safety system interactions are being introduced, the NRC staff identified each shared sensor signal and confirmed that the functional requirements of the replacement system do not alter the nature of these interactions. The following signal interactions were identified and analyzed by the NRC staff:

- RCS temperature signals are shared between the PPS and the rod speed and direction control system.
- RCS flow signals are shared between the PPS and control room indicators.
- Steam line flow signals are shared between the PPS and control room indicators as well as the digital feedwater control system.

- Steamline pressure signals are shared between the PPS and the digital feedwater control system.

- Steam generator level signals are shared between the PPS and the control room indicators, digital feedwater control system, and auxiliary feedwater control systems.

- Steam generator level signals are shared between the PPS and the anticipated transient without scram (ATWS) mitigating system actuation circuitry (AMSAC) system.

- The temperature signals listed below are shared between the PPS and control room indicators:
    - Wide range temperature
    - Pressurizer vapor temperature
    - Delta-T/T_{ave} temperature

The degree of independence between control systems and protection systems depends, in part, on the signal validation functions performed within the non-safety-related control systems. Because of this, by letter dated March 31, 2014 (Reference 190), the NRC staff requested additional information on these functions so that an evaluation of the effects of failed sensor inputs to these control systems could be performed. By letter dated April 30, 2014 (Reference 17), the licensee provided a table which identified various signal validation features that have been incorporated into the feedwater control, auxiliary feedwater control and AMSAC systems. This evaluation confirmed that there are no unanalyzed interactions between the control and protection systems that share sensor signals. Therefore, the replacement PPS continues to meet the regulatory requirements of Clause 6.3.1.

3.9.3.3.2 IEEE 603-1991, Clause 6.3.2, Interaction with Other Systems

This clause states that provisions must be included so that the requirements of Clause 6.3.1 can be met in conjunction with the requirements of Clause 6.7 if a channel is in maintenance bypass.

The failure modes and effects analysis (FMEA) specifically addresses the consequences of single failure, as required by Clause 6.3.2. The FMEA is performed to assure that the single-failure criterion is met assuming the bypassed channels cannot provide the safety function. There are no failures of the interfaced non-safety-related systems that will cause the loss of a safety function of the PPS, assuming one channel is in manual bypass. The NRC staff, therefore, determined that the replacement PPS meets the requirements of Clause 6.3.2.

3.9.3.4 IEEE 603-1991, Clause 6.4, Derivation of System Inputs

This clause states 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.4, "Derivation of System Inputs" (Reference 41), provides acceptance criteria for Clause 6.4. This acceptance criterion states that if indirect parameters are used, the indirect parameter must be shown to be a valid representation of the desired direct parameter for all events, and that for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate, are consistent with the analysis provided in Chapter 15, "Accident Analyses," of the Final Safety Analysis Report Update (Reference 52).

The sensor inputs used by the replacement PPS are the same as those for the existing Eagle 21 PPS and do not change from those used in the safety analysis. The replacement PPS therefore continues to meet the regulatory requirements of Clause 6.4.

3.9.3.5 IEEE 603-1991, Clause 6.5, Capability for Testing and Calibration

Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.5, "Capability for Testing and Calibration" (Reference 41), provides acceptance criteria for Clause 6.5 and states that SRP Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions" (Reference 47), discusses issues that should be considered in sensor check and surveillance test provisions for digital computer instrumentation and control (I&C) systems.

3.9.3.5.1 IEEE 603-1991, Clause 6.5.1, Checking for Operational Availability

This clause states that it must be possible to check, 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603" (Reference 41), states that the operational availability can be checked by varying the input to the sensor or by cross checking between redundant channels. The SRP Chapter 7, Appendix 7.1-C, Section 6.5 also states that SRP BTP 7-17 contains guidance concerning sensor check and surveillance test provisions for digital computer I&C systems.

The NRC staff reviewed the means used to determine PPS operability as defined by Section 3.3, "Instrumentation," of the DCPP technical specifications. The technical specification surveillance requirements pertaining to the PPS are being revised by this modification. These requirements include performance of channel operability tests and performance of channel calibrations. The PPS channel operability tests are being re-defined as part of the Tricon/ALS PPS modification. The revised channel operability tests entail (1) verifying that system setpoints and tunable parameters are correct and (2) injection of simulated process data into the channel as close to the sensor input as is practical. The replacement PPS provides the capability to perform periodic channel calibrations. Calibrations for instrument loops are performed by using measuring and test equipment to calibrate the field devices locally. Verification of proper response of the PPS engineered safety functions includes actuation of the final devices (pumps, valves, etc.) to ensure they respond to an engineered safety functions actuation system signal and that they move to the proper engineered safety functions actuation system state (on/off, open/closed, etc.). Verification of proper response of the reactor trip system includes testing of the reactor trip breakers.

The replacement PPS includes diagnostic features which continually test and verify system hardware performance. These features are also being credited for the purpose of ensuring channel operability. The NRC staff determined that these means provide an adequate degree of confidence that the operational availability of each PPS safety function will be maintained during reactor operation. Based upon the NRC staff's review of the channel operability and channel calibration tests, the NRC staff has determined that the replacement PPS meets the requirements of Clause 6.5.1, "Checking for Operational Availability."

3.9.3.5.2 IEEE 603-1991, Clause 6.5.2, Checking for Operational Availability

This clause requires that one of two means must be provided for assuring the operational availability of each sense and command feature required during the post-accident period. The first is by using the same methods described in Clause 6.5.1 (i.e., checking post-accident is same as checking during normal operation). The second is by specifying equipment that is stable and the period of time it retains its calibration during the post-accident period.

The channel check method described in Section 3.3 of the DCPP Technical Specifications is used to assure that the sense and command features used during the post-accident period are still operational and available. The NRC staff has determined that this method is acceptable and, therefore, the replacement PPS meets the requirements of Clause 6.5.2.

3.9.3.6 IEEE 603-1991, Clause 6.6, Operating Bypasses

This clause states that if the applicable permissive 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 permissive conditions once again exist, or initiate the appropriate safety function(s). Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.6, "Operating Bypasses" (Reference 41), provides acceptance criteria for Clause 6.6. This acceptance criterion states that the requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

The replacement PPS does not change the functional characteristics of the operational bypass features. Operational bypass features are accomplished by the P-11, "Low Pressurizer Pressure Safety Injection Operational Bypass," P-12, "Low-Low T_{ave} Steam Dump Block," P-13, "Turbine Low Power Permissive," and P-14, "High-High Steam Generator Level Turbine Trip Feedwater Isolation," permissive functions which are described in Section 3.1.3.15, "PPS Permissive Functions," of this safety evaluation.

The PPS performs the bistable comparator operations to support each of these bypass functions. The bistable outputs from the PPS are sent to the solid state protection system, which performs voting operations and determines when each of the permissive functions becomes active. This determination is based on the input status received from each of the PPS protection sets.

The NRC staff reviewed the PPS functional requirements associated with the operational bypass features and confirmed that the automatic bypass removal capabilities of these permissives are retained in the modified system design. The NRC staff therefore determined that the replacement PPS will continue to automatically prevent the activation of operating safety function bypass features associated with the PPS. The staff further determined that the replacement PPS is designed to automatically remove activated operating bypasses when plant conditions for bypass operation are not satisfied. Based on the above, the replacement PPS meets the criteria of Clause 6.6.

3.9.3.7 IEEE 603-1991, Clause 6.7, Maintenance Bypass

This clause states that the safety system be designed such that while sense and command features equipment is in maintenance bypass, the capability of a safety system to accomplish its safety function must be retained, and during such operation, the sense and command features must continue to meet the requirements of Clauses 5.1 and 6.3. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.7, "Maintenance Bypass" (Reference 41), provides acceptance criteria for Clause 6.7. This acceptance criteria states that provisions for this bypass need to be consistent with the required actions of the plant technical specifications.

The capability of the PPS to perform its safety functions are established such that these functions will remain operable during system testing and when a single channel is placed into the maintenance bypass mode for any reason. The bypassed and inoperable status indications in the control room are not being modified as a result of the PPS replacement and operators will be provided with continuous indication via a "PPS channel in bypass" alarm whenever a PPS channel is in bypass mode.

The DCPP failure modes and effects analysis (FMEA) for the PPS replacement project assumes that one PPS channel is in the channel bypass mode as an initial condition. The FMEA then analyzes the effect of an additional failure on the safety system's capability to perform the required safety functions. The FMEA results as evaluated in Section 3.4.3.4 of this safety evaluation demonstrate that the replacement PPS is capable of performing its required safety functions even while a channel is in the maintenance bypass mode. Thus, the replacement PPS is capable of meeting the single-failure criteria of Clause 5.1 as well as the interaction between control and protection criteria of Clause 6.3 of IEEE 603-1991 while any channel is in the maintenance bypass mode. Based on the above, the NRC staff concludes that the replacement PPS meets the criteria of Clause 6.7.

3.9.3.8 IEEE 603-1991, Clause 6.8, Setpoints

This clause states that the allowance for uncertainties between the process analytical limit documented in Clause 4.4 and the device setpoint must be determined using a documented methodology and, where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design must provide a positive means of ensuring that the more restrictive setpoint is used when required. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.8, "Setpoints" (Reference 41), provides acceptance criteria for Clause 6.8. This acceptance criteria states that the setpoint analysis should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system, and should confirm that an adequate margin exists between setpoints and safety limits, and that additional guidance on establishment of instrument setpoints can be found in Regulatory Guide (RG) 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation," December 1999 (Reference 67), SRP Branch Technical Position (BTP) 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints" (Reference 45), and in Regulatory Issue Summary (RIS) 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," dated August 24, 2006 (Reference 224). Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, Section 6.8, further states that where it is necessary to provide multiple setpoints as discussed in Clause 6.8.2, the NRC staff interpretation of "positive means" is that automatic action is provided to ensure that the more restrictive setpoint is used when required, and that BTP 7-3, Revision 5, "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service," March 2007 (Reference 225), provides additional guidance on multiple setpoints used to allow operation with reactor coolant pumps out of service.

Setpoint calculations used for the replacement PPS are derived from Westinghouse document WCAP-17696-P, Revision 0, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," January 2013 (Reference 220), using the setpoint methodology contained in WCAP-17706-P, Revision 0, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," January 2013 (Reference 221). The approach used for the methodology is consistent with Instrument Society of America (ISA)-S67.04.01-2006, "Setpoints for Safety-Related Instrumentation" (Reference 68), and included input from RIS 2006-17 (Reference 224) and Technical Specification Task Force (TSTF)-493-A, Revision 4, "Clarify Application of Setpoint Methodology for LSSS [Limiting Safety System Setting] Functions," dated January 5, 2010 (Reference 226). The NRC staff determined that this documented setpoint methodology provides an acceptable basis for determination of PPS setpoints and therefore meets the criteria of Clause 6.8.1.

The revised calculations confirm that there is adequate margin between the current technical specification 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. A summary of the analytical limits and current technical specification setpoints for the PPS was provided in Table 4-10 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12). The NRC staff reviewed and evaluated these setpoints as well as the established margins and determined that they provide adequate protection for anticipated operating conditions. Only the over power delta temperature and over temperature delta temperature PPS functions provide multiple (variable) setpoints that are determined based on operating conditions. The calculations for these setpoints defined in the Final Safety Analysis Report Update, Section 7.2.2.1.2, "Core Thermal Overpower Trips" (Reference 52), and Table 3.3.3-1, "Post Accident Monitoring Instrumentation," of the DCPP technical specifications, are not being revised for the replacement PPS and, therefore, will continue to ensure that appropriate restrictive setpoints will be used when required. Based on the above, the NRC staff concludes the replacement PPS meets the criteria of Clause 6.8.2.

3.9.4 IEEE 603-1991, Clause 7, Execute Features

This clause requires that Clauses 7.1 through 7.5 apply to the execute features. The evaluation of the DCPP PPS against Clauses 7.1 through 7.5 is documented in the subsections below.

3.9.4.1 IEEE 603-1991, Clause 7.1, Automatic Control

This clause states that the safety system will have the capability incorporated into 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 7.1, "Automatic Controls" (Reference 41), provides acceptance criteria for Clause 7.1. The acceptance criteria states the automatic initiation should be precise and reliable, and the evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis.

In SRP Chapter 7, Appendix 7.1-C, Section 7.1, states that for digital computer-based systems, the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real time performance is deterministic and known. Standard Review Plan (SRP) Branch Technical Position (BTP) 7-21, Revision 5, "Guidance on Digital Computer Real-Time Performance," March 2007 (Reference 50), provides guidance for this evaluation.

Based on the evaluation documented in Section 3.10.1.1, "IEEE 7-4.3.2-2003, Clause 5.3, Quality," of this safety evaluation, the functional requirements have been appropriately allocated into hardware and software requirements. Based on the evaluation documented in Section 3.17, "Deterministic System Behavior," of this safety evaluation, the system's real time performance is deterministic and known. Based on the above, the NRC staff concludes that the replacement PPS meets the criteria of Clause 7.1.

3.9.4.2 IEEE 603-1991, Clause 7.2, Manual Control

This clause states that if manual control of any actuated component in the execute features is provided, the additional features needed to accomplish such manual control shall not defeat the requirements of the single failure and manual control criteria; any capability to receive and act upon manual control signals from the sense and command features must be consistent with the design basis. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 7.2, "Manual Control" (Reference 41), provides the same acceptance criteria for Clause 7.2, as was provided for Clause 6.2.

The means for providing manual initiation of protection actions at the division level are performed by systems that are external to the PPS. These means are provided at the solid state protection system actuation level, which is downstream of the PPS. The PPS replacement does not affect any of the division-level manual initiation features or functions in the DCPP protection system.

The replacement PPS does not impact the ability of the solid state protection system to receive and act upon manual control signals initiated by the plant operators. This is consistent with the plant design basis and, therefore, the NRC staff concludes that the modified DCPP protection systems meet the requirements of Clause 7.2.

3.9.4.3 IEEE 603-1991, Clause 7.3, Completion of Protective Action

This clause states 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. In addition, when the sense and command features reset, the execute features shall not automatically return to normal, but shall require separate, deliberate operator action to be returned to normal. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 7.3, "Completion of Protective Action" (Reference 41), provides acceptance criteria for Clause 7.3. This acceptance criteria states the review should include review of functional and logic diagrams, and that the seal-in feature may incorporate a time delay as appropriate for the safety function.

All execute features of the protection system are performed by the solid state protection system which is not being modified by the PPS replacement. The NRC staff reviewed the functional requirements of the replacement PPS and verified that the ability of the solid state protection system portion of the DCPP protection system will not be affected by the PPS replacement.

Manual initiation of safety functions is accomplished by the downstream solid state protection system, which is not being modified by the PPS modification; however, the NRC staff confirmed that these functions continue to meet the completion of protective function criteria. The solid state protection system is designed so that the safety functions will remain active upon reset of the input signals received from the replacement PPS. All solid state protection system reactor trip or engineered safety features actuation system signals require manual action to reset following completion of the protective action after the PPS initiating signals have reset.

3.9.4.4 IEEE 603-1991, Clause 7.4, Operating Bypass

This clause states that if 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), 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 permissive conditions once again exist, or initiate the appropriate safety function(s). Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 7.6, "Operating Bypasses" (Reference 41), provides acceptance criteria for Clause 7.6. This acceptance criteria states that the requirement for automatic removal of operational bypasses means that the reactor operator may not have a role in such removal; however, the operator may take action to prevent the unnecessary initiation of a protective action.

The replacement PPS does not change the functional characteristics of the operational bypass features. Operational bypass features are accomplished by permissive functions P-11, "Low Pressurizer Pressure Safety Injection Operational Bypass," P-12, "Low-Low T_{ave} Steam Dump Block," P-13, "Turbine Low Power Permissive," and P-14, "High-High Steam Generator Level Turbine Trip – Feedwater Isolation," which are described in Section 3.1.3.15, "PPS Permissive Functions," of this safety evaluation.

The solid state protection system performs functions to accomplish execute features associated with the operating bypasses. See Section 3.9.3, "IEEE 603-1991, Clause 6, Sense and Command Features," of this safety evaluation for evaluation of the PPS sense and command features associated with operating bypass. Because the solid state protection system is not being revised as a result of the PPS replacement, the NRC staff determined that the solid state protection system will remain capable of meeting the execute features requirements of Clause 7.4.

3.9.4.5 IEEE 603-1991, Clause 7.5, Maintenance Bypass

This clause has similar requirements as Clause 6.7, but also states that portions of the execute features with a degree of redundancy of one must be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 7.5, "Maintenance Bypass" (Reference 41), provides acceptance criteria for Clause 7.5. This acceptance criteria states that provisions for this bypass need to be consistent with the required actions of the plant technical specifications.

All execute features associated with the safety functions that the replacement PPS supports are performed by the solid state protection system. Therefore, the proposed PPS modification will not affect the capability of the DCPP safety systems to accomplish safety functions during execute feature maintenance bypass operation. The maintenance bypass execute features will remain consistent with the required actions of the DCPP technical specifications.

3.9.5 IEEE 603-1991, Clause 8, Power Source Requirements

Clause 8 contains no requirements, but has three sub clauses that contain requirements for evaluating the DCPP PPS in the subsections below. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 8, (Reference 41), does not provide acceptance criteria for Clause 8.

3.9.5.1 IEEE 603-1991, Clause 8.1, Electrical Power Sources

This clause states 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.

The replacement PPS uses the same electrical power sources as the Eagle 21 PPS. Each PPS replacement protection set is powered from a separate 120 Volts alternating current vital bus via a Class 1E uninterruptible power supply. Since this aspect is not being changed by this license amendment request, the replacement PPS remains compliant with Clause 8.1.

3.9.5.2 IEEE 603-1991, Clause 8.2, Non-Electrical Power Sources

This clause states that non-electrical power sources required to provide the power to the safety system must be a portion of the safety systems and must provide power consistent with the requirements of IEEE Std. 603.

The PPS replacement does not rely on non-electrical power sources for performance of its safety-related functions; therefore, Clause 8.2 is not applicable, and no evaluation was performed with respect to Clause 8.2.

3.9.5.3 IEEE 603-1991, Clause 8.3, Maintenance Bypass

This clause states that the capability of the safety systems to accomplish their safety functions shall be retained with the power sources in maintenance bypass. Clause 8.3 also states that the portions of the power sources with a degree of redundancy of one must be designed such that when a portion is placed in maintenance bypass, the remaining portions provide acceptable reliability.

The replacement PPS uses the same power sources as does the existing Eagle 21 PPS that it will replace. If an external power source for a safety-related protection set fails, the remaining safety-related protection sets are designed to ensure that the safety system remains capable of performing the assigned safety functions. The replacement PPS will behave the same as the existing Eagle 21 PPS when power supplies are in maintenance bypass. Since this aspect is not being changed by this license amendment request, the criteria of Clause 8.3 will continue to be satisfied by the replacement PPS.

Tricon

Each Tricon chassis within the PPS has two redundant chassis power supplies. Each chassis power supply is capable of supplying a full chassis load in the event of failure (or bypass) of the other power supply. The power supply modules possess built-in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator light-emitting diodes on the front face of each power module provide module status.

ALS

Advanced Logic System (ALS) boards are designed with local voltage regulators and monitors to ensure stable and reliable local board voltages. The ALS boards are supplied by two redundant power feeds which are diode auctioneered and fuse protected to provide enhanced reliability. The ALS boards are also equipped with voltage supervisors, which monitor power sources to ensure adequate voltage levels for reliable operation of the field programmable gate array (FPGA) logic and channel circuits.

3.10 Conformance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

Regulatory Guide (RG) 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011 (Reference 71), states that conformance with the requirements of Institute for Electrical and Electronics Engineers (IEEE) Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33), is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2" (Reference 42), contains guidance for the evaluation of the implementation of the requirements of IEEE Std. 7-4.3.2-2003. This section documents the evaluation of the proposed DCPP process protection system (PPS) replacement system against this guidance or references other sections of this safety evaluation where the evaluation is documented.

3.10.1 IEEE Std. 7-4.3.2-2003, Clause 5, Safety System Criteria

Clause 5 contains 15 subclauses, which contain requirements that were used to evaluate the DCPP PPS replacement system in the subsections below. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5, "Safety System Criteria" (Reference 42), provide acceptance criteria for subclauses of Clause 5.

3.10.1.1 IEEE 7-4.3.2-2003, Clause 5.3, Quality

Clause 5.3 states that computer development activities must include the development of computer hardware and software. In addition, Clause 5.3, also states that the integration of computer hardware and software and the integration of the computer with the safety system shall be addressed in the development process. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.3.1, "Software Development" (Reference 42), states that SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems," dated March 2007 (Reference 46), contains SRP acceptance criteria for software development processes.

The computer development activities of the Tricon and Advanced Logic System (ALS) platforms were reviewed and approved as part of the topical report safety evaluations for the Triconex Approved Topical Report (Reference 29) and the Advanced Logic System Topical Report (Reference 30). These activities included the development of the system hardware as well as platform software and logic configurations. Changes to the Tricon platform computer development process were evaluated in Section 3.8, "Tricon V10 Platform Reference Design Changes," of this safety evaluation, and were determined to be acceptable. The computer development activities of the replacement PPS ALS and Tricon PPS applications were evaluated in Section 3.4, "Software/Core Logic Development Process," of this safety evaluation, and were determined to be acceptable. These activities included the development of the Tricon application software, ALS application logic, and the configuration of previously developed hardware.

The NRC staff concludes that integration of Tricon computer hardware and software is a planned activity included in the PPS development processes. The NRC also concludes that integration of the ALS hardware and the ALS logic implementation is a planned activity included in the PPS development processes. The planning aspects of these activities were evaluated in Section 3.4.1.4, "Software/Core Logic Integration Plan, of this safety evaluation. These activities include aspects of integrating hardware with application software and logic configurations as well as integration of each of the digital subsystems with the DCPP safety systems.

3.10.1.1.1 IEEE 7-4.3.2-2003, Clause 5.3.1, Software Development

Clause 5.3.1 requires an approved quality assurance plan for the development modification and acceptance of all software that is resident at run time. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.3.1, "Software Development" (Reference 42), states that SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems," dated March 2007 (Reference 46), describes the characteristics of a software development process that the NRC staff evaluates when assessing the quality criteria of Clause 5.3.

Tricon

The software that is resident in the Tricon PPS subsystem at run time can be grouped into two categories: (1) Tricon platform software and (2) Test System Application Program (TSAP) software. Software for each of these categories is generated using different development processes. Both development processes were evaluated by the NRC using the criteria of SRP BTP 7-14. Both categories of software are developed, modified, and accepted in accordance with different software quality assurance plans (SQAPs). The platform software quality assurance processes were evaluated as part of the review of the Triconex Approved Topical Report (Reference 29), and changes to these processes were determined to be acceptable (see Section 3.8.4, "Development Process Changes," of this safety evaluation). The TSAP SQAP evaluation is documented in Section 3.4.1.3, "Software/Core Logic Quality Assurance Plan," of this safety evaluation.

ALS

The ALS platform has no resident software at run time; however, software is utilized for the development of logic that is implemented on the ALS field programmable gate arrays (FPGAs) to perform safety functions. The processes used for configuring the ALS FPGAs are subject to the Westinghouse Quality Management System which was evaluated during the platform review for compliance with this clause. The safety evaluation for the Advanced Logic System Topical Report (Reference 30) concluded that the Westinghouse Quality Management System meets the requirements of Appendix B to 10 CFR Part 50 and is therefore acceptable. The NRC staff further concluded that all FPGA programming resident in the ALS platform has or will be developed, modified, and accepted in accordance with a quality assurance plan that is appropriate for the FPGA technology and for use in safety-related systems of nuclear power plants.

The NRC staff evaluated the quality of the PPS application software and logic development plans by reviewing the "Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102) as well as the "ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, dated May 2013 (Reference 163). The software/FPGA logic development plans (see Section 3.4.1, "Software/Core Logic Planning Documentation," of this safety evaluation), the implementation of the plans (see Section 3.4.2, "Software Implementation Documentation," of this safety evaluation), and the design outputs produced (see Section 3.4.3, "Software Design Outputs," of this safety evaluation). Based on these evaluations, the NRC staff determined that the replacement PPS conforms to Clause 5.3.1.

3.10.1.1.1.1 IEEE 7-4.3.2-2003, Clause 5.3.1.1, Software Quality Metrics

Clause 5.3.1.1 states that the use of software quality metrics shall be considered throughout the software lifecycle to assess whether software quality requirements are being met. SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.3.1.1, "Software Quality Metrics" (Reference 42), states that metrics are considered in the review of the software development process in accordance with SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems," dated March 2007 (Reference 46).

The DCPP "Software Quality Assurance Plan (SQAP)," Revision 1, 993754-1-801-P, dated March 14, 2012 (Reference 129), used for the Tricon portion of the PPS identifies process metrics used during the development lifecycle in order to identify common features and potential changes in procedure or process needed to prevent recurrence of problems encountered.

The ALS platform development lifecycle includes consideration of methods to assess satisfactory implementation of FPGA programming quality. The "ALS V&V Plan" which is evaluated in Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation addresses correctness and completeness of requirements during the requirements phase, compliance with requirements as part of the design phase, compliance with design as part of the implementation phase, and functional compliance with requirements as part of the test and integration phase.

3.10.1.1.2 IEEE 7-4.3.2-2003, Clause 5.3.2, Software Tools

Clause 5.3.2 states that software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management, and that the tools shall either be developed to a similar standard as the safety-related software, or that 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. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2" (Reference 42), guides the reviewer to thoroughly evaluate software tool use.

Tricon Software Tools

Tricon applications are developed using the TriStation 1131 software development tool. The TriStation 1131 is maintained under the Invensys Operations Management (IOM) configuration management program. Usage of this software tool was evaluated by the NRC during the evaluation for the Triconex Approved Topical Report (Reference 29), and was determined to be acceptable. Software developed with the TriStation 1131 tool is independently verified and validated to ensure that any defects not detected by the tool will be detected and corrected through other means. The software V&V activities performed during the DCPP PPS application development (evaluated in Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation) do not utilize the TriStation 1131 tool and therefore can be used as an independent means of ensuring that the tool output is correct.

ALS Software Tools

The design and development of the ALS platform's FPGAs rely on several commercially available software-based tools. Each of these tools has been placed under the Westinghouse configuration management program for control and maintenance. These software-based tools are subjected to an assessment and tool qualification to ensure that each tool is capable of performing its design or verification functions.

In-process V&V activities include tool output assessments. Verification and validation (V&V) testing is performed on the programmed FPGA to confirm correct device operation, and this testing represents a verification of the final software-based tool's output.

Software tools used for ALS are maintained under configuration management and Westinghouse has implemented a tool validation program to provide confidence that the necessary features of software tools function as required.

Conclusion

Based on the review of the V&V processes as described in Sections 3.4.1.6, "Software/Core Logic Verification & Validation Plan," and 3.4.2.2, "V&V Analysis and Reports," of this safety evaluation, and verified during audits, the NRC staff determined that the output of the tools used for application development were subject to V&V activities which would detect any defects or errors caused by the usage of the tools. The use of tools in the development of the replacement PPS is consistent with the requirements in this section and is, therefore, acceptable. Although the software tools used for the DCPP PPS application development are not qualified as safety-related, the NRC staff concludes that the tool assessment and qualification processes satisfy IEEE Std. 7-4.3.2-2003, Clause 5.3.2.

3.10.1.1.3 IEEE 7-4.3.2-2003, Clause 5.3.3, Verification and Validation

This clause states that a V&V program shall address the computer hardware and software, integration of digital components, and interaction of the resulting computer system with the nuclear power plant. The V&V program must exist throughout the entire system lifecycle. Standard Review Plan (SRP), Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2" (Reference 42), states that the software V&V effort should be performed in accordance with IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74), which is endorsed by Regulatory Guide (RG) 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013 (Reference 73).

The NRC staff used RG 1.168 and IEEE Std. 1012 to evaluate the V&V planning processes used for the PPS replacement system (see Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation) and the V&V summary reports (see Section 3.4.2.2, "V&V Analysis and Reports," of this safety evaluation). The NRC staff also evaluated the plan for the integration of digital components (see Section 3.4.1.4, "Software/Core Logic Integration Plan," of this safety evaluation); and the plan for testing (see Section 3.4.1.8, "Software/Core Logic Test Plan," of this safety evaluation). Based on these evaluations the NRC staff determined that the replacement PPS conforms to the criteria of Clause 5.3.3. The V&V of the PPS interactions with the plant will be reviewed as an inspection activity during site acceptance testing and commissioning of the replacement PPS.

3.10.1.1.4 IEEE 7-4.3.2-2003, Clause 5.3.4, Independent V&V (IV&V) Requirements

This clause defines the levels of independence required for the V&V effort, in terms of technical independence, managerial independence, and financial independence. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.3.4, "Independent V&V (IV&V) Requirements" (Reference 42), provides detailed guidance to assist the reviewer in determining the extent of independence of the V&V activities from the design activities.

The Invensys/Tricon "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), and the Westinghouse "ALS V&V Plan," Revision 8, 6002-00003-P, January 2013 (Reference 134), as well as the "System Verification and Validation Plan (SyVVP), Nuclear Safety Related," Revision 1, dated February 19, 2013, used by the licensee (Reference 111), identify the organizational entities responsible for performance and oversight of V&V activities associated with the replacement PPS development. These plans also describe the V&V activities performed by these organizations. The NRC staff evaluated the level of independence between each of the V&V organizations and the associated design organization. The NRC staff also evaluated the qualification of assigned V&V personnel within each of these organizations. These aspects of the system design V&V were found acceptable (see Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation). The NRC staff determined the technical competence of organizations assigned to perform V&V tasks to be adequate and that individuals performing V&V tasks were not the same individuals that perform the design and development activities.

The responsibility for oversight of the project V&V activities as defined in the software verification and validation plans is divided between different people and organizations for each of the vendors and for the licensee.

For V&V activities performed by the licensee, the oversight responsibilities are assigned to the project manager (PM) as identified in Section 4.1 of the SyVVP (Reference 111). The PM's oversight responsibilities include releasing the system-level V&V plan and reports, and reviewing progress of the V&V program. The PM is not responsible for system development or for program management. Therefore, the PG&E responsibilities for independent verification and validation (IV&V) oversight comply with the criteria of Clause 5.3.4.

Each of the Appendix B supplier PMs are responsible for providing direction in implementation of the vendor V&V activities to ensure that they are performed per the respective control procedures.

The Tricon SVVP (Reference 118) assigns the oversight responsibilities of software V&V activities to the Nuclear IV&V director, and to the IV&V manager who reports to the Nuclear IV&V director. Their responsibilities include:

- Providing resources and expertise to the V&V operations,
- Implementing V&V activities, and
- Ensuring that V&V activities are managerially, technically, and financially independent of the development organization.

The ALS V&V Plan (Reference 134) assigns the oversight responsibilities of V&V activities to the ALS project manager and to the IV&V manager. Their responsibilities include:

- IV&V team staffing and resource allocation determinations,
- Approval of IV&V products, and
- Ensure resolution of issues raised by IV&V.

The NRC staff reviewed the following activities and determined that they were being conducted independently from all design and development activities:

- Selection of the PPS application to be analyzed,
- Selection of techniques used to perform analysis,
- Selection of issues or problems to be acted upon, and
- Allocation of independent resources.

Personnel responsible for V&V oversight activities are not responsible for system development or for program management. Therefore, the vendor-assigned responsibilities for IV&V oversight also comply with the criteria of Clause 5.3.4. The NRC staff concludes that the degree of independence established by the licensee and by the respective suppliers of the replacement PPS equipment is adequate and meets the criteria of Clause 5.3.4.

3.10.1.1.5 IEEE 7-4.3.2-2003, Clause 5.3.5, Software Configuration Management

Clause 5.3.5 states that software configuration management shall be performed in accordance with IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management," (Reference 78), and that IEEE Std. 828-1998, "IEEE Standard for Software Configuration Management Plans" (Reference 227), provides guidance for the development of software configuration management plans (SCMPs). IEEE Std. 828-1990, "IEEE Standard for Software

Configuration Management Plans" (Reference 77), and IEEE Std. 1042-1987, are endorsed by RG 1.169, Revision 0, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (Reference 76). Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2" (Reference 42), states that SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems," March 2007 (Reference 46), and RG 1.169 provide SRP acceptance criteria for SCMPs and activities.

The configuration management plans used for the PPS replacement project were evaluated against the criteria of BTP 7-14, Section B.3.1.11, "Software Configuration Management Plan (SCMP)"; SRP Appendix 7.1-D, Section 5.3.5, "Software Configuration Management" (Reference 42); RG 1.169; and IEEE Std. 1042-1987 (see Section 3.4.1.7, "Software/Core Logic Configuration Management Plan," of this safety evaluation). The implementation of software configuration management was evaluated in Section 3.4.2.3, "Configuration Management Activities," of this safety evaluation. The system build documents were evaluated in Section 3.4.3.7, "System Build Documents," of this safety evaluation. Based on these evaluations, the NRC staff determined that the configuration management activities performed for the PPS replacement system conform to the requirements of Clause 5.3.5.

3.10.1.1.6 IEEE 7-4.3.2-2003, Clause 5.3.6, Software Project Risk Management

Clause 5.3.6 defines the risk management criteria for a software project. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.3.6, "Software Project Risk Management" (Reference 42), provides acceptance criteria for software project risk management. This section states that software project risk management is a tool for problem prevention, and should be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. It also states that 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.

Tricon

Invensys uses a standardized project management process to assess risks, as described in Sections 3.4, "Risk Management," and 3.5, "Monitoring and Controlling Mechanisms," of the Triconex "Project Management Plan (PMP)," Revision 3, 993754-1-905-P, dated December 18, 2012 (Reference 114). The risk management methodology described in the Tricon PMP includes identification, assessment, monitoring, and control of risks that arise during the software development project.

ALS

The risk management process for the ALS portion of the DCPP PPS is described in Section 4.4, "Risk Management Plan," of the Diablo Canyon PPS "Management Plan," Revision 8, 6116-00000, September 2015 (Reference 105). This section explains the use of a Risk Assessment Worksheet to document risk management activities used during the application development process. It also describes how the project leadership team analyzes identified risks and determines the risk mitigation plan to be used.

The methodologies employed for software project risk management utilize processes to rate the complexity and risks of projects to optimize project planning and execution. In the course of project execution, the project risks are monitored, and the original rating is reviewed to determine if the rating needs to be modified. The software development and project management plans address development risks throughout the lifecycle, and these plans include the development and use of the Tricon and ALS platforms. The NRC staff has reviewed the software development plans (see Section 3.4.1.2, "Software/Core Logic Development Plan," of this safety evaluation) and the implementation of those plans (see Section 3.4.2, "Software Implementation Documentation," of this safety evaluation), and determined that the DCPP PPS meets the criteria of Clause 5.3.6.

3.10.1.2 IEEE 7-4.3.2-2003, Clause 5.4, Equipment Qualification

Clause 5.4 defines the equipment qualification required for a software project. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.4, "Equipment Qualification" (Reference 42), which provides acceptance criteria for equipment qualifications, states that in addition to the equipment qualification criteria provided by IEEE Std. 603 and Section 5.4, "Equipment Qualification," of SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603" (Reference 41), additional criteria, as defined in Clauses 5.4.1, "Computer System Testing," and 5.4.2, "Qualification of Existing Commercial Computers," of IEEE 7-4.3.2-2003, are necessary to qualify digital computers for use in safety systems. These sections are discussed in the following subsections of this safety evaluation.

3.10.1.2.1 IEEE 7-4.3.2-2003, Clause 5.4.1, Computer System Testing

Clause 5.4.1 discusses the software that should be operational on the computer system while qualification testing is being performed. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.4.1, "Computer System Testing" (Reference 42), provides acceptance criteria for equipment qualifications. This section states that computer system equipment qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation.

Tricon

The Tricon programmable logic controller (PLC) has been qualified in accordance with Electric Power Research Institute (EPRI) technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), which included extensive testing and encompasses the criteria of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33). The Tricon V10 system was evaluated by the NRC and was determined to be acceptable for use in safety-related applications. Changes made to V10 of the Tricon platform were further qualified to the same standard (TR-107330) per the Triconex Approved Topical Report (Reference 29). These changes are evaluated in Section 3.8, "Tricon V10 Platform Reference Design Changes," of this safety evaluation.

ALS

Section 12.2.12.1, "IEEE 7-4.3.2 Clause 5.4.1 - Computer System Testing," of the Advanced Logic System Topical Report (Reference 30) describes the qualification testing and how the ALS platform meets the requirement of Clause 5.4.1. The DCPP "Test Plan," Revision 4, 6116-00005, October 2014 (Reference 136), describes the scope and content of the test program for Westinghouse scope of the PPS replacement project. Testing of the ALS portion of the PPS was performed with the ALS application boards functioning. The ALS system does not use software at run time; however, all diagnostic features of the ALS system were operational during system testing.

A multi-level test program was used to ensure quality in the DCPP PPS hardware and software. The testing addresses the hardware and software used, from input to output terminals. The testing includes the maintenance work station and the ALS Service Unit. The overall qualification testing includes component testing, qualification testing, and development testing.

PPS replacement equipment qualification testing for both the Tricon and ALS was performed with the digital equipment functioning and with software and diagnostics representative of operational service. Future testing, including installation and post-installation, will be performed with the computers fully functional as well.

The DCPP PPS "Factory Acceptance Test Report," Protection Set I, Revision 0, 6116-70033; Protection Set II, Revision 0, 6116-70034; Protection Set III, Revision 0, 6116-70035; and Protection Set IV, Revision 0, 6116-70036, August 2015 (Reference 162), and the "Independent Verification and Validation Summary Report," Revision 1, 6116-00500, dated October 2015 (Reference 104), demonstrate compliance with performance requirements related to safety functions. The plant-specific action items regarding equipment qualifications have been addressed satisfactorily (see Section 3.12, "Secure Development and Operational Environment," of this safety evaluation). The NRC staff has determined the DCPP PPS conforms to Clause 5.4.1.

3.10.1.2.2 IEEE 7-4.3.2-2003, Clause 5.4.2, Qualification of Existing Commercial Computers

Clause 5.4.2 defines the qualification of existing commercial computers for use in safety-related applications in nuclear power plants. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.4.2, "Qualification of

Existing Commercial Computers" (Reference 42), provides acceptance criteria for equipment qualifications. This section states that EPRI technical report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996 (Reference 228), and EPRI technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), provide specific guidance for the evaluation of commercial grade digital equipment and existing programmable logic controllers (PLCs).

The qualification of the Tricon and ALS equipment was addressed in the Triconex Approved Topical Report (Reference 29) and the Advanced Logic System Topical Report (Reference 30), respectively. Changes to the approved Tricon equipment have been evaluated (see Section 3.8, "Tricon V10 Platform Reference Design Changes," of this safety evaluation). The plant-specific action items regarding equipment qualifications have been addressed satisfactorily (see Section 3.12, "Secure Development and Operational Environment," of this safety evaluation).

The safety-related portions of the DCPP PPS do not contain any other commercial digital computers; therefore, no evaluation of the qualification of existing commercial computers is required. Based on these evaluations, the NRC staff has determined that the DCPP PPS conforms to Clause 5.4.

3.10.1.3 IEEE 7-4.3.2-2003, Clause 5.5, System Integrity

Clause 5.5 states that in addition to the system integrity criteria provided by IEEE Std. 603, the digital system shall be designed for computer integrity, test and calibration, and fault detection and self-diagnostics activities. These attributes are further defined in IEEE Std. 7-4.3.2-2003, Clause 5.5.1, "Design for Computer Integrity," Clause 5.5.2, "Design for Test and Calibration," and Clause 5.5.3, "Fault Detection and Self-diagnostics"; these subclauses are evaluated in the subsections below. There are no specific acceptance criteria shown in SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.5, "System Integrity" (Reference 42).

3.10.1.3.1 IEEE 7-4.3.2-2003, Clause 5.5.1, Design for Computer Integrity

Clause 5.5.1 states that 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.

Tricon

Within each protection set, the Tricon portion of the PPS is triple modular redundant (TMR) from input terminal to output terminal (see Section 3.1.6.1, "Tricon Components," of this safety evaluation for a more detailed description of the TMR architecture). The TMR architecture is intended to maintain protection set subsystem operation in the presence of any single point of failure within the subsystem and thus is designed to maintain safety functions during component failure or degraded conditions that can result from malfunctions. The Tricon subsystem architecture is also designed to detect and correct individual faults on-line, without interruption of system monitoring, control, or protection capabilities. The Tricon subsystem is designed to activate an alarm, remove the affected portion of the system from operation, and perform safety functions in a dual-redundant mode when a fault occurs. The system is also designed to return to the triple-redundant mode of operation when the affected module is replaced.

Each of the Tricon main chassis are powered by two redundant power supply modules installed within the chassis. Each of these power supply modules is capable of providing the power requirements of a fully populated chassis so that all subsystem functions will be maintained when one of the two power supply modules fails. The alarm contacts for a power supply module actuate when a condition that could have significant potential for defeating the safety function exists.

ALS

The field programmable gate array (FPGA)-based ALS PPS equipment 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. Each ALS safety system cabinet contains two redundant power supplies. Each power supply is capable of providing the power requirements of the ALS cabinet load. The cabinet load consists of all ALS platform components and peripheral devices. Power supply failures (loss of output voltage) and opening of distribution breakers will actuate alarms in the control room.

Single failures are conditions that have potential for defeating the safety function, and have been evaluated (see Section 3.9.2, "IEEE 603-1991, Clause 5, System," of this safety evaluation). Environmental conditions also have significant potential for defeating the safety function, and have been evaluated (see Section 3.5.1, "Environmental Qualification of System," of this safety evaluation). Another aspect of the PPS development that has a significant potential for defeating the safety function is the security of the system development and operating environment (see Section 3.12, "Secure Development and Operational Environment," of this safety evaluation). Based on these evaluations, the NRC staff has determined that the DCPP PPS conforms to Clause 5.5.1.

3.10.1.3.2 IEEE 7-4.3.2-2003, Clause 5.5.2, Design for Test and Calibration

Clause 5.5.2 states that test and calibration functions shall not adversely affect the ability of the computer to perform its safety function, and it must be verified that the test and calibration functions do not affect computer functions that are not included in a calibration. The clause further states that verification and validation (V&V), configuration management, and quality assurance shall be required for test and calibration functions on separate computers (e.g., test and calibration computers) that provide the sole verification of test and calibration data, but that V&V, configuration management, and quality assurance is 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.

Calibration of the PPS will be performed when the portion of the system being calibrated is not performing its safety functions. Channel bypass switches are included in the PPS design to facilitate this capability. Additionally, because the PPS operating and maintenance procedures are not available for review as part of this safety evaluation; NRC inspection activities will verify that these procedures are consistent with the design capability and plant technical specifications. Refer to Section 3.14, "Site Inspection Follow-up Items," of this safety evaluation for associated the site inspection follow-up item. Based on these evaluations, the NRC staff has determined that the DCPP PPS conforms to the requirements of Clause 5.5.2.

3.10.1.3.3 IEEE 7-4.3.2-2003, Clause 5.5.3, Fault Detection and Self-Diagnostics

Clause 5.5.3 discusses fault detection and self-diagnostics, and states that if reliability requirements warrant self-diagnostics, then computer programs should contain functions to detect and report computer system faults and failures in a timely manner, and that these 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.

The reliability requirements for the PPS warrant the use of self-diagnostics functions within the system design. Both the ALS and Tricon portions of the PPS employ self-diagnostics features as a means of identifying system failures that cannot otherwise be detected. The PPS diagnostics include features that are performed during system startup and those which are performed periodically during system operation.

The self-diagnostic functions for the ALS and Tricon systems are either built into the platform design or are being implemented as part of the DCPP application. In either case, the same V&V processes that are being used for the qualification of the safety system functions are being applied to the self-diagnostics functions.

The PPS factory acceptance testing was performed with the ALS and Tricon system self-diagnostic tests running; therefore, the factory acceptance testing demonstrated that these tests did not adversely affect the ability of the PPS to perform its safety functions (see Section 3.4.2.4, "Testing Activities," of this safety evaluation). The diagnostic functions for both subsystems are designed to report test results and to actuate alarm functions via the main annunciator system to inform plant operators when conditions that could affect safety function operability exist. Based on these evaluations, the NRC staff determined that the DCPP PPS conforms to the requirements of Clause 5.5.3.

3.10.1.4 IEEE 7-4.3.2-2003, Clause 5.6, Independence

Clause 5.6 states that in addition to the requirements of IEEE Std. 603, data communication between safety channels or between safety and non-safety systems shall not inhibit the performance of the safety function. In addition, if safety and non-safety software reside on the same computer and use the same computer resources, then the non-safety software functions shall be developed in accordance with safety-related software development practices. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.6, "Independence" (Reference 42), provides acceptance criteria for equipment qualifications.

The DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance," dated March 6, 2009 (Reference 34), was developed to address communication independence.

The DCPP PPS does not include any data communication paths between protection sets (i.e., safety divisions); therefore, there is no potential for such communication to inhibit the performance of any PPS safety function. The NRC evaluation of data communication between the PPS and non-safety systems is documented in Section 3.7, "Communications," of this safety evaluation.

All 1E to non-1E communication barriers associated with the PPS are identified in the system design. These barriers are:

Tricon

- The Tricon communication module (TCM) interfaces between the Tricon and the maintenance work station and gateway switch.
- The interfaces between the Tricon local remote extender module (RXM) and the remote RXM chassis.

See Section 3.7.1, "Tricon-Based PPS Equipment Communications," of this safety evaluation for further detail on these links.

ALS

- The TxB1 communication links between the ALS chassis and the gateway switch.
- The TxB2 communication links between the ALS chassis and the ALS maintenance work station computer.
- The TAB communication link between the ALS chassis and the ALS maintenance work station computer.

See Section 3.7.2, "ALS-Based PPS Equipment Communications," of this safety evaluation for further detail on these links.

Each of these communication barriers is evaluated in Section 3.7, "Communications," of this safety evaluation to ensure that non-safety functions cannot interfere with performance of the safety functions of the PPS.

Because the DCPP PPS design establishes barriers between the safety system software and all non-safety software, the non-safety software functions did not need to be developed in accordance with the requirements of IEEE 7-4.3.2 and no evaluation of non-safety software was performed by the NRC staff.

The NRC staff evaluated communication aspects of Clause 5.6 (see Sections 3.7.1, "Tricon-Based PPS Equipment Communications," and 3.7.2, "ALS-Based PPS Equipment Communications," of this safety evaluation) and evaluated communication independence per DI&C-ISG-04 (see Section 3.7.3, "DI&C-ISG-04 Compliance," of this safety evaluation). Based on these evaluations, the NRC staff determined that the DCPP PPS conforms to Clause 5.6.

3.10.1.5 IEEE 7-4.3.2-2003, Clause 5.7, Capability for Test and Calibration

Clause 5.7 states that there are no requirements beyond those found in in IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32). Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.7, "Capability for Test and Calibration" (Reference 42), provides no acceptance criteria for IEEE Std. 7-4.3.2-2003, Clause 5.7. Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.7, "Capability for Test and Calibration" (Reference 41), states that for digital computer-based systems, test provisions should address the increased potential for subtle system failures such as data errors and references SRP Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions" (Reference 47). BTP 7-17 describes additional considerations in the evaluation of test provisions in digital computer-based systems.

The DCPP self-diagnostics test provisions evaluated under IEEE 7-4.3.2 Clause 5.5.3 above address the increased potential for system failures such as data errors. The PPS factory acceptance tests (FATs) were performed with the ALS and Tricon system self-diagnostic tests running; therefore, the FATs demonstrated that these tests did not adversely affect the ability of the PPS to perform its safety functions. The NRC staff also considered the criteria of BTP 7-17, and determined that the DCPP PPS complies with the criteria of Clause 5.7.

3.10.1.6 IEEE 7-4.3.2-2003, Clause 5.8, Information Displays

Clause 5.8 states that there are no requirements beyond those found in IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32); however, SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2" (Reference 42), states that the NRC staff should ensure that incorrect functioning of the information displays does not prevent the safety function from being performed.

The maintenance work stations are information displays that are included in the PPS. These displays are used for maintenance and surveillance testing purposes only. The PPS also provides signals to several control panel indicators.

Some of these indicators are safety-related and are considered to be part of the same protection set as the PPS subsystem that provides the signal. Because these indicators are part of the associated protection set, any single failure of such a device would only affect the associated PPS protection set and the remaining protection sets would retain the capability of performing all required safety functions. See also the evaluation of single-failure criteria in Section 3.9.2, "IEEE 603-1991, Clause 5, System," of this safety evaluation.

Other indicators are non-safety-related and are isolated from the PPS through qualified 1E safety-related devices so failures of these indicators cannot adversely affect the PPS.

The PPS was evaluated against the independence criteria of IEEE 603 and the communication independence criteria of IEEE 7-4.3.2 (see Sections 3.9.5, "IEEE 603-1991, Clause 8, Power Source Requirements," and 3.10.1, "IEEE Std. 7-4.3.2-2003, Clause 5, Safety System Criteria," of this safety evaluation). The NRC staff determined that incorrect functioning of information displays including the maintenance work stations will not prevent the PPS safety functions from being performed. Based on these evaluations, the NRC staff determined that the DCPP PPS conforms to the guidance of Clause 5.8.

3.10.1.7 IEEE 7-4.3.2-2003, Clause 5.11, Identification

Clause 5.11 states that the following identification requirements specific to software systems shall be met: (1) firmware and software identification shall be used to assure the correct software is installed in the correct hardware component; (2) means shall be included in the software such that the identification may be retrieved from the firmware using software maintenance tools; and (3) physical identification requirements of the digital computer system hardware shall be in accordance with the identification requirements in IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32). Standard Review Plan (SRP) Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.11, "Identification" (Reference 42), states that the identification should be clear and unambiguous, should include the revision level, and should be traceable to configuration control documentation that identifies the changes made by that revision.

Tricon

Software identification control for embedded software is described in Section 1.2.1 of the Triconex "Software Quality Assurance Plan (SQAP)," Revision 1, 993754-1-801-P, dated March 14, 2012 (Reference 129). Invensys maintains the embedded software and associated configuration information in its configuration management program.

Software identification control for application software is described in Section 3.1 of the Triconex "Software Configuration Management Plan (SCMP)," Revision 1, 993754-1-909-P, dated December 18, 2012 (Reference 116). The TriStation 1131 tool assigns version numbers to all of the functional software elements of the application. Elements which are used and tracked to uniquely identify software include the project version number which is incremented during each download to a controller, program version number, and an implementation identifier. Hardware identification control is described in Section 2.0 of the Triconex Approved Topical Report (Reference 29). The topical report provides a reference to the Triconex Master Configuration List.

The TriStation 1131 tool on the Tricon maintenance work station can be used to verify that the correct application version and functional elements are installed and running on the Tricon safety processors.

During an audit conducted on June 3-5, 2014, at the Invensys facilities (Reference 38), the NRC staff observed the Tricon maintenance work station application software provides an indication of the current Test Application Software Program (TSAP) version and that a Tricon software verification activity can be performed with the PPS operable. The licensee also confirmed periodic tests will be performed to verify that installed software is correct during plant operation. This audit activity was used to support development of Tricon inspection item 5 (see Section 3.14.1, "Tricon Site Inspection Follow-up Items," of this safety evaluation).

ALS

Section 2.1.5.2, "Non-Volatile Memory Device," of the Advanced Logic System Topical Report (Reference 30), describes the method for conformance with the identification requirement of Clause 5.11. Section 6.1, "Configuration Management Plan," of the "Management Plan," Revision 8, 6116-00000, dated September 2015 (Reference 105), identifies the configuration requirements applicable to satisfying Clause 5.11. This configuration management Plan specifies what project files are to be included in the Configuration Status Accounting document and where these files are to be stored.

The DCPP application-specific logic implemented on the ALS-102 core logic boards is identified by the project number, 6116, and revision level. The non-volatile memory of the ALS-102 board stores this identification information for maintenance and verification purposes. The non-volatile memory of other ALS boards is used to store DCPP-specific configuration parameters as well.

The board identification and channel configuration information can be retrieved to assure that the correct logic and channel configuration is implemented in the installed ALS system boards; however, this information cannot be changed with the boards in service. The ALS maintenance work station or ALS Service Unit is used as a means of monitoring the ALS-102 board information.

During the June 22-26, 2015, regulatory audit conducted at the Westinghouse facilities (Reference 39), the NRC staff conducted an audit activity to observe how the ALS maintenance work station can be used to verify that correct logic implementation is installed into the DCPP system core logic boards. The NRC staff determined this verification activity can be performed with the system operable. The NRC staff also determined that accessing the board's non-volatile memory requires connecting the Test ALS Bus. This audit activity was used to support development of ALS inspection item 3 (see Section 3.14.2, "ALS Site Inspection Follow-up Items," of this safety evaluation).

The following documents are used to identify the DCPP PPS software and logic implementation versions:

1. Software/logic configuration management reports (see Section 3.4.2.3, "Configuration Management Activities," of this safety evaluation)

2. System build documents (see Section 3.4.3.7, "System Build Documents," of this safety evaluation)

The NRC staff notes that there are setpoints stored in the DCPP PPS that are not controlled by these documents; therefore, measures for identifying and controlling system setpoint configuration must be taken to ensure proper system operability. See Section 3.16, "System Setpoints Evaluation," of this safety evaluation for evaluation of the PPS setpoints. Based on these evaluations, the NRC staff determined that the DCPP PPS conforms to Clause 5.11.

3.10.1.8 IEEE 7-4.3.2-2003, Clause 5.15, Reliability

Clause 5.15 states that, in addition to the requirements of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32), when reliability goals are identified, the proof of meeting the goals shall include the software. Guidance is provided in SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.15, "Reliability," and Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," Section 5.15, "Reliability" (Reference 42). SRP Appendix 7.1-D, Section 5.15, identifies Regulatory Guide 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," January 2006 (Reference 71), containing guidance regarding digital computer reliability.

The SRP Appendices 7.1-C and 7.1-D, and RG 1.152 state that quantitative reliability goals are not sufficient as a sole means of meeting the NRC's regulations for the reliability of digital computers used in safety systems.

Tricon

Reliability of the Tricon programmable logic controller computer system is addressed in the "Reliability/Availability Study for the Tricon Version 10 Programmable Logic Controller," Revision 0, 9600164-532, dated May 23, 2007 (Reference 229). The NRC staff also reviewed the "Tricon v10 Software Qualification Report," Revision 0, 9600164-535, dated August 5, 2009 (Reference 230), and the "Critical Digital Review of the Triconex Tricon V10.2.1," Revision 1, 9600164-539, dated August 4, 2009 (Reference 231), to determine the extent to which software is considered as proof for meeting system reliability goals. The NRC staff concluded that system platform and application software was adequately factored into the reliability analyses for the Tricon portion of the PPS. Invensys processes provide a means by which software errors are identified, analyzed, and corrected during software development. Field performance data was also factored into the reliability of the system.

ALS

The ALS does not utilize executable software; however, software tools are used extensively during the development processes. The NRC considers that errors in these software tools have the potential to introduce errors in the logic implementation on the field programmable gate array devices. Errors in logic implementation and measures taken to address and mitigate such errors such as independent verification and validation activities are considered within the ALS reliability analysis.

The "ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Reference 153), includes both qualitative and quantitative elements of system reliability. Qualitative elements include a failure modes and effects analysis (evaluated in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation), and a system-level hazards analysis. The quantitative elements of reliability include analyses of mean time between failure, repair time, spurious actuation rate, and surveillance test interval.

Both Invensys and Westinghouse performed reliability analyses of the respective PPS subsystems. Each of these was reviewed by the NRC staff and each considered the level of testing performed on the designed system as well as the performance history of the equipment involved.

For both of the PPS subsystems, software and logic implementation errors were factored into the reliability analysis assumptions. Both vendors utilize processes for recording and analyzing system errors identified during development. These processes are evaluated as part of the quality assurance programs in Sections 3.4.1.3, "Software/Core Logic Quality Assurance Plan," and 3.4.2.2, "V&V Analysis and Reports," of this safety evaluation. Based on these evaluations, the NRC staff determined that the DCPP PPS conforms to the guidance of Clause 5.15.

3.11 Technical Specification Changes

The regulations under 10 CFR 50.36 require that technical specifications include limiting safety system settings, limiting conditions for operations, and surveillance requirements.

Criterion 19, 1967, "Protection Systems Reliability" of the DCPP FSARU requires that Protection systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

Regulatory Guide (RG) 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0, February 1972 (Reference 58), provides guidance for periodic testing of protection system actuation functions (from sensor to actuation device input terminals). Additionally, NUREG-1431, "Standard Technical Specifications, Westinghouse Plants," Volume 1, "Specifications" (STS), and Volume 2, "Bases," April 2012 (Reference 232), provides the NRC staff precedence for plant-specific technical specifications. The NUREG-1431 STS are based on the criteria in the Final Commission Policy Statement published in the *Federal Register* on July 22, 1993 (58 FR 39132). Because the TS are part of the license, then, as described in 10 CFR 50.90, whenever a licensee desires to amend the TS, application for an amendment must be filed with the Commission fully describing the changes desired, and following as far as applicable, the form prescribed for original applications. As stated in 10 CFR 50.92(a), in determining whether an amendment to a license will be issued to the applicant, the Commission will be guided by the considerations which govern the issuance of initial licenses to the extent applicable and appropriate.

Pacific Gas and Electric Company submitted the DCPP, Units 1, and 2, proposed changes to Technical Specification 1.1, "Definitions." Because the DCPP technical specifications are common to both units, proposed technical specifications use notes and qualifiers, as appropriate, to differentiate the technical specification requirements for operation with the Tricon/ALS PPS and with the Eagle 21 PPS.

No changes to surveillance requirements or surveillance frequencies are being requested and no changes to required action completion times are being made as a result of the PPS upgrade.

Each of the PPS replacement subsystems differ in methods for detecting functional failures. Each of the replacement PPS subsystems uses self-contained diagnostic testing, which can be credited for surveillance testing of PPS functions. These diagnostics features have been evaluated as part of the safety evaluations for the Triconex Approved Topical Report (Reference 29) and the Advanced Logic System Topical Report (Reference 30). Additionally, PPS setpoints are stored in digital memory and are therefore not subject to drift as are setpoints in analog systems. The licensee is revising the PPS testing and calibration procedures to accommodate technical specification requirements that PPS channels must be periodically tested during facility operation and calibrated from sensor to final actuation device during facility outages.

The PPS digital protective channels are divided into the following three portions:

1. The portion of the channel unique to each sensor input, which would include the sensor and input circuitry,

2. The digital portion of the channel which is common to multiple protective action signals, and

3. The output of actuation signals to the solid state protection system.

Consideration of the overall channel in this manner allows for a number of considerations regarding failures and testing methods. The failure of a sensor causes an entire channel within a protection set to be out of service.

Another type of failure to consider is the failure of the digital portion of the channel. For the DCPP PPS Tricon subsystem, input consolidation and signal processing is performed by a set of three safety function processors for each protection set. The failure of all signal processors in a protection set affects all of the Tricon safety functions being processed within that protection set. If a hardware or software failure causes the Tricon portion of the overall protection set to stop functioning, then one redundancy is lost for every Tricon protective function provided by this protection set.

The ALS subsystem consolidates inputs into core logic boards for each protection set where system signal processing is performed; however, two separate and diverse implementations core logic which are designed to perform identical safety functions are being implemented in the PPS design. The failure of one protection set core logic board affects only one of these two processing circuits and the ALS safety functions for that protection set will not be affected.

Several activities are performed to verify proper and accurate functionality of individual input portions of each protection set. These are channel calibration, channel operational tests, channel functional tests, and channel checks. The requirement to calibrate the sensors is not being revised because the PPS sensors are not being changed as a part of this modification. The channel functional test to verify channel operability is also not being changed so the replacement PPS will be functionally tested in the same manner in which the existing Eagle 21 system is currently being tested.

Instrument channel checks are a qualitative assessment, by observation, of channel behavior during operation. Channel check determinations include comparison of the channel indication and status to other indications or status derived from independent instrument channels measuring the same parameter. For DCPP, the channel check is a comparison of a plant parameter as indicated on one protection set to the same plant parameter on other protection sets. Channel checks are performed to determine if the values are approximately the same and are used as an indication of proper operation of the sensor and input circuitry. Channel checks will continue to be performed manually by DCPP personnel as a means of determining PPS operability during plant operation.

The licensee is revising the definition of the term "Channel Operability Test" as follows:

Channel Operational Test (COT):

Current Definition:

> 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.

Revised Definition:

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 NRC guidance on self-test and surveillance test provisions is contained in Standard Review Plan (SRP), Chapter 7, Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions" (Reference 47). These guidelines are based on reviews of applicant/licensee submittals and vendor topical submittals describing self-test and surveillance test assumptions, terminology, methodology, and experience gained from NRC inspections of operating plants.

Continuous self-monitoring and online diagnostics (which are implemented as a continuous test process in each Tricon processor and input/output module) provide a means of detecting hardware and software faults. The Tricon processor and input/output module diagnostics and self-test capabilities are described and evaluated in Sections 3.1.2.7, "3008N main processor Modules," 3.1.2.8, "Input/Output Modules," and 3.4.3, "Diagnostics and Self-Test Capabilities," of the safety evaluation for Triconex Approved Topical Report (Reference 29). Tricon system module self-diagnostic features are designed to detect single failures within the associated modules. The cyclic self-monitoring task checks the functions of the Tricon processors and the connected components during operation while retaining the capability to accomplish its safety functions.

The ALS platform diagnostics are described and evaluated in Section 3.4.3, "Self-Diagnostics, Test and Calibration Capabilities," of the safety evaluation for the Advanced Logic System Topical Report (Reference 30). The ALS platform supports test and calibration from field input to instrument output without lifting of leads or installation of jumpers. Design features for maintenance allow an individual instrument input or output channel to be disabled, placed into bypass, or placed into calibration. The field terminal block design also allows the injection of test signals without lifting leads to field wiring. With this approach, the test signal can be injected at the field terminal blocks and then processed through the ALS platform using the actual safety signal path. The ALS platform architecture and communication protocols also include design features to verify continued logic processing and the correctness of data.

The revised channel operational test definition provides separate and more appropriate definitions for analog and digital components of the PPS channels. Since DCPP, Units 1 and 2, will have the Tricon/ALS PPS replacement installations completed at different times and due to existing instrumentation technical specification requirements; it is necessary to include both analog and Eagle 21 PPS as well as Tricon/ALS PPS surveillance test requirements within the channel operational test definition. The online diagnostic programs provide a means of detecting hardware faults and of simulating process data into a channel to verify the channel operability of all devices in the channel. In the safety evaluation for the Triconex Approved Topical Report, the NRC staff determined that the Tricon V10 meets the criteria of RG 1.22, RG 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995 (Reference 69), and IEEE Std. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems" (Reference 70).

The NRC staff determined that the DCPP PPS is designed for in-service testability commensurate with the safety functions to be performed through all modes of plant operation. The staff also determined that the positive aspects of the PPS self-test features are not compromised by the additional complexity that has been added to the safety system. The revised PPS hardware and software design will continue to support required periodic testing of the system. The Failure Modes and Effects Analyses performed for the PPS, as evaluated in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation, adequately identifies the means of detecting assumed failure modes within the PPS.

The NRC staff determined that the revised technical specification definition of "Channel Operability Test (COT)," satisfies 10 CFR 50.36(c)(3) because this definition assures that the necessary quality of systems and components is maintained, that the facility will be operated within safety limits, and that the limiting conditions for operation will be met.. Furthermore, the NRC staff determined that the self-test features of the revised PPS satisfy the criteria of BTP 7-17. Based on the above, the NRC staff concludes that the proposed revision to the definition of Channel Operability Test is acceptable.

3.12 Secure Development and Operational Environment

Regulatory Guide (RG) 1.152, Revision 3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," July 2011 (Reference 71), describes a method that the NRC considers acceptable to comply with the regulatory criteria to promote high functional reliability, design quality, and establish secure development and operational environments (SDOEs) for the use of digital computers in safety-related systems at nuclear power plants. The overall guidance provides the basis for physical and logical access controls to be established throughout the digital system development process to address the susceptibility of a digital safety system to inadvertent access and modification.

A secure development environment must be established to ensure that unneeded, unwanted, and undocumented code is not introduced into a digital safety system—either operating system software or application software. A secure operational environment must be established to ensure that predictable, non-malicious events will not degrade the reliable performance of the safety system. Regulatory Positions 2.1-2.5 of RG 1.152 specifically identify analyses and associated design activities that should be addressed during the safety-related system development. 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.

Pacific Gas and Electric Company (PG&E, the licensee), Invensys Operations Management (IOM), and Westinghouse Electric Company LLC (Westinghouse) are responsible for establishing the SDOE controls of the DCPP PPS replacement project. The licensee's letter dated December 20, 2011 (Reference 2), provides a description of the security features and controls implemented to establish an SDOE. The licensee also made reference to the IOM and Westinghouse documents that addressed the SDOE.

Tricon

The NRC staff's SDOE evaluation of the Tricon V10 platform is documented in Section 3.8 of the safety evaluation for the Triconex Approved Topical Report (Reference 29). The staff's evaluation of the topical report concluded that the Tricon V10 platform was developed and is maintained in a secure development environment. For the DCPP PPS replacement project, IOM prepared the "Regulatory Guide 1.152 Conformance Report," Revision 0, 993754-1-913-P, dated September 6, 2011 (Reference 128), which identifies the lifecycle vulnerabilities for the Tricon V10 PPS replacement and the associated mitigation measures.

ALS

The NRC staff's SDOE evaluation of the ALS platform is documented in Section 3.8 of the safety evaluation for the Advanced Logic System Topical Report (Reference 30). The staff's evaluation of the topical report concluded that the ALS platform was developed and is maintained in a secure development environment. For the DCPP PPS replacement project, Westinghouse did not prepare a separate RG 1.152 conformance report. Instead, Westinghouse followed the SDOE control mechanisms established for the ALS platform, as described in the "ALS Security Plan," Revision 3, 6002-00006, dated May 2014 (Reference 233). The ALS Security Plan identifies the lifecycle vulnerabilities for the ALS PPS replacement and the associated mitigation measures.

Several specific platform design features that support a secure operational environment were addressed in the respective topical report safety evaluations. Those features are discussed below in the evaluation of the PPS replacement secure operational environment.

3.12.1 Lifecycle Phases

Regulatory Guide (RG) 1.152, Revision 3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," July 2011 (Reference 71), uses the lifecycle phases of the waterfall model as a framework for describing specific guidance for the protection of digital safety systems and the establishment of a secure development and operational environment (SDOE) for those systems. The regulatory guide states the digital safety system development process should identify and mitigate potential weakness or vulnerabilities in each phase of the digital safety system lifecycle that may degrade the SDOE or degrade the reliability of the system.

The Invensys Operations Management (IOM) and Westinghouse lifecycle frameworks do not match one to one against the lifecycle phases identified in RG 1.152. Table 3.12.1-1 compares the IOM Nuclear Systems Integration Program Manual and Westinghouse development phases with RG 1.152.

RG 1.152	IOM	Westinghouse
Concepts	Acquisition and Planning	Planning
Requirements	Requirements	
Design	Design	Development
Implementation	Implementation	Manufacturing
Test	Test	
Installation, Checkout, and Acceptance Testing	Delivery	System Test, Installation, and Maintenance
Operation		
Maintenance		
Retirement		

Table 3.12.1-1 Lifecycle Phases Comparison

3.12.1.1 Concepts Phase

3.12.1.1.1 Identification of Secure Operational Environment Design Features

As stated in the Regulatory Position 2.1 of RG 1.152 (Reference 71), the concepts phase is the phase in which the licensee should identify digital safety system design features required to establish a secure operational environment for the system and describe these design features as part of its application.

Licensee

The licensee identified the following PPS replacement secure operational environment design features in the Functional Requirements Specification (Reference 126):

- Physical Security - The PPS processing instrumentation shall have provisions for accommodating physical security devices such as keylocks, cabinet locks, etc., to ensure that only appropriate personnel have access to the PPS processing instrumentation.
- System Logon Protection - Access to the PPS processing instrumentation will be administratively controlled using physical security and/or password logon security measures (as applicable).
- Communications with External (Non-PPS) Systems - All communications between external systems/devices and the PPS instrumentation shall be read only by the external system.

Pacific Gas and Electric Company's letter dated December 20, 2011 (Reference 2), identified the security features and controls within the PPS replacement component cabinets and in the interfacing components. **[[**

]].

Tricon

The following Tricon V10 platform features protect against failure of a single module, removing the wrong module during maintenance, unauthorized or unintended application code changes, and ensure a controlled firmware upgrade process for the Tricon V10 modules:

[[

•

]]

ALS

The following ALS platform features protect against unauthorized and inadvertent access that could impede the safety functions:

[[

]].

Based on the information reviewed by the NRC staff, the licensee has identified the design features required to establish a secure operational environment and, therefore, meets the criteria of Regulatory Position 2.1 of RG 1.152 for the DCPP PPS replacement.

3.12.1.1.2 Assessment of Potential Susceptibilities

Regulatory Guide (RG) 1.152 (Reference 71) states that licensees should assess the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's lifecycle that could degrade its reliable operation.

Both IOM and Westinghouse performed vulnerability assessments of their respective platforms to ensure the PPS replacement system is protected from unauthorized access and modification throughout the safety system lifecycle in accordance with RG 1.152.

Tricon

The Tricon PPS replacement "Regulatory Guide 1.152 Conformance Report" (Reference 128), provides a list of vulnerabilities and mitigation measures for the Tricon V10 PPS replacement. These vulnerabilities address physical and network access controls, personnel security, administrative controls, and application program configuration and source code controls. Appendix A of the Tricon Regulatory Guide 1.152 Conformance Report provides a list potential vulnerabilities of the Tricon PPS replacement that are not mitigated by platform or application design. These vulnerabilities are mitigated by physical, logical, and administrative controls.

To confirm the secure development environment evaluated for the Tricon V10 platform continues to meet the guidance of RG 1.152, PG&E audited the Tricon development facilities. The PG&E cyber security project manager accompanied members of the PG&E quality verification group to examine the IOM design and production facilities in Lake Forest, California during the November 13-16, 2012, regulatory audit (Reference 36). These activities included examining the code production practices, security controls, and the application development environments. PG&E determined IOM had maintained a secure development environment in accordance with NRC RG 1.152.

ALS

Appendix A of the ALS Security Plan (Reference 233) provides a list of vulnerabilities and mitigation measures for the ALS PPS replacement. These include unintentional changes caused by employees or software due to lack of training, negligence, ambiguous procedures, unintuitive procedures, flawed software tools, etc. Westinghouse performed a security assessment for compliance of plans and processes against cyber security regulations regarding the establishment of a secure development environment. These vulnerabilities are mitigated by physical, logical, and administrative controls.

To confirm that the secure development environment evaluated for the ALS platform continues to meet the guidance of RG 1.152, PG&E audited the ALS development facilities. The cyber security supervisor accompanied members of the PG&E quality verification group to examine the Westinghouse (previously CS Innovations) design and production facilities in Scottsdale, Arizona. These activities included examining the code production practices, security controls, and the application development environments. PG&E determined Westinghouse had maintained a secure development environment in accordance with NRC RG 1.152.

Based on the information reviewed by the NRC staff, the licensee has assessed the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's lifecycle and, therefore, meets the criteria of Regulatory Position 2.1 of RG 1.152 for the DCPP PPS replacement.

3.12.1.1.3 Remote Access

The guidance in Regulatory Position 2.1 of RG 1.152 (Reference 71), states that licensees should not allow remote access to the safety system. In RG 1.152, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).

By letter dated December 20, 2011 (Reference 2), PG&E identified the security features and controls outside PPS replacement layer. The PPS replacement design does not allow for remote access to the Tricon or ALS platforms. There is one Tricon maintenance work station and one ALS maintenance work station per protection set which only communicate with the safety-related controllers in that protection set. **[[**

]]. There are no communication paths between the redundant protection sets in either the Tricon portion or the ALS portion of the PPS replacement. The safety and reliability of the communication between the safety-related platforms and the non-safety maintenance work stations is discussed in Section 3.7, "Communications," of this safety evaluation.

Tricon

Two-way communication is only allowed between the Tricon Communications Module and the Tricon maintenance work station by means of the port aggregator network tap device. The port tap permits only one-way communication between the Tricon processors and the packet data network gateway computer. The NRC staff's evaluation of the port tap is contained in Section 3.1.7.3, "Port Tap Aggregator," of this safety evaluation. The electrical isolation provided by the fiber optic cables and the data isolation provided by the port aggregator tap and the Tricon Communications Module prevent that a fault or failure within the packet data network gateway computer or the maintenance work station will adversely affect the ability of the PPS to accomplish its safety functions.

ALS

Two-way communication is only allowed between the ALS and the ALS maintenance work station through the use of the Test ALS Bus. The ALS Service Unit Test ALS Bus is not connected to the ALS during normal operation, and the pathway exists only when the ALS Service Unit is being used in a test or maintenance mode. The ALS platform uses a simple serial communication scheme based on Recommended Standard (RS)-485, and does not support advanced communications ports and protocols, such as the Institute for Electrical and Electronics Engineers (IEEE) 802.x protocols. The core logic board contains serial one-way transmit-only communication links. These links transmit only and no data from the outside of the ALS can be received.

Based on the information reviewed by the NRC staff, the licensee does not allow remote access to the safety system and, therefore, meets the criteria of Regulatory Position 2.1 of RG 1.152 for the DCPP PPS replacement.

3.12.1.2 Requirements Phase

Regulatory Position 2.2 of RG 1.152 (Reference 71), describes the secure development and operational environment (SDOE) activities to be performed during the requirements phase of system development.

3.12.1.2.1 Definition of Secure Operational Environment Functional Requirements

Section 2.2.1 of RG 1.152 states, in part, that "the licensee should define the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance."

The licensee identified the SDOE functional performance requirements for the PPS replacement in the DCPP Interface Requirements Specification (Reference 98). One of these requirements calls for the safety-related PPS application software to be developed in an SDOE per RG 1.152. Based on the design features and vulnerabilities identified in the concepts phase, the licensee identified the following functional performance requirement areas:

- Account management
- Access enforcement (e.g., privileged functions, access levels, etc.)
- System use notification
- Password requirements
- System hardening
- Maintenance work station startup automatic login

Based on the information reviewed by the NRC staff, the licensee has defined the functional performance requirements and system configuration for a secure operational environment and, therefore, meets the criteria of Regulatory Position 2.2 of RG 1.152 for the DCPP PPS replacement.

3.12.1.2.2 Verification of SDOE Requirements

Regulatory Position 2.2 of RG 1.152 states, in part, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE feature.

Tricon

The Tricon DCPP PPS replacement Regulatory Guide 1.152 Conformance Report (Reference 128) states that all requirements of the system, including security features, are validated and certified. For the Tricon V10-based PPS, the development process for safety-related application software is governed by the Invensys Nuclear Systems Integration Program Manual (Reference 112). In compliance with the Nuclear Systems Integration Program Manual, the PPS replacement "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), describes the project verification and validation activities.

Invensys nuclear independent verification and validation (IV&V) uses the Tricon "Project Traceability Matrix" (Reference 103) to confirm the forward and backward traceability of the overall system requirements between the project design inputs and design outputs, including security requirements. Both the Tricon Project Traceability Matrix and the ALS subsystem Requirements Traceability Matrix (Reference 161) provide a means by which system design requirements can be traced between the design implementation documents and the Functional Requirements Specification and Interface Requirements Specification.

ALS

The ALS Security Plan (Reference 233) states that all requirements and design documentation shall be controlled to ensure documents are adequately protected from inadvertent changes that could adversely affect security. This procedure describes the process to ensure adequate and correct documents are used, including identification, preparation, review and approval, issuances, and change control.

Additionally, Westinghouse IV&V activities cover safety-related field programmable gate array (FPGA) design outputs, by document and source code review or by simulation. The independent reviews and simulations ensure that no undocumented and unwanted code has been incorporated into the design that could adversely affect security.

Based on the information reviewed by the NRC staff, the licensee has taken measures to ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE features and, therefore, meets the criteria of Regulatory Position 2.2 of RG 1.152 for the DCPP PPS replacement.

3.12.1.2.3 Use of Predeveloped Software and Systems

Section 2.2.1 of RG 1.152, "System Features," further states the requirements specifying the use of pre-developed software and systems (e.g., reused software and commercial off-the-shelf systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).

Tricon

Invensys Operations Management notes in the DCPP PPS replacement Regulatory Guide 1.152 Conformance Report (Reference 128) that the Tricon V10 application software for the PPS replacement was developed specifically for the DCPP PPS design and does not use predeveloped software beyond the nuclear-qualified TriStation 1131 programming software. Project procedures require the development of various documents such as a software quality assurance plan, software requirements specification, software verification and validation plan, test procedures, and that all software is tested and validated.

ALS

Westinghouse notes in the ALS Security Plan that any source code developed prior to an isolated development infrastructure development network being available shall be evaluated to verify the integrity, reliability, and functionality of the safety-related FPGA or software. Additionally, all source code developed outside the protection of an isolated development infrastructure development network shall be ported to an isolated development infrastructure; recompiled, retested, and complete IV&V of the code shall be performed.

Based on the information reviewed by the NRC staff, the licensee has accounted for the use of predeveloped software and implemented controls and procedures to maintain the reliability of the safety system and, therefore, meets the criteria of Regulatory Position 2.2 of RG 1.152 for the DCPP PPS replacement.

3.12.1.2.4 Prevention of Unnecessary Requirements

The guidance in RG 1.152 states the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.

Tricon

The DCPP PPS Regulatory Guide 1.152 Conformance Report (Reference 128) states that during development of the PPS application program, peer reviews are performed on documents, logic, tests, and other electronic documents to ensure that the contents are complete, logical, correct, and also that the Tricon and TriStation 1131 designs include only the required functionality. These activities eliminate the possibility of inadvertent or malicious injection of faults and failures into the system and application program logic.

ALS

The ALS Security Plan states that design-related documentation, configuration items and electronic design assets created during the concept and requirements phases address internal and external threats, unintended functions and unauthorized access using the following methods. Requirement documents are reviewed using the IV&V process according to the "ALS V&V Plan," Revision 8, 6002-00003-P, January 2013 (Reference 134). These methods ensure that the ALS platform is correct, accurate, and complete per the security-related ALS platform requirements.

Based on the information reviewed by the NRC staff, the licensee has taken measures to prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code and, therefore, meets the criteria of Regulatory Position 2.2 of RG 1.152 for the DCPP PPS replacement.

3.12.1.3 Design Phase

Regulatory Position 2.3 of RG 1.152 (Reference 71), describes the SDOE activities to be performed during the design phase of system development.

3.12.1.3.1 Translation of SDOE Requirements into Design Configuration Items

The guidance in RG 1.152 states the safety system design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description.

Tricon

The Tricon V10 PPS replacement application configuration items addressing a secure operational environment are identified in the PPS "Software Requirements Specification (SRS)," Revision 4, 993754-11-809-P, dated January 21, 2014 (Reference 166); "Software Requirements Specification (SRS), Protection Set II," Revision 2, 993754-12-809-P, dated October 17, 2012 (Reference 167); "Software Requirements Specification (SRS), Protection Set III," Revision 2, 993754-13-809-P, dated October 17, 2012 (Reference 168); and "Software Requirements Specification (SRS), Protection Set IV," Revision 2, 993754-14-809-P, dated October 17, 2012 (Reference 169), and "Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102). These configuration items include:

- System Logon Protection

  [[

  -

  ]]

- Communications with External (non-Tricon Protection Set) Systems

  - [[ ]]

- Safety and Security Considerations

  [[

-

]]

ALS

The ALS PPS replacement application configuration items addressing a secure operational environment are identified in the ALS Subsystem "System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127). These configuration items include:

- Security

  [[

  -

  ]]

- Access Control

  [[

  -

  ]]

- System Hardening Documentation

  - [[

-

]]

Based on the information reviewed by the NRC staff, the licensee has translated the safety system design features for a secure operational environment into design configuration items to ensure reliable system operation. Therefore, the licensee meets the criteria of Regulatory Position 2.3 of RG 1.152 for the DCPP PPS replacement.

3.12.1.3.2 Physical and Logical Access Controls

The guidance in RG 1.152 states, in part, that physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the lifecycle.

In the concepts phase, both Invensys Operations Management (IOM) and Westinghouse performed vulnerability assessments of their respective platforms to ensure the PPS replacement system is protected from unauthorized access and modification throughout the safety system lifecycle, in accordance with RG 1.152. These vulnerabilities are mitigated by the following physical, logical, and administrative controls:

3.12.1.3.2.1 Secure Development Environment Controls

Tricon

The Tricon safety-related nuclear system integration for the PPS replacement project was performed at the IOM facility in Irvine, California, and later in Lake Forest, California. These facilities implemented physical and logical access control features to prevent the unauthorized access or alteration (inadvertent or by unauthorized personnel) of media or electronic versions of the application program during the project lifecycle defined in the Nuclear Systems Integration Program Manual (Reference 112). **[[**

]]

Security controls are provided to prevent unauthorized changes via network connections during engineering development and nuclear system integration projects. **[[**

]]

ALS

The ALS safety-related nuclear system integration for the PPS replacement project was performed at the Westinghouse facility in Scottsdale, Arizona, and later at the Westinghouse facility in Warrendale, Pennsylvania. These facilities implemented access control features to prevent unauthorized physical access to the development areas. **[[**

]]

3.12.1.3.2.2 Secure Operational Environment Controls

Tricon

[[

]]

The Tricon keyswitch position is voted between the three 3008N main processors and the voted value is used to perform keyswitch functions. The PPS replacement application software provides a general "protection set trouble" alarm output when the voted keyswitch position changes.

Two-way communication is only allowed between the Tricon Communications Module and the Tricon maintenance work station by means of the port aggregator network tap device. The port tap permits only one-way communication between the Tricon processors and the Packet Data Network (PDN) gateway computer. The staff's evaluation of the port tap is contained in

Section 3.1.7.3, "Port Tap Aggregator," of this safety evaluation. The data isolation provided by the port aggregator tap and the Tricon Communications Module prevent that a fault or failure within the PDN gateway computer or the maintenance work station will adversely affect the ability of the PPS to accomplish its safety functions.

ALS

[[

]]

The field programmable gate array (FPGA) contents cannot be modified while in service. In addition, any FPGA contents must be implemented based on ALS proprietary architecture; otherwise, the board is rejected by the ALS system.

[[

]]

Two-way communication is only allowed between the ALS and the ALS maintenance work station through the use of the Test ALS Bus. The ALS Service Unit Test ALS Bus is not connected to the ALS during normal operation, and the pathway exists only when the ALS Service Unit is being used in a test or maintenance mode.

Based on the information reviewed by the NRC staff, the licensee has implemented physical and logical access control features based on the results of the assessment performed in the concepts phase of the lifecycle and, therefore, meets the criteria of Regulatory Position 2.3 of RG 1.152 for the DCPP PPS replacement.

3.12.1.3.3 Prevention of Unnecessary Design Features

The guidance in RG 1.152 states that during the design phase, measures should be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.

Tricon

For the Tricon PPS replacement configuration, the development process for safety-related application software is governed by the Nuclear Systems Integration Program Manual (Reference 112) and supporting Project Procedures Manual procedures. The PPS replacement

"Project Management Plan (PMP)," Revision 3, 993754-1-905-P, dated December 18, 2012 (Reference 114), describes the security requirements at the project level based on PG&E design inputs. The "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), discusses independent verification and validation (IV&V) activities required for the V&V effort. The "Software Safety Plan (SSP)," Revision 1, 993754-1-911-P, dated October 13, 2011 (Reference 119), discusses the types of analyses performed.

ALS

Westinghouse performed a software design evaluation to evaluate the FPGA Design Specification documents and to ensure the FPGA design satisfies the requirements in the Software FPGA Requirements, does not introduce unintended features, and provides the information necessary to generate the FPGA design. Westinghouse verification and validation (V&V) performed line-by-line reviews of the FPGA hardware descriptive language listings to prevent inadvertent coding.

Based on the information reviewed by the NRC staff, the licensee has taken measures to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code and, therefore, meets the criteria of Regulatory Position 2.3 of RG 1.152 for the DCPP PPS replacement.

3.12.1.4 Implementation Phase

Regulatory Position 2.4 of RG 1.152, Revision 3 (Reference 71), describes the secure development and operational environment (SDOE) activities to be performed during the implementation phase of system development.

3.12.1.4.1 Transformation from System Design Specification to Design Configuration Items

The guidance in RG 1.152 states the developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.

Tricon

The Nuclear Systems Integration Program Manual and supporting quality assurance procedures define the integration process controls for all phases of the project to assure the functional system requirements are correctly and completely translated. Project Procedures Manual procedures define the software development process actions, including periodic application code reviews during implementation. The software design review requires, in part, structural walk-through of the Tricon application program based on PG&E requirements. The application code walk-through ensures that all design configuration items from the "Software Design

Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102), implemented in the application code correctly, accurately, and completely.

Invensys Operations Management Nuclear IV&V uses the PPS replacement "Project Traceability Matrix," Revision 1, 993754-1-804-P, dated October 17, 2012 (Reference 103), to confirm the forward and backward traceability of the overall system requirements between the project design inputs and design outputs, including security requirements. Nuclear IV&V also independently confirms that all design configuration items from the Software Design Description have been implemented in the application code.

ALS

Westinghouse performs a software design evaluation to evaluate the FPGA Design Specification documents to ensure that the FPGA design satisfies the requirements in the Software FPGA Requirements, does not introduce unintended features, and provides the information necessary to generate the FPGA design. Westinghouse uses the PPS replacement "ALS Subsystem Requirements Traceability Matrix," Revision 3, 6116-00059, November 2014 (Reference 161), to document the V&V of specified requirements.

Based on the information reviewed by the NRC staff, the developers have ensured that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete. Therefore, the licensee meets the criteria of Regulatory Position 2.3 of RG 1.152 for the DCPP PPS replacement.

3.12.1.4.2 Implementation of Secure Development Environment Procedures and Standards

The guidance in RG 1.152 states the developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system.

Tricon

For the Tricon PPS replacement configuration, the development process for safety-related application software is governed by the Nuclear Systems Integration Program Manual and supporting Project Procedures Manual procedures: the PPS replacement project "Project Management Plan (PMP)," Revision 3, 993754-1-905-P, dated December 18, 2012 (Reference 114), describes the security requirements at the project level based on PG&E design inputs; the "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), discusses IV&V activities required for the V&V effort; the "Software Safety Plan (SSP)," Revision 1, 993754-1-911-P, dated October 13, 2011 (Reference 119), discusses the types of analyses performed; and the project Coding Guidelines referenced in the "Software Development Plan (SDP)," Revision 2, 993754-1-906-P, dated December 18, 2012 (Reference 115), contain guidance to the Nuclear Delivery design team relevant to configuration of the TriStation 1131 application program.

During the June 3-5, 2014 audit of IOM (Reference 38), the NRC staff reviewed IOM Project Instruction 6.1, "Secure Development Laptop Control," which defines the requirements for securing the laptops for development of the Test System Application Program (TSAP) associated with the PG&E DCPP PPS replacement project. The requirements in this project instruction ensure that only authorized personnel have access to the software and that no unintended code is allowed into the software.

ALS

Westinghouse's secure development procedures are contained in the ALS Security Plan (Reference 233) and the ALS V&V Plan (Reference 134). During the NRC staff's June 22-26, 2015, audit of Westinghouse (Reference 39), the staff reviewed the Westinghouse "NA Cyber Security Program" which addresses the secure development and test environment where standard and project-specific software development will occur. This program references physical and cyber security guidelines for controlling the isolated development infrastructure and the development and test environment, as well as training expectations for Westinghouse employees and contractors.

During the audit, the NRC staff also reviewed the Westinghouse Isolated Development Infrastructure Requirements, which contain the requirements established for the isolated development infrastructure and associated development and test environment. These requirements cover isolated development infrastructure network monitoring, isolated development infrastructure work stations, control of portable media, user accounts, and software installation.

Based on the information reviewed by the NRC staff, the licensee has implemented secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system and, therefore, meets the criteria of Regulatory Position 2.4 of RG 1.152 for the DCPP PPS replacement.

3.12.1.4.3 Accounting for Hidden Functions in the Code

The guidance in RG 1.152 states the developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system.

Tricon

The IOM Project Procedures Manual procedures implementing the Nuclear Systems Integration Program Manual (Reference 112) define the detailed software development process actions, including periodic application code reviews during implementation. The IOM Nuclear Systems Integration Program Manual requires that security requirements have traceability through system integration testing. Invensys addresses these requirements, in part, through code reviews and walkthroughs of the PPS replacement Tricon V10 application software to prevent undocumented codes (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely impact the reliable operation of the digital system.

The application code walk-through ensures that all application code features are traceable back to the system specifications, thus accounting for hidden and vulnerable functions in the application code.

<u>ALS</u>

Westinghouse V&V activities are responsible for determining all software requirements are implemented and there is no unintended functionality existing in the software which does not satisfy the software requirements. This is accomplished by performing software design evaluation and source code evaluation, which evaluates the actual software produced by the design team to ensure that it satisfies the software design specification without introducing unintended features. The source code is evaluated against a set of attributes and coding standards.

Source code development is completed, maintained under configuration management, and available on the isolated development infrastructure. Westinghouse IV&V performs code, synthesis and coverage reviews on the FPGA register transfer level code to identify commented out functional code, debug code, and any other undesired remnants from the design process that could constitute unintended functionality.

Based on the information reviewed by the NRC staff, the licensee has accounted for hidden functions and vulnerable features embedded in the code, their purpose, and their impact on the integrity and reliability of the safety system. Therefore, the licensee meets the criteria of Regulatory Position 2.4 of RG 1.152 for the DCPP PPS replacement.

3.12.1.5 Test Phase

Regulatory Position 2.5 of RG 1.152 (Reference 71), describes the secure development and operational environment activities to be performed during the test phase of system development.

3.12.1.5.1 Validation of Secure Operational Environment Design Configuration Items

The guidance in RG 1.152 states the secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items.

<u>Tricon</u>

In accordance with the Nuclear Systems Integration Program Manual and Project Procedures Manual procedures, the Tricon V10 application program is verified and the combined hardware-software system is validated such that every system feature, including security features, is tested. The on-line test and calibration functions are tested to ensure that the Tricon V10 protection set safety function is not adversely impacted by undesirable operation of the maintenance work station and inadvertent operator action during testing. **[[**

]]

ALS

The DCPP ALS "Test Plan," Revision 4, 6116-00005, October 2014 (Reference 134), notes that code coverage statistics are collected on all register transfer level files during simulation runs and evaluated. The goal for code coverage is 100 percent justified statement and branch. If this goal is not achievable due to practical limitations, justifications will be provided in the associated IV&V Summary Report.

Based on the information reviewed by the NRC staff, the licensee has validated the secure operational environment design requirements and, therefore, meets the criteria of Regulatory Position 2.5 of RG 1.152 for the DCPP PPS replacement.

3.12.1.5.2 Configuration of Secure Operational Environment Design Features

The guidance in RG 1.152 states the developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity.

Licensee

After development and delivery of the software from the vendors to PG&E, DCPP procedures CF2, Revision 8, Computer Hardware, Software, and Database Control (Reference 106), CF2.ID2, Revision 10, Software Configuration Management for Plant Operations and Operations Support (Reference 107), and CF2.ID9, Revision 2, Software Quality Assurance for Software Development (Reference 108), provide the DCPP station control procedures for software configuration management throughout the remaining lifecycle phases under the control of PG&E. In addition, a project-specific "System Quality Assurance Plan (SyQAP), Nuclear Safety Related," Revision 1, dated May 9, 2013 (Reference 110), and "System Verification and Validation Plan (SyVVP), Nuclear Safety Related," Revision 1, dated February 19, 2013 (Reference 111), have been developed by PG&E to control and administer the software during all lifecycle phases.

Pacific Gas and Electric Company (PG&E) Program Directive CF2 establishes overall policies and general requirements related to the quality and security of computer hardware, software, and database control processes for the plant. Program Directive CF2 notes that access to systems shall be controlled as needed to prevent unauthorized changes. The licensee's CF2.ID2 identifies requirements for preparing the software configuration management plan and software quality assurance plan and maintaining configuration control of computer systems and applications.

Using CF2.ID2, PG&E prepared "SCM 36-01, Revision 1, Process Protection System Replacement Software Configuration Management Plan (SCMP)," dated March 18, 2013 (Reference 143), 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 PG&E project integration and test facility, and for the remainder of its lifecycle following installation at DCPP, including the operation phase and maintenance phase. This plan states that changes or upgrades to the Tricon application program would be performed by IOM, and changes or upgrades to the code in the ALS platform would be performed by Westinghouse. In the SyQAP, PG&E notes it will not perform software modifications following factory acceptance testing. If any modifications are necessary, they will be performed by the 10 CFR 50 Appendix B suppliers.

Tricon

For the PPS replacement application program, the "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), describes the IV&V activities for independently verifying and validating each engineering software feature, including security features. The on-line test and calibration functions are tested to ensure that the Tricon protection set safety function is not adversely impacted by undesirable operation of the maintenance work station and inadvertent operator action during testing. **[[**

]], Hardware Design Description, and Software Design Description. Invensys verified the validation testing tool and methods could not modify the TSAP or introduce new hazards.

ALS

Testing is performed during the test phase to verify that all requirements are implemented as intended. **[[**

]]

The field programmable gate array (FPGA) configuration can only be modified by removing the ALS board from the chassis which will generate a trouble alarm. It is not possible to change the configuration of an FPGA by modifying only part of the already configured FPGA image. The licensee will have limited capability to change the non-volatile random access memory configuration for a specific ALS input/output board to support board replacement (such as to replace a failed board) by loading non-volatile random access memory images that are under Westinghouse configuration control and that have been previously verified and validated at the system level by Westinghouse. Configuring the non-volatile random access memory in order to replace an ALS input/output board will be performed by PG&E under an approved plant maintenance procedure.

Based on the information reviewed by the NRC staff, the licensee has configured and enabled the design features of the secure operational environment and, therefore, meets the criteria of Regulatory Position 2.5 of RG 1.152 for the DCPP PPS replacement.

3.13 Plant-Specific Action Items Identified in Platform Topical Report Safety Evaluations

3.13.1 Tricon V10 PSAIs

Section 4.2, "Plant Specific Action Items," of the safety evaluation for the Triconex Approved Topical Report (Reference 29) identified 19 plant-specific action items (PSAIs) to be addressed by Pacific Gas and Electric Company (PG&E, the licensee) during the development of a safety-related system using Tricon V10 platform. The following is the NRC's assessment of the licensee's compliance with each of these items:

1. As noted in Section 2.1, "Scope of Triconex Platform Changes V9.5.3 to V10.5.1," of the Tricon V10 safety evaluation, Invensys Operations Management (IOM) also submitted the Nuclear Systems Integration Program Manual (Reference 112). The Nuclear Systems Integration Program Manual 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 the Tricon V10 safety evaluation. It is an application-specific action item for the NRC staff to perform a review of any application-specific development activities governed by the Nuclear Systems Integration Program Manual when requesting NRC approval for the installation of a safety-related system based on the Tricon V10 platform.

   The application development processes used for the DCPP PPS Tricon subsystem are defined and evaluated in Section 3.4, "Software/Core Logic Development Process," of this safety evaluation. These are the development processes governed by the Nuclear Systems Integration Program Manual and the NRC staff determined these processes to be acceptable.

2. Section 3.2, "Development Process," of the Tricon V10 safety evaluation 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 safety-related applications in nuclear power plants. Section 3.4.1, "Software/Core Logic Planning Documentation," of this safety evaluation provides an evaluation of development process planning activities, including those performed by the licensee.

3. Determination of compliance with the applicable regulations remains subject to plant-specific licensing review of a full system design based on the Tricon V10 platform. The licensee has made a determination of compliance with the design criteria and regulations identified in Standard Review Plan (SRP) Chapter 7, Table 7-1, relevant to the Tricon portion of the DCPP process protection system (PPS). This determination was reviewed by the NRC staff and relevant regulatory criteria are identified in Section 2.1, "Regulatory Criteria," of this safety evaluation. The Tricon subsystem was evaluated using these criteria as a basis for acceptability and was determined to be acceptable.

4. Section 3.1.3.2, "TriStation 1131 V4.7.0 Programming Software," of the Tricon V10 safety evaluation 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 personal computer during safety-related operation. The plant-specific procedures which disconnect or control the connection of the TriStation personal computer such that the TriStation tool cannot affect the safety-related functions of the Tricon programmable logic controller (PLC) system during operation will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a safety-related system based on the Tricon V10 platform.

   As described in Section 3.1.6.1.7, "Tricon Communications," of this safety evaluation, Tricon maintenance work stations will be connected to the Tricon safety processors during PPS operation. These maintenance work stations will have TriStation 1131 software installed. Connectivity of these maintenance work stations is, however, restricted by the Tricon application during system operation. Communications between these maintenance work stations and the Tricon safety processors are evaluated in Section 3.7, "Communications," of this safety evaluation. Independence between the Tricon Safety processors and the maintenance work station is also evaluated in Section 3.9.2.6, "IEEE 603-1991, Clause 5.6, Independence," of this safety evaluation. The NRC staff determined that independence between the Tricon safety processors and the maintenance work stations was acceptable and that operation of the non-safety-related maintenance work stations will not adversely affect the safety functions performed by the Tricon portion of the PPS.

   Testing of the operational software produced by the TriStation 1131 including test plans, procedures, and results were reviewed by the NRC staff. The results of these reviews are included in Sections 3.4.1.8, "Software/Core Logic Test Plan," 3.4.2.2, "V&V Analysis and Reports," and 3.4.2.4, "Testing Activities," of this safety evaluation.

5. Section 3.2 of the Tricon V10 safety evaluation discusses verification and validation. Although IOM did not strictly follow guidelines of Institute for Electrical and Electronics Engineers (IEEE) Std. 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74), 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(V&V) for software that is intended for safety-related 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 safety-related use at nuclear power plants.

   The DCPP PPS uses a Tricon PLC system beyond Tricon V10.5.1; however, all Tricon platform changes were reviewed and evaluated by the NRC staff. The NRC staff determined the independent V&V used for these changes to be acceptable. An evaluation of changes made to the Tricon platform is included in Section 3.8, "Tricon V10 Platform Reference Design Changes," of this safety evaluation.

6. Sections 3.3, "Environmental Qualification," and 3.10.2.4, "IEEE Std 603-1991 Clause 5.4, 'Equipment Qualification,'" of the Tricon V10 safety evaluation discuss environmental qualification. The Electric Power Research Institute (EPRI) technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), which was accepted by NRC safety evaluation dated July 30, 1998 (Reference 241), presents a set of requirements to be applied to the generic qualification of PLCs for application to safety-related instrumentation and control (I&C) systems in nuclear power plants. It is intended to provide a qualification envelope for a plant-specific application. Several equipment qualification tests did not fully meet the acceptance criteria of TR-107330 (e.g., electromagnetic capability and seismic withstand).

   The licensee made a determination that the as-tested envelope bounds the requirements of the PPS application within its installed environment. The licensee has verified that the maximum test voltages cited in Section 3.3 of the Tricon V10 safety evaluation envelop the maximum credible voltages applied to non-Class 1E interfaces at the DCPP facility. The licensee provided additional test documentation as well as environmental information for the areas into which the PPS will be installed at the plant to show that all of the PPS equipment meets plant-specific environmental requirements. See Section 3.5.1, "Environmental Qualification of System," of this safety evaluation for details of the environmental qualifications of the DCPP PPS.

7. Section 3.4.1, "Response Time," and 3.10.2.5, "IEEE Std 603-1991 Clause 5.5, System Integrity," of the Tricon V10 safety evaluation 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 safety-related applications in nuclear power plants.

   The licensee has made a determination that the response time performance of the Tricon PPS subsystem satisfies the DCPP PPS requirements for system response time presented in the accident analysis in Chapter 15 of the Final Safety Analysis Report Update (FSARU) for the plant. Response time characteristics of the Tricon subsystem were evaluated by the NRC staff and determined to be acceptable. See Section 3.15, "Response Time Characteristics," of this safety evaluation.

8. Section 3.4.3, "Diagnostics and Self-Test Capabilities," of the Tricon V10 safety evaluation discusses diagnostics and self-test capabilities. The NRC staff reviewed these self-test capabilities, and found them to be suitable for a digital system used in safety-related applications in nuclear power plants. It may also be possible to use some of these diagnostic capabilities to modify or eliminate certain technical specification-required periodic surveillance tests; however, this is a plant-specific, application-dependent issue and, therefore, is not addressed in the Tricon V10 safety evaluation. The licensee is therefore required to provide any such surveillance test modifications or eliminations as part of plant-specific license amendment requests. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a safety-related system based on the Tricon V10 platform.

   Changes being made to the DCPP technical specifications were provided as Attachment 2 to the Enclosure of the licensee's letter dated October 26, 2011 (Reference 1). These changes redefined the term "Channel Operational Test (COT)" to address differences between the Eagle 21 PPS and the replacement PPS. This redefined term does credit diagnostic and self-test capabilities of the Tricon PPS subsystem. No changes to surveillance requirements or surveillance frequency are being requested and no changes to required action completion times are being made as a result of the PPS upgrade. An evaluation of these changes was performed by the NRC staff and is documented in Section 3.11, "Technical Specification Changes," of this safety evaluation.

9. Section 3.7.2.1, "NSR [Non-Safety-Related] Communications via the TCM Modules," of the Tricon V10 safety evaluation discusses communications interconnections. All external communications connections will require justification of the deterministic quality of Tricon Communications Module routed data in the application-specific review. The licensee must provide a justification that should include the minimum guaranteed throughput on the communications

bus based on application-specific scan time and number of input/output and the selected protocol. The justification should also include an assessment of Tricon Communications Module vulnerabilities based on the application-specific design.

External communications interfaces to the PPS Tricon subsystem via the Tricon Communications Module are described in Section 3.1.6.1.7, "Tricon Communications," of this safety evaluation. They include:

- Communications between the Tricon and the TriStation maintenance work station, and
- Communications between the Tricon and the plant process plant computer system through port aggregator devices.

A detailed evaluation of all communications aspects of the PPS Tricon subsystem is provided in Section 3.7, "Communications," of this safety evaluation. The NRC also evaluated deterministic performance of the PPS Tricon subsystem. The results of this evaluation are included in Section 3.17, "Deterministic System Behavior," of this safety evaluation. This evaluation determined that minimum guaranteed throughput on the communications bus based on application-specific scan time and the DCPP PPS-specific input/output is adequate and the DCPP PPS meets the criteria for deterministic and predictable performance. An assessment of Tricon Communications Module vulnerabilities based on the DCPP PPS application is included in the Tricon Failure Modes and Effects Analysis which was evaluated by the NRC as documented in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation.

10. Section 3.7.2.2, "NSR [Non-Safety-Related] Communications via the Remote RXMs [Remote Extender Modules]," of the Tricon V10 safety evaluation discusses non-safety input/output connected to a remote RXM chassis. The NRC staff concluded that adequate protection is provided to the safety side input/output 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 input/output 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 safety-related system based on the Tricon V10 platform.

    Remote RXM chassis are being used in the DCPP PPS to process non-safety-related signals. This communications interface between the safety-related primary RXM chassis and the non-safety-related secondary RXM chassis is described in Section 3.1.6.1.7, "Tricon Communications," of this safety evaluation. The NRC staff evaluated the replacement PPS against each of the criteria for communications provided in DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance," Revision 1, dated March 6, 2009 (Reference 34). The results of this evaluation are provided in Section 3.7, "Communications," of this safety evaluation.

11. Section 3.7.3.1, "DI&C-ISG-04, Staff Position 1 - Interdivisional Communications," of the Tricon V10 safety evaluation discusses the 20 individual points of DI&C-ISG-04, Section 1, Interdivisional Communications. The Tricon V10 licensing topical report 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 the Tricon V10 safety evaluation. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a safety-related system based on the Tricon V10 platform.

    The licensee provided an assessment of the PPS conformance with DI&C-ISG-04 Section 1 in Section 4.8 of the Enclosure to its letter dated April 30, 2013 (Reference 12). This assessment included justifications for each of the compliance positions stated. The NRC staff evaluated the replacement PPS against each of the criteria provided in DI&C-ISG-04. The results of this evaluation are provided in Section 3.7, "Communications," of this safety evaluation.

12. Section 3.7.3.2, "DI&C-ISG-04, Staff Position 2 - Command Prioritization," of the Tricon V10 safety evaluation 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 Tricon V10 topical report 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 safety-related system based on the Tricon V10 platform.

    The DCPP PPS application does not use the Tricon subsystem for field device interface functions. Instead, the solid state protection system (SSPS), which is described in Section 3.1.1.2, "Solid State Protection System Description (Not Within PPS Replacement Scope)," of this safety evaluation, provides field device interface functions for all reactor protection system (RPS) and engineered safety features actuation system (ESFAS) functions. The SSPS is not being modified by this license amendment request.

13. Section 3.7.3.3, "DI&C-ISG-04, Section 3 - Multidivisional Control and Display Stations," of the Tricon V10 safety evaluation discusses DI&C-ISG-04, Section 3,

Multidivisional Control and Display Stations. The design of information displays and operator work stations and the determination of information sources and interconnections are application-specific activities. Since the topical report 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 work stations 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 safety-related system based on the Tricon V10 platform.

The DCPP PPS application does not include any use of multidivisional control or display stations. Instead, all PPS control and display functions are to be provided on existing control panel meters indications and discrete alarm displays. The maintenance work station computers, which are described in Section 3.1.7.1, "Maintenance Work Station," of this safety evaluation, can be used to obtain system information; however, the PPS includes separate maintenance work station displays for each protection set. Therefore, these displays are not considered to be multidivisional control or display stations. Therefore, no evaluation of the PPS against ISG-04 Section 3 criteria was required for the DCPP PPS Tricon subsystem.

14. Section 3.8.1, "Lifecycle Phases," of the Tricon V10 safety evaluation discusses the secure development environment. The NRC staff observed elements of the secure development environment during the December 15-17, 2010, audit at IOM's facility in Irvine, California (see Reference 6 of the safety evaluation for the Tricon V10 platform topical report). The NRC staff also reviewed Sections 4.2, "Plant-Specific Action Items," and 5.1, "Regulatory Compliance," of the Tricon V9 safety evaluation (Reference 219), and find that the previous conclusions still apply. Based on a review of "Tricon V10 Conformance to RG 1.152," IOM document NTX-SER-10-14, regarding secure development environment and a comparison to the previously reviewed development environment from the Tricon V9 safety evaluation 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. 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. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a safety-related system based on the Tricon V10 platform.

An evaluation of the DCPP replacement PPS Tricon subsystem secure development and operational environment (SDOE) characteristics was performed by the NRC staff and the results of this evaluation are included in

Section 3.12, "Secure Development and Operational Environment," of this safety evaluation.

15. Section 3.8.1, "Lifecycle Phases," of the Tricon V10 safety evaluation 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 safety-related system based on the Tricon V10 platform.

    An evaluation of the DCPP replacement PPS Tricon subsystem secure development and operational environment (SDOE) characteristics was performed by the NRC staff and the results of this evaluation are included in Section 3.12, "Secure Development and Operational Environment," of this safety evaluation.

16. Section 3.9, "Conformance with IEEE Std. 603-1991, 'IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,'" of this safety evaluation discusses diversity and defense-in-depth (D3). Since both diversity and defense-in-depth are plant-specific topics, the topical report did not address these topics and, therefore, are not within the scope of this safety evaluation. Section 3.6.2, "Defense-In-Depth and Diversity Requirements," and 3.6.3, "Diversity Implementation," of Appendix B, "Application Guide," to the Triconex Approved Topical Report (Reference 29), 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 D3 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 safety-related system based on the Tricon V10 platform.

    An evaluation of the DCPP replacement PPS Tricon subsystem D3 analysis was performed by the NRC staff and the results of this evaluation are documented in the NRC's safety evaluation for topical report "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," dated April 19, 2011 (Reference 196). Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation provides additional application-specific evaluation results regarding PPS D3.

17. Section 3.10.3, "IEEE Std 603-1991 Clause 6, 'Sense and Command Features - Functional and Design Requirements," of the Tricon V10 safety evaluation discusses conformance with IEEE Std. 603-1991, including setpoint determination. Invensys Operations Management 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 safety-related system based on the Tricon V10 platform.

18. Section 3.7.1, "Tricon-Based PPS Equipment Communications," of this safety evaluation discusses communications with safety-related equipment. The documentation confirms testing of the TriStation 1131 library with the session announcement protocol. However, the protocol will also be implemented at the application layer of the connected safety-related equipment, presumably a safety-related video display unit. The documentation does not confirm that the protocol has been tested with any specific external safety-related devices. Therefore, it is an application-specific action item for the applicant to verify that the session announcement protocol library is tested in any proposed application-specific safety-related devices. This determination will be reviewed by the NRC staff when an applicant requests NRC approval for the installation of a safety-related system based on the Tricon V10 platform.

    The DCPP PPS does not use safety-related video display units. The Tricon subsystem of the PPS does not contain any communications interfaces with other safety-related equipment (either within the same protection set or between protection sets). Therefore there is no relevant session announcement protocol for connected safety-related devices and there is no need to test or verify such a session announcement protocol library. No evaluation was required for this application-specific action item.

19. Section 3.7.3.1.10, "Staff Position 1, Point 10," of this safety evaluation 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 safety-related system based on the Tricon V10 platform.

    An evaluation of the Tricon PPS subsystem against the criteria for Point 10 of ISG-04 was performed by the NRC staff. This evaluation includes consideration of the Tricon keyswitch function and associated logic. System failures affecting the key switch functions are also considered in the Tricon Failure Modes and Effects Analysis which was evaluated by the NRC as documented in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation. Testing of keyswitch functions was included in system validation and factory acceptance tests. An evaluation of the test documentation and test results was performed by the NRC staff and the results are included in Sections 3.4.1.8, "Software/Core Logic Test Plan," 3.4.2.2, "V&V Analysis and Reports," and 3.4.2.4, "Testing Activities," of this safety evaluation. The results of the DI&C-ISG-04 Point 10 evaluation are documented in Section 3.7.3.1 of this safety evaluation.

3.13.2 ALS PSAIs

Section 4.2, "Plant-Specific Action Items," of the safety evaluation for the Advanced Logic System Topical Report (Reference 30) identified 23 plant-specific action items (PSAIs) to be addressed by the licensee during the development of a safety-related system using this platform. The following is the NRC's assessment of the licensee's compliance with each of these items:

1. Application-specific ALS-102 Requirements Specification(s) - An applicant or licensee referencing the ALS topical report safety evaluation should demonstrate it has provided application specification(s) to govern each unique ALS-102 FPGA logic program's development.

   The NRC staff reviewed the DCPP PPS project Functional Requirements Specification (Reference 126) and Interface Requirements Specification (References 98). These documents contain specifications used to govern the ALS-102 logic development. Through performance of reviews and thread audits, the NRC staff confirmed proper implementation of identified specifications applicable to the ALS subsystem functions. The NRC staff verified these functions were properly translated into the "ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, dated May 2013 (Reference 163), as well as detailed core logic board design specifications, "ALS-102 Core A FPGA Design Specification," Revision 0, 6116-10203, May 2013 (Reference 164), and "ALS-102 Core B FPGA Design Specification," Revision 0, 6116-10204, dated April 18, 2013 (Reference 165). The NRC staff concludes that these specifications are an adequate means of controlling logic development activities.

2. Application Conformance to ALS Platform Development Process - An applicant or licensee referencing the ALS topical report safety evaluation should demonstrate the development of its application-specific ALS-102 FPGA logic programs followed a development process equivalent to the one described and evaluated in Section 3.2.3, "Standardized FPGAs," of the ALS platform safety evaluation.

Because of the diversity requirements associated with the functions performed by the ALS subsystem, the ALS application development process for the DCPP PPS includes both "Core A" and "Core B" design variants, rather than a single core design. The NRC staff evaluated the core logic development processes and confirmed the processes to be compliant with those processes evaluated during the platform safety evaluation. The results of this PPS core logic application development evaluation are included in Section 3.4, "Software/Core Logic Development Process," of this safety evaluation.

3. Application Conformance to "Embedded Design Diversity" Development Process - When an applicant or licensee referencing the ALS topical report safety evaluation specifies "embedded design diversity," the applicant or licensee should demonstrate the development of its application-specific ALS-102 FPGA logic programs followed equivalent development processes to those described and evaluated in Section 3.2.4, "FPGA Design Variants," of the ALS topical report safety evaluation. This demonstration should include the production and configuration control of the related lifecycle development products, including those identified in Table 3.2.5-1 for both "Core A" and "Core B."

The DCPP PPS design specifies embedded design diversity for the ALS portion of the system. The NRC staff reviewed the DCPP PPS "Management Plan," Revision 8, 6116-00000, September 2015 (Reference 105), to determine compliance with this PSAI. See Section 3.4.1.1, "Software/Core Logic Management Plan," of this safety evaluation. The process used for development of both A and B core logic boards included production and configuration control of all lifecycle development products. The NRC staff compared the lifecycle products of the PPS design to the products identified in Table 3.2.5-1 of the platform topical report for both "Core A" and "Core B." The results of this comparison identified several documents from Table 3.2.5-1 which were not created for the PPS project. In request for additional information (RAI) 55 dated March 31, 2014 (Reference 190), the NRC requested that the licensee provide an explanation for this inconsistency. In its RAI response dated April 30, 2014 (Reference 17), the licensee explained that the document numbering scheme is project-specific. Though the ALS topical report identifies a list of potential design products, not all of the documents listed in Table 3.2.5-1 are necessarily developed or required for every project. For example, it is not necessary to replicate an ALS board requirements document at the DCPP document level if its generic design is not altered for the application. The licensee also provided a summary list of documents developed for the DCPP PPS application as well as an explanation of why certain platform documents could be applied directly to the DCPP project without alteration.

The NRC staff determined that the licensee has adequately demonstrated the development of the application-specific ALS-102 FPGA logic programs followed equivalent development processes to those described and evaluated in

Section 3.2.4 of the ALS topical report safety evaluation. This demonstration included the production and configuration control of the applicable life-cycle development products as identified in Table 3.2.5-1 for both "Core A" and "Core B" of the DCPP ALS subsystem.

4. ALS Platform Boundary/Interface Conditions and Installation Limitations - An applicant or licensee referencing the ALS topical report safety evaluation should address its conformance to or deviations from the manufacturer-identified boundary/interface conditions and installation limitations within the "ALS Platform EQ Summary Report," Revision 2, 6002-00200, January 2013 (Reference 183). An applicant or licensee referencing this safety evaluation should identify the applicability of each condition and limitation. For each applicable condition or limitation, the applicant or licensee should either demonstrate its conformance or provide justification for any deviation. For any deviation, an applicant or licensee should demonstrate the deviation does not invalidate the ALS platform qualification in a manner adverse to the reliable performance of a safety function. Such demonstrations that deviations are justified should consider performance of supplemental testing, supplemental analysis, or both.

   The interface/boundary conditions specified in Section 7.1, "Equipment Interface/Boundary Conditions," as well as the installation limitations specified in Section 7.2, "Installation Limitations," of the ALS Platform EQ Summary Report apply to the PPS ALS subsystem. Conformance to the interface/boundary conditions and installation limitations of the DCPP PPS ALS subsystem are documented in Sections 6.2, "Equipment Interface/Boundary Conditions Compliance Information," and 6.3, "Installation Limitations Compliance Information," of the "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235).

   The NRC staff reviewed the ALS Platform EQ Summary Report and determined that conformance with boundary conditions was generally achieved; however, there were exceptions. One deviation identified minor differences in mounting hardware. For this exception, a justification was provided which determined the deviation did not invalidate the ALS platform qualification in a manner adverse to the reliable performance of a safety function.

   Several installation limitations will need to be performed by the licensee upon plant installation. Because the NRC staff is unable to confirm completion of these requirements, the following recommended inspection items are included in Section 3.14.2, "ALS Site Inspection Follow-up Items," of this safety evaluation.

   - Inspect cables interfacing to the rear of the ALS chassis.
   - Inspect field cable installation.

- Determine if electrostatic discharge precautions are being used during installation of PPS ALS equipment.

- Ensure maximum temperature, including temperature rise, within each cabinet containing ALS components does not exceed the platform specification.

- Inspect chassis ground-braid installations.

See Section 3.5, "Equipment Environmental Qualification," of this safety evaluation for additional information regarding the NRC evaluation of DCPP PPS ALS subsystem equipment qualification.

5. ALS Platform Application Restrictions - An applicant or licensee referencing the ALS topical report safety evaluation should address its adherence to the manufacturer identified application restrictions within the "ALS Application Guidance." An applicant or licensee referencing the ALS platform topical report safety evaluation should identify the applicability of each restriction. For each applicable restriction, the applicant or licensee should either demonstrate its adherence or provide justification for excluding the restriction. For any exclusion, an applicant or licensee should also demonstrate the exclusion does not invalidate the ALS platform qualification in a manner adverse to the reliable performance of a safety function. Such demonstrations should consider performance of supplemental testing, supplemental analysis, or both.

The DCPP PPS ALS subsystem adherence to the ALS platform application restrictions specified in the ALS Application Guidance document is described in Appendix D of the ALS Subsystem "System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127).

The NRC staff reviewed the application restriction tables in Appendix D to assess compliance of the DCPP application design with applicable restrictions. Forty-nine application restrictions were identified in Appendix D of which 31 were determined to be applicable to the DCPP PPS subsystem.

The NRC staff confirmed that each of the application restrictions was evaluated for applicability to the DCPP PPS subsystem. In cases where the restriction was not applicable to the DCPP project, an explanation and justification was provided. For cases where the application restriction was determined to be applicable to the DCPP PPS project, an explanation of how the restriction was implemented into the design was provided and applicable requirements were identified. As a result, the NRC staff was able to review traceability of implementation via the "ALS Subsystem Requirements Traceability Matrix," Revision 3, 6116-00059, November 2014 (Reference 161). During the June 22-26, 2015, regulatory audit of the Westinghouse facilities (Reference 39), the NRC staff used application restriction tables as a basis for a requirements thread tracing activity and confirmed that the restriction criterion for two selected items: 1) System Coverage of Serial Link Faults, Item A1 and 2) RTD [Resistance Temperature Detectors] Open Circuit Detection, Item H1, were satisfied in the PPS design.

6. Demonstration of Equipment Qualification - An applicant or licensee referencing the ALS topical report safety evaluation should demonstrate the equipment qualification testing documented and evaluated within this safety evaluation remains valid and bounding. Otherwise, additional plant-specific equipment qualification efforts should be performed, which may include analyses and/or tests. If an applicant or licensee cannot demonstrate the ALS topical report equipment qualification remains valid and bounding, then the applicant or licensee should demonstrate plant-specific qualification efforts are bounding. The demonstration should identify the non-volatile memory configuration for each ALS standardized circuit board it uses and the equipment qualification that shows the circuit board's performance has been bounded for each application-specific configuration.

   The "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235), documents an evaluation of the PPS ALS subsystem with respect to the equipment qualification testing evaluated during the ALS platform safety evaluation.

   Section 3, "Non-Volatile Memory (NVM) Comparison," of the equipment qualification evaluation documents the application-specific non-volatile memory configurations for the ALS circuit boards and includes DCPP specific configuration evaluations. Section 8, "Summary and Conclusions," of the equipment qualification evaluation states that "the ALS platform qualification may be extended to all aspects of the DCPP PPS ALS subsystem without additional testing (i.e., the ALS platform qualification remains valid and bounding)."

   The PPS ALS subsystem includes a line sense module which was not tested during platform equipment qualification testing. This line sense module was subsequently qualified by testing to the requirements specified in Section 12, "Equipment Qualifications," of the PPS "System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127). This line sense module component qualification is documented in "Advanced Logic System and Line Sense Module Equipment Qualification Summary Report," Revision 0, EQ-QR-120-PGE, dated September 2014 (Reference 184).

   The licensee determined that the as-tested envelope bounds the requirements of the PPS application within its installed environment. The licensee has verified that the maximum test voltages cited in Section 3.3, "Equipment Qualification," of the ALS platform safety evaluation envelop the maximum credible voltages applied to non-Class 1E interfaces at the DCPP facility. The licensee provided additional test documentation as well as environmental information for the areas into which the PPS will be installed at the plant to show that all of the PPS equipment meets plant-specific environmental requirements. See Section 3.5.1, "Environmental Qualification of System," of this safety evaluation for details of the environmental qualifications of the DCPP PPS.

7. Response Time Performance - An applicant or licensee referencing the ALS topical report safety evaluation should: (1) establish application-specific design timing requirement(s) for the system; (2) perform application-specific analysis to budget the timing requirement(s) to associated components of the system architecture; (3) validate the most restrictive timing requirement for each ALS platform component used within the system architecture has been bounded by the qualified performance envelope for that ALS platform component; (4) perform verification testing that demonstrates the integrated ALS platform-based system meets each design timing requirement and performs as expected; and (5) include appropriate technical specification surveillance requirements to confirm the equipment's digital response time characteristics, as applicable.

   The licensee has made a determination that the response time performance of the ALS PPS subsystem satisfies the DCPP PPS requirements for system response time presented in the accident analysis in Chapter 15 of the Final Safety Analysis Report Update for the plant (Reference 52). Response time requirements and budgeting of response time between PPS subsystems are established in the PPS functional requirements specification. Response time performance was validated during verification and validation (V&V) testing activities including the factory acceptance test. Response time monitoring will be performed during system operation in the plant as a part of the surveillance testing program. Response time characteristics of the ALS subsystem were evaluated by the NRC staff and determined to be acceptable. See Section 3.15, "Response Time Characteristics," of this safety evaluation.

8. Deterministic Performance - An applicant or licensee referencing the ALS topical report safety evaluation should confirm the application specifications identify the board access sequence, frame time, and implementation of the design features to activate system alarms upon detection of a failure to meet timing requirements, so an operator can take corrective action. An applicant or licensee referencing this safety evaluation should also verify the application-specific logic does not introduce non-deterministic computation or non-deterministic digital data communications.

   The "ALS-102 Core A FPGA Design Specification," Revision 0, 6116-10203, May 2013 (Reference 164), identifies the sequence and timing of the Reliable ALS Bus (RAB) transaction (board access) assignments during each frame. Table 5.5-1 of that document specifies each sequencer step. Subsection 4.4.3, "Slot Table," of the "ALS-102 Core B FPGA Design Specification," Revision 0, 6116-10204, dated April 18, 2013 (Reference 165), identifies the sequence and timing of RAB transaction (board access) assignments during each frame.

The ALS platform-specific self-diagnostic fault conditions are supplemented by an application-specific ALS-102 board timeout fault condition. Subsection 7.2.2, "Self-Diagnostics," of the" ALS Subsystem, System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127), describes these fault conditions and specifies their assignment to the system failure alarm.

The ALS-102 board FPGA application-specific logic is designed to operate in a deterministic manner. It does not introduce conditions that require the associated finite state machines to wait for responses from unreliable sources. Furthermore, the ALS FPGA build procedures require use of encoding methods to ensure that undefined finite state machine transitions result in reset to a valid (defined) state, thereby preventing non-deterministic behavior.

A more detailed evaluation of ALS system deterministic performance is provided in Section 3.17, "Deterministic System Behavior," of this safety evaluation.

9. Self-Diagnostics, Test, and Calibration Capabilities - An applicant or licensee referencing the ALS topical report safety evaluation should demonstrate the adequacy of the application-specific use of ALS platform diagnostic, self-test, and manually initiated test and calibration features. The following should be considered:

    a. Test Coverage - The applicant or licensee should demonstrate ALS platform diagnostic, self-test, and manually initiated test and calibration features are sufficient to verify the operational integrity of all logic components (i.e., all relays and contacts, trip units, solid state logic elements, etc.) of a logic circuit, from as close to the sensor as practicable up to but not including the actuated device for each safety function and with sufficient overlap.

       The licensee will continue to perform periodic surveillance tests on the ALS portion of the PPS during system operation. The channel functional tests will, however, be revised and will no longer include injection of process data signals at system input terminals. Continuous self-test features of the ALS platform will be credited for ensuring functional correctness of the ALS logic portion of the PPS during operation. Surveillance tests will include verification of ALS setpoints and tunable parameter values. Channel calibration surveillances to be performed at refueling intervals will include injection of process data signals at system input terminals to verify ALS logic functionality.

In DCPP Technical Specification Section 1.1, "Definitions," the "Channel Operability Test (COT)" definition is being revised to address this new method of ensuring channel operability. The NRC staff performed an evaluation of this revised test methodology and determined that the DCPP PPS is designed for in-service testability commensurate with the safety functions to be performed through all modes of plant operation. Details of this evaluation are included in Section 3.11, "Technical Specification Changes," of this safety evaluation. Based on the above, the NRC staff concludes that the surveillance test program established for the ALS portion of the PPS in conjunction with self-test features of the ALS subsystem are sufficient to verify the operational integrity of all logic components during plant operation.

b. Relationship to Existing Surveillances - If a licensee proposes to use ALS platform built-in self-test features to justify the elimination of existing surveillances or less frequent performance of existing surveillances, then the licensee should also demonstrate the built-in self-testing provides equivalent assurance to the surveillances performed on the equipment being replaced.

The licensee is not requesting to eliminate current technical specification-required periodic surveillance tests or to revise current technical specification surveillance frequencies for the replacement PPS; however, changes to the channel operability test (COT) surveillance tests will be made to eliminate injection of process data signals during tests; therefore, the criteria of this application-specific action item are applicable for the replacement PPS. ALS self-test features are being used to justify elimination of signal injection tests from the COT surveillance test.

The licensee stated that on-line self-testing and diagnostic functions are being implemented to improve the availability of the system and improve system maintainability. ALS input boards are designed to provide self-test capability to continuously verify vital components within the channel to be operational. ALS output boards are also designed with similar self-test capabilities. More detailed discussion of the ALS self-test features is provided in Section 3.4.3, "Self-Diagnostics, Test and Calibration Capabilities," of the ALS platform safety evaluation for the Advanced Logic System Topical Report (Reference 30), and in Section 3.10.1.3.3, "IEEE 7-4.3.2-2003 Clause 5.5.3, Fault Detection and Self Diagnostics," 3.10.1.5, "IEEE 7-4.3.2-2003 Clause 5.7, Capability for Test and Calibration," and 3.11, "Technical Specification Changes," of this safety evaluation. Also, see PG&E's April 30, 2014 (Reference 17) to the NRC staff's request for additional information (RAI) 59 dated March 31, 2014 (Reference 190).

The NRC staff's review confirmed self-diagnostic features and tests performed by the ALS platform will place the PPS into a safe state and will annunciate failure status to the operators. The NRC staff also determined the built-in self-testing of the ALS in conjunction with revised COT surveillance tests provide an equivalent level of system operability assurance to the surveillance tests performed on the Eagle 21 PPS equipment being replaced.

c. Reliance upon Automatic Testing - If an applicant or licensee relies upon the continued performance of diagnostic or self-test features that an ALS platform-based system has been designed to automatically perform, then the surveillance procedures that the plant's technical specification references through surveillance requirements should verify the built-in self-tests results and ensure these tests continue to acceptably operate. This activity should confirm the plant's installation does not exhibit unjustified intermediate errors without reported failures that could adversely affect a safety function.

The revised surveillance test methodology does rely upon continued performance of self-test features of the ALS system. The DCPP surveillance procedures will verify the results of the ALS self-tests by testing the alarm annunciation functions of the ALS subsystem and ensuring that no self-test initiated alarm is present upon completion of the COT. A channel functional test will also be performed on a refueling interval to verify channel functionality independently from the ALS self-test functions.

The NRC staff determined that functionality of ALS self-test features can be adequately confirmed by ensuring system setpoints and configurable parameters are correct and by observing that no self-test initiated alarms or messages are present in the system. The NRC staff also confirmed that self-test status and diagnostic information can be obtained via the associated ALS maintenance work station. The DCPP surveillance test methods are adequate to ensure the ALS PPS subsystem will not exhibit unjustified intermediate errors that could adversely affect a safety function without providing an alarm indication to the operators.

d. No Adverse Impact on the Reliability of Safety Functions - The applicant or licensee should demonstrate the application-specific diagnostic, self-test, and manually initiated test and calibration features will not adversely affect channel independence, system integrity, or the system's ability to meet the single-failure criterion.

Built-in self-test functions are an integral part of each of the ALS board designs. As such, built-in self-test functions are operational during all test activities including qualification tests performed on the ALS components as well as DCPP plant application testing performed during factory acceptance resting and site acceptance testing. The results of these test activities did not indicate any adverse impact on the reliability of the DCPP ALS safety functions.

None of the failure modes identified and analyzed in the ALS Failure Modes and Effects Analysis (FMEA) affect the ability of self-test functions to identify application or ALS board errors as designed. Because of this, the FMEA did not postulate the effects of a self-test error on the safety functions of the system. Failures in the application-specific diagnostic self-test features are bounded by the failures considered in Table 4-4 of the FMEA. All ALS failures considered in this analysis had no impact on the safety function performed by the ALS because of the built-in diversity and protection set redundancy included in the ALS design.

The NRC staff determined the ALS self-test and diagnostic features do not adversely affect the PPS's ability to meet the single-failure criterion. See the single-failure criteria evaluation in Section 3.9.2.1, "IEEE 603-1991, Clause 5.1, Single-Failure Criterion," of this safety evaluation. A review of the "ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Reference 153), was also performed and the results are documented in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation.

e. Administrative Controls to Prevent Limiting Conditions for Operation - For manual calibration or surveillance activities, the applicant or licensee should demonstrate adequate administrative controls to ensure a limiting condition for operation is not routinely entered. This demonstration should consider the functionality per channel and the overall channel, division, and voting logic arrangement of the system.

Activation of the Test ALS Bus communication link is monitored by the ALS subsystem and administratively controlled through physically disconnecting the communication link when the Test ALS Bus is not in use. Only the core logic components being tested will be rendered inoperable during COT surveillance test activities. Thus, ALS channel safety functions are not impacted during these tests. This design is expected to significantly reduce the number of entries into technical specification limiting conditions for operation required actions compared to the current Eagle 21 PPS.

The maintenance work station functions that use interactive Test ALS Bus communications are only available when the Test ALS Bus is physically connected to the ALS maintenance work station by qualified personnel under administrative controls and then only on one of the ALS "A" or "B" subsystems (chassis) at a time. Recommended ALS site inspection follow-up items 1 and 2 have been included in Section 3.14.2, "ALS Site Inspection Follow-up Items," of this safety evaluation as means of confirming administrative controls over the use of the Test ALS Bus connector during system operation and testing activities.

The NRC staff determined the administrative controls implemented for the DCPP PPS for ensuring correct limiting conditions for operation to be acceptable for normal plant operations and for support of system testing and maintenance activities.

f. Conformance to Regulatory Guides (RGs) - The applicant or licensee should demonstrate the relationship between (a) the application-specific diagnostic, self-test, and manually initiated test and calibration features provided by the ALS platform and (b) the conformance to the NRC staff positions in RG 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0, February 1972 (Reference 58), and RG 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995 (Reference 69).

RG 1.22 provides guidance criteria for ensuring protection system designs permit periodic testing of initiation functions during reactor operations.

RG 1.118 describes a method acceptable to the NRC staff for complying with the Commission's regulations with respect to the periodic testing of the electric power and protection systems.

The solid state protection system logic and relay portion of the protection system are not being changed as part of the PPS replacement project, and are tested separately on-line using COTs and during refueling outages using channel calibrations and trip actuation device tests.

The PPS ALS subsystem design provides the capabilities for test and calibration while retaining the equipment's ability to accomplish its safety function during plant operation. The ALS supports tripping or bypassing individual safety channels when technical specification limiting conditions for operation require such actions. The ALS also provides continuous indication of the system status including safety channel trip or bypass status in the control room.

An evaluation of the revised COT methods including the use of ALS self-test features was performed by the NRC staff. The details of this evaluation are included in Section 3.11, "Technical Specification

Changes," of this safety evaluation. That evaluation concludes that the DCPP PPS is designed for in-service testability commensurate with the safety functions to be performed through all modes of plant operation and that the revised PPS hardware and software design will continue to support required periodic testing of the system.

The DCPP protection system design allows individual testing of the reactor trip system, engineered safety features actuation system, and solid state protection system portions of the protection system. External hard-wired switches are provided on all PPS replacement trip and actuation outputs to support testing of each redundant PPS channel within each protection set. The switches may be used for solid state protection system 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 solid state protection system partial trip indicators. Operation of bypass switches for ALS subsystem is indicated in the control room through the main alarm system and is administratively controlled.

Manual bypass switches are provided for each comparator output in the ALS, to prevent expansion of the bypass condition to redundant channels and protection sets.

The NRC staff determined the DCPP application diagnostic, self-test, and manually initiated test features to be compliant with the criterion provided in RGs 1.22 and 1.118 and are, therefore, acceptable.

10. Failure Mode and Effects Analysis – An applicant or licensee referencing the ALS topical report safety evaluation should perform a system-level FMEA to demonstrate the application-specific use of the ALS platform identifies each potential failure mode and determines the effects of each. The FMEA should demonstrate single failures, including those with the potential to cause a non-safety system action (i.e., a control function) resulting in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable.

    The licensee performed a DCPP ALS system level FMEA. This FMEA identifies each potential failure mode of the DCPP ALS PPS application and determines the effects of each. It also demonstrates that single failures resulting in a condition requiring an ALS subsystem protective action do not adversely affect the ALS protection functions needed for each analyzed condition. An evaluation of the ALS subsystem FMEA is provided in Section 3.4.3.5, "System Failure Modes and Effects Analysis," of this safety evaluation.

11. Reliability and Availability Analysis – An applicant or licensee referencing the ALS topical report safety evaluation should perform a deterministic system-level evaluation to determine the degree of redundancy, diversity, testability, and quality provided in an ALS platform-based safety system is commensurate with the safety functions that must be performed. An applicant or licensee should confirm a resultant ALS platform-based system meets any applicable reliability goals that the plant has established for the system. This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass to support plant operations. An applicant or licensee should demonstrate the ALS platform reliability analysis method provides an equivalent level of assurance to the applicant's or licensee's reliability analysis method.

    Section 3.9.1.9, "IEEE 603-1991 Clause 4.9, Methods Used to Determine Adequate Reliability of the Safety System," 3.9.2.15, "IEEE 603-1991, Clause 5.15, Reliability," and 3.10.1.8, "IEEE 7-4.3.2-2003, Clause 5.15, Reliability," of this safety evaluation provide evaluations of the ALS subsystem reliability. A plant application-specific ALS PPS "ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Reference 153), was performed and provided to the NRC for evaluation. The NRC staff concludes that the reliability goals and the methods employed by the ALS platform vendor to meet these goals are appropriate and determined to provide an adequate means of meeting the performance requirements of the PPS.

12. Application-specific ALS-102 Digital Communications – An applicant or licensee referencing the ALS topical report safety evaluation and using either TxB1 or TxB2 digital data communication interface of the ALS-102 core logic board should produce the application specification(s) that govern the interface and demonstrate conformance of its application to DI&C-ISG-04 (Reference 34) staff Points 2, 3, 4, 5, 7, 18, 19, and 20 under the NRC staff position for interdivisional communications, which includes data communications between different safety divisions and data communications between a safety division and equipment that is not safety-related.

    The ALS PPS subsystem uses both the TxB1 and TxB2 digital communication interfaces of the ALS-102 core logic boards to facilitate communication with the DCPP process plant computer and with the PPS ALS maintenance work station. Section 3.1.6.2.4, "ALS Communications," of this safety evaluation provides a description of how these interfaces are used. Application specifications for these two communications interfaces are included in the PPS Functional Requirements Specification (Reference 126) and in the PPS Interface Requirements Specification (Reference 98).

The NRC staff performed a DI&C-ISG-04 conformance evaluation of the PPS including the TxB communications interfaces and the results of this evaluation are provided in Section 3.7, "Communications," of this safety evaluation. This evaluation includes assessments of conformance of the ALS subsystem to all staff points of DI&C-ISG-04 including those cited in this PSAI.

13. Application-specific Test ALS Bus Communications – An applicant or licensee referencing the ALS topical report safety evaluation and using the TAB digital data communication interface, which is provided by each ALS platform standardized circuit board, should produce the application specification(s) that govern the interface and demonstrate conformance of its application to DI&C-ISG-04 (Reference 34) staff Points 1, 2, 3, 4, 5, 7, 8, 10, 11, 12, and 18 under the NRC staff position for interdivisional communications, which includes data communications between different safety divisions and data communications between a safety division and equipment that is not safety-related.

    The ALS PPS subsystem uses the Test ALS Bus digital data communication interface to facilitate communication with the PPS ALS maintenance work station which is also referred to as the ALS Service Unit during maintenance and testing activities. Section 3.1.6.2.4, "ALS Communications," of this safety evaluation provides a description of how the Test ALS Bus communication interface is used. Operation of the Test ALS Bus connector to the ALS maintenance work station is also discussed in Section 3.1.7.1, "Maintenance Work Station," of this safety evaluation. Application specifications for the Test ALS Bus communications interface are included in the PPS Functional Requirements Specification (Reference 126) and in the PPS Interface Requirements Specification (Reference 98).

    The NRC staff performed a DI&C-ISG-04 conformance evaluation of the PPS including the Test ALS Bus communication interface and the results of this evaluation are provided in Section 3.7, "Communications," of this safety evaluation. This evaluation includes assessments of conformance of the ALS subsystem to all staff points of DI&C-ISG-04 including those cited in this PSAI.

14. Application-specific ALS-601 Digital Communications – An applicant or licensee referencing the ALS topical report safety evaluation and using the ALS-601 communication board should produce the application specification(s) that govern each communication channel and demonstrate conformance of its application to DI&C-ISG-04 (Reference 34) staff Points 1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 15, 16, 17, 18, 19, and 20 under the NRC staff position for interdivisional communications.

    The DCPP ALS subsystem design does not include the ALS-601 Digital communications board; therefore, the criteria of this PSAI are not applicable to the DCPP PPS.

15. Application-specific Command Prioritization – An applicant or licensee referencing the ALS topical report safety evaluation and implementing command prioritization with ALS platform components should produce the application specification(s) that govern each priority module application and demonstrate conformance of each application to DI&C-ISG-04 (Reference 34) staff Points 1 through 10 under the NRC staff position for command prioritization.

    The DCPP PPS does not perform command prioritization functions and the DCPP ALS subsystem design does not include command prioritization functions; therefore, this PSAI is not applicable to the DCPP PPS replacement project.

16. Application-specific Multidivisional Control and Display Stations – An applicant or licensee referencing the ALS topical report safety evaluation and implementing multidivisional control or a multidivisional display station should produce the application specification(s) that govern each multidivisional control or multidivisional display station application and demonstrate conformance of each application to DI&C-ISG-04 (Reference 34) Staff Position 3 for multidivisional control and display stations.

    The DCPP ALS subsystem design does not include multidivisional controls or multidivisional display stations. Each of the ALS maintenance work stations is assigned and dedicated to a single division or protection set so they are not considered to be multidivisional. The criteria of this PSAI is not applicable to the DCPP PPS.

17. Secure Development Environment for Applications – An applicant or licensee referencing the ALS topical report safety evaluation for a safety-related plant-specific application should ensure the development environment for its plant-specific application continues to meet the applicable regulatory evaluation criteria of RG 1.152.

    The NRC performed an evaluation of the secure development environment aspects of the DCPP PPS. That evaluation included an assessment of conformance to the criteria of RG 1.152 and the results of that evaluation are included in Section 3.12, "Secure Development and Operational Environment," of this safety evaluation.

18. Secure Operational Environment – An applicant or licensee referencing the ALS topical report safety evaluation for a plant-specific application should ensure the operational environment for its safety-related plant-specific applications meets the applicable regulatory evaluation criteria of RG 1.152.

    The NRC performed an evaluation of the secure operational environment aspects of the DCPP PPS. That evaluation included an assessment of conformance to the criteria of RG 1.152 and the results of that evaluation are included in Section 3.12, "Secure Development and Operational Environment," of this safety evaluation.

19. Demonstration of Adequate Diversity – An applicant or licensee referencing the ALS topical report safety evaluation should identify the approaches specified to provide built-in diversity and mitigations against common-cause failures within its application of the ALS platform. The following should be considered:

   a. Embedded Design Diversity – ALS application specifications should designate whether embedded design diversity is required in addition to core diversity for each safety function performed by that application. When embedded design diversity is required, the specifications should also identify the required arrangement of the independent designs among channels, trains and electrical separation groups.

      The DCPP ALS subsystem requires embedded design diversity in addition to the core diversity of the ALS platform for all of the PPS safety functions assigned to the ALS. The DCPP PPS Interface Requirements Specification (Reference 98) contains specific design details of the arrangement of the independent ALS sub-channel and protection set design. Electrical separation group assignments are also designated in the Interface Requirements Specification. Based on the above, the NRC staff concludes that the DCPP ALS subsystem meets the criteria of this PSAI.

   b. Application Specific Core Diversity Comparison Checks – Specifications should identify any application-specific ALS-102 logic signals that need to be subject to the core diversity comparison checks.

      Though the DCPP ALS subsystem uses core diversity for all ALS processed safety functions, no application-specific comparison checks are specified or required for the design. The NRC staff determined no application-specific ALS-102 logic signal comparisons are used in the DCPP design; therefore, the criteria of this PSAI are not applicable.

   c. Fail Safe Behavior – Specifications should identify application-specific fail-safe behavior that should result from any comparison check mismatch.

      Section 3.2.1.16.3 thru 3.2.1.16.6 of the Functional Requirements Specification (Reference 126) specify preferred failure states for PPS analog and discrete outputs. The preferred failure state for analog and discrete ALS outputs is also specified in the ALS "System Design Specification," Revision 9, 6116-00011, September 2015

(Reference 127), Appendix A through Appendix D, for cases where the output can be set. The tables in these annexes also specify the failure state for each ALS output signal upon loss of power (i.e., Energize To Trip (ETT) or De-energize To Trip (DTT)).

The diverse Core A and Core B execution path outputs are combined in hard-wired logic to ensure that the protective action is taken if directed by either path. The system is designed such that a single failed safety actuation path cannot prevent a protective action from being performed. Based on Westinghouse's January 5, 2016, response (Reference 198) to the NRC staff's request for additional information (RAI) 73 dated December 23, 2015 (Reference 237), if an ALS-102 board detects a mismatch between the outputs of its diverse logic cores, it will set its outputs to a prescribed fail-safe state before entering the HALT mode of operation.

The NRC staff reviewed the Functional Requirements Specification and Interface Requirements Specification (Reference 98) documents to determine the "safe state" for ALS safety functions; however, the licensee did not initially designate fail-safe states for the ALS subsystem. In request for additional information (RAI) 64 dated March 31, 2014 (Reference 190), the NRC requested that the licensee establish a basis for the ALS fail-safe states that are specified in the "ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, May 2013 (Reference 163). In its RAI response dated April 30, 2014 (Reference 17), the licensee revised Sections 3.2.1.16.3 and 3.2.1.16.6 of the Functional Requirements Specification to add information regarding requirements for fail-safe states of the ALS subsystem. Additional information was also provided by Westinghouse by letter dated January 5, 2016, in response to RAI 73 (Reference 198). These requirements serve as the licensee's basis for the fail-safe states of the ALS subsystem. The ALS Functional Requirements Specification therefore identifies the fail-safe behaviors that should result from a redundancy checker comparison check mismatch. The NRC staff determined the DCPP ALS subsystem satisfies the criteria of this PSAI.

d. Additional Diversity Measures – Specifications should identify any additional diversity measures, such as functional, signal, or additional logic diversity, that are included in the safety system in the context of maintaining plant safety.

The DCPP PPS diversity design includes external systems that provide diversity for the digital PPS including the Nuclear Instrumentation System and the Anticipated Transient Without Scram Mitigation System. These systems are not being modified for the PPS replacement and were determined by the NRC staff to be sufficiently diverse from the digital ALS subsystem. Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation provides an evaluation of the diversity and defense-in-depth (D3) aspects of the DCPP PPS. The PPS replacement D3 analysis credits these external systems to ensure the PPS safety functions are performed for all required failures to be considered. The NRC staff also evaluated the level of diversity between the ALS and the Tricon PPS subsystems and determined these systems to be sufficiently diverse from each other.

e. Extent of Built-in Diversity – The applicant or licensee should describe the extent that it relies upon the techniques and processes that provide levels of defense against programming common-cause failures, which are described in the "ALS Diversity Analysis," Revision 2, 6002-00031, January 2013 (Reference 141), for its use of the ALS platform and its application-specific ALS-102 logic. Using this information, the licensee should demonstrate the application adequately addresses potential plant vulnerabilities to common-cause programming failures in consideration of Standard Review Plan (SRP) Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," July 2012 (Reference 49), and DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance," Revision 2, dated June 5, 2009 (Reference 236), as applicable.

The DCPP license amendment request describes the level of diversity required for the ALS subsystem as including both core diversity features and embedded design diversity features for all safety functions allocated to the ALS subsystem. Both of these diversity features were evaluated as part of the ALS platform in the NRC staff's safety evaluation dated April 19, 2011 (Reference 196).

Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation provides an NRC staff evaluation of the replacement DCPP PPS diversity characteristics. The NRC staff determined that the DCPP PPS ALS subsystem adequately addresses potential plant vulnerabilities to common-cause programming failures. The criteria of BTP 7-19 and DI&C-ISG-02 were considered in this evaluation and the NRC staff determined that the DCPP PPS ALS subsystem meets the diversity requirements specified in these documents.

f. Identification of Echelons of Defense – The applicant or licensee's D3 analysis should identify the echelon(s) of defense (i.e., control, reactor trip system (RTS), engineered safety features actuation system (ESFAS), and monitoring and display) within the plant that each ALS platform-based instrumentation and control (I&C) function is assigned.

The D3 analysis for the PPS replacement identified the control, reactor trip, ESFAS, and monitoring and display information associated with the functions that are assigned to the ALS subsystem. This analysis was evaluated by the NRC staff and found to be an acceptable means for addressing the potential for common-cause programming errors in the DCPP PPS ALS subsystem. See Section 3.6, "Defense-in-Depth and Diversity," of this safety evaluation for a detailed summary of the D3 analysis as well as an evaluation of the DCPP plant-specific diversity features.

g. Diverse Manual Control Features – When manual controls are not provided as discrete hard-wired components connected to the safety equipment at a point downstream of the plant's digital I&C safety system outputs, the applicant or licensee's D3 analysis should demonstrate simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse program-based digital equipment performs any coordinated system-level actuation logic, if applicable.

Manual controls associated with the PPS safety actuation functions are provided in the main control room. These controls provide signals to the solid state protection system which is downstream and independent from the digital PPS being replaced. These controls are provided as discrete hard-wired components connected to the solid state protection system safety equipment at a point downstream of the plant's digital PPS safety system outputs. The criteria of this plant-specific action item (PSAI) does not apply to the DCPP PPS replacement project because these controls are not being modified by this amendment and because they will remain functionally independent from the digital PPS.

20. IEEE Std. 603-1991 Compliance – As discussed within Section 3.10, "Compliance to IEEE Std 603-1991," of the ALS platform safety evaluation (Reference 30), although the NRC staff determined the ALS platform supports meeting various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing this safety evaluation should identify the approach taken to meet each applicable clause of IEEE Std. 603-1991. The applicant or licensee should demonstrate the plant-specific and application-specific use of the ALS platform meets the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

The NRC staff performed an application-specific evaluation of the replacement DCPP PPS using the criteria of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995 (Reference 32). The results of that evaluation are provided in Section 3.9, "Conformance with IEEE Std. 603-1991, 'IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,'" of this safety evaluation. The licensee has demonstrated the DCPP ALS PPS subsystem application satisfactorily meets all applicable criteria of IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Reference 32), and, therefore, the requirements of this PSAI are satisfied.

21. Demonstration of Sufficient Isolation – An applicant or licensee referencing the safety evaluation for the Advanced Logic System Topical Report (Reference 30), should identify all safety/non-safety interfaces and interdivisional interfaces. In addition, for each interface, the applicant or licensee should demonstrate sufficient isolation has been provided by a qualified isolation device to meet IEEE Std. 603, Clause 5.6.3.1(2), IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" (Reference 64), as endorsed by Regulatory Guide (RG) 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, February 2005 (Reference 63), and in accordance with Standard Review Plan (SRP) Branch Technical Position (BTP) 7-11, "Guidance on Application and Qualification of Isolation Devices" (Reference 44), and DI&C-ISG-04 (Reference 34), as applicable. The application-specific information should identify the maximum credible voltage associated with each plant-specific use of each interface, and demonstrate each qualified isolation device applied to each interface is compatible with its maximum credible voltage and sufficient to prevent damage to the ALS platform safety-related components.

Communications Interfaces

Section 3.1.6.2.4, "ALS Communications," of this safety evaluation describes all communications interfaces associated with the DCPP PPS ALS subsystem. The PPS design does not include communication paths between redundant safety divisions (i.e., protection sets). The PPS ALS subsystem design does include two communication interfaces between the PPS and non-safety-related systems; the process plant computer via the gateway computer and the ALS maintenance work station computer.

The ALS communication interfaces between each ALS subsystem chassis to the DCPP gateway computer are isolated, serial, and one-way. The TxB1 communications channel does not receive any data, handshaking, or instructions from the gateway computer. The ALS-102 core logic board communication channel TxB1 is a communication link where the receive capability is physically disabled by hardware as described in the ALS-102 Design Specification. The receiver is configured such that the transmit data are looped back for channel integrity testing. The ALS-102 core logic board is electrically incapable of receiving information from outside the ALS-102 via the transmit busses TxB1 and

TxB2. Thus, the ALS does not require use of an isolation device to prevent communication to the ALS from the gateway computer.

The TxB2 communication channel that transmits data to the non-safety-related maintenance work station is also a serial, one-way link which has no handshaking. The third ALS serial communications channel enables Test ALS Bus functions between ALS Service Unit maintenance software in the maintenance work station and the ALS controller. This communication path is normally disabled, with two-way communications permitted only when the Test ALS Bus communication link is physically connected between the Test ALS Bus and the ALS maintenance work station. Communications are not possible on the Test ALS Bus when the communication link is physically disconnected.

Electrical Non-Communications Interfaces

The NRC staff performed an application-specific evaluation of the replacement DCPP PPS using the criteria of IEEE Std. 603-1991 which includes an evaluation of Clause 5.6.3.1(2) criteria. The results of that evaluation are provided in Section 3.9, "Conformance with IEEE Std. 603-1991, 'IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,'" of this safety evaluation.

Sections 4.2.3.2, "ALS Input Modules," and 4.2.3.3, "ALS Output Modules," of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12) describe the ALS input and output modules. The input channels are protected against electrostatic discharge and surge voltages using transient voltage suppressors. All input channels are isolated from the ALS logic and are designed to withstand 1500 Volts (V) root mean squared (RMS) difference between the field domain and the digital domain.

The NRC staff evaluated the implementation of this isolation requirement by reviewing the PPS Functional Requirements Specification (Reference 126) as well as the ALS platform "System Design Specification," Revision 9, 6116-00011, dated September 2015 (Reference 127). The NRC staff found that the 1500 V isolation requirement is an ALS platform requirement that is not application-specific. The ALS platform specification states that the isolation domain is rated for, and tested for, 1500 V RMS and 1500 Volts direct current (VDC); however, operational voltage across this isolation domain should not exceed 500 V RMS and 500 VDC.

Section 4.2.13, "Communications (Section D.1.2 of DI&C-ISG-06 [1])," of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), describes the ALS-102 core logic board isolation. The Class 1E/non-1E data communication for the ALS-102 core logic board is described in Section 2.2.1.3, "ALS-102 Communication Channels," and 5.3.2, "Broadcasting Information to

Non-Safety Devices using TxB Busses," of the Advanced Logic System Topical Report (Reference 30), and in Position 2 of the "Diablo Canyon PPS ISG-04 Matrix, Nuclear Safety Related," 6116-00054, Revision 0, dated November 9, 2012 (Reference 200). The electrical isolation of the transmit busses is performed by magnetic couplers located on the ALS-102 core logic board. The TxB isolators are described in the ALS-102 Hardware Design Specification. Fault isolation occurs by way of board-mounted transient voltage suppressors, board-mounted fuses, and external fuses. As stated in Section 4.2.13, 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 RG 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, February 2005 (Reference 63), and will be documented in a supplemental test report to be issued at a future date.

22. IEEE Std. 7-4.3.2-2003 Compliance – As discussed within Section 3.11, "Conformance with IEEE Std 7-4.3.2-2003," of the ALS platform safety evaluation, although the NRC staff determined the ALS platform supports meeting various sections and clauses of IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Reference 33), an applicant or licensee referencing this safety evaluation should identify the approach taken to meet each applicable clause of IEEE Std. 7-4.3.2-2003. The applicant or licensee should demonstrate the plant-specific and application-specific use of the ALS platform meets the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.

    The NRC staff performed an application-specific evaluation of the replacement DCPP PPS using the criteria of IEEE Std. 7-4.3.2-2003. The results of that evaluation are provided in Section 3.10, "Conformance with IEEE Std. 7-4.3.2-2003, 'IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,'" of this safety evaluation. The licensee has demonstrated the DCPP ALS PPS subsystem application satisfactorily meets all applicable criteria of IEEE Std. 7-4.3.2-2003 and, therefore, the requirements of this PSAI are satisfied.

23. IEEE Std. 1012-1998 Compliance –As discussed within Section 3.11.2.3.3, "IEEE Std 7-4.3.2-2003 Clause 5.3.3 - Verification and Validation," of the ALS platform safety evaluation (Reference 30), although the NRC staff determined the ALS platform independent verification and validation (IV&V) processes support various sections and clauses of IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74), an applicant or licensee should demonstrate it has fulfilled the tasks that have been deferred to an applicant's or licensee's use of the ALS platform. Some IEEE Std. 1012-1998 tasks cannot be fulfilled within the ALS platform topical report scope, because the

task is project-specific, such as hazard analysis and risk analysis. Other IEEE Std. 1012-1998 tasks cannot be fulfilled within the ALS platform topical report scope, because the task is not performed on a platform component, such as system integration test, system acceptance test, installation, operation, and maintenance tasks. An applicant or licensee referencing the Advanced Logic System Topical Report safety evaluation should ensure appropriate activities are included in its project-specific V&V plan and the performance of each activity is acceptably independent. The project-specific V&V plan should identify any alternative method(s) to IEEE Std. 1012-1998 for any IV&V task and demonstrate the alternative method(s) provides equivalent assurance.

The NRC staff performed an evaluation of the "Automation and Field Services Independent Verification and Validation, Diablo Canyon PPS VV Plan," Revision 3, 6116-00003, November 2014 (Reference 135), using the criteria of IEEE Std. 1012-1998. The results of that evaluation are provided in Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation. The licensee has demonstrated the DCPP ALS PPS subsystem application satisfactorily meets all applicable criteria of IEEE Std. 1012-1998 and, therefore, the requirements of this PSAI are satisfied.

3.14 Site Inspection Follow-up Items

This section includes recommended inspection activities to be addressed by the NRC during site acceptance testing, installation, startup testing, and operation of the Diablo Canyon Power Plant (DCPP) process protection system (PPS). The inspection activities are intended to verify licensee activities that are not part of the licensing process but are related to the safe operation of the digital PPS. These inspection items provide the context and basis for inspection activities and should be used in the development of the on-site inspection plans.

3.14.1 Tricon Site Inspection Follow-up Items

1. Ensure that the new Tricon keyswitch (used for setting the subsystem operating mode) is added to the Key Control Procedure.

2. Ensure that the procedures to be used for Tricon subsystem configuration activities include controls for the operation of the channel out-of-service switches such that only channels being tested can be configured when other channels of the associated protection set are to remain operable during the activity. Refer to Section 3.7, "Communications," of this safety evaluation for additional information regarding this evaluation item.

3. Ensure that Tricon out-of-service switch operations are appropriate for testing activities such that no test is performed to render a Tricon system safety function inoperable without first declaring the affected channel inoperable and entering the appropriate limiting condition for operation (LCO) for this condition. Refer to

Sections 4.2.1.1, "Triconex Tricon-Based PPS Equipment," and 4.8.10, "ISG-04 Interdivisional Communications Staff Position No. 10," of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12). Refer to Section 3.7, "Communications," of this safety evaluation for additional information regarding this inspection item.

The licensee has committed to place PPS channels out of service prior to changing any associated configuration parameters. Ensure procedures which include activities for changing configuration parameters include steps to declare the affected channel inoperable prior to operation of the Tricon out-of-service switches.

4. Review Surveillance Test Procedures associated with the PPS and ensure any steps to operate the Tricon out-of-service switches do not conflict with operations procedural controls to address channel operability during test activities. Refer to Section 3.1.6.1.1, "Tricon Main Chassis," and 3.7, "Communications," of this safety evaluation for additional information regarding this evaluation item.

5. Perform a comparison of the required Tricon subsystem software configuration data to the software installed onto the delivered plant PPS equipment. The intended system software is recorded in the Tricon Master Configuration List and must be consistent with the Test System Application Program (TSAP) Project file (i.e., .pt2 file) and in the current Software Development Checklist. Refer to Section 3.4.1.7, "Software/Core Logic Configuration Management Plan," and 3.4.3.7, "System Build Documents," of this safety evaluation for additional information regarding this evaluation item.

6. Verify the PPS operating procedures, and maintenance procedures are consistent with the design capability of the Tricon PPS subsystem and plant technical specifications. Refer to Section 3.10.1.3.2, "IEEE 7-4.3.2-2003, Clause 5.5.2, Design for Test and Calibration," of this safety evaluation for additional information regarding this evaluation item.

7. Ensure the licensee performs an evaluation of the user documentation (e.g., technical manuals, training material, procedural changes) associated with the Tricon PPS subsystem prior to plant startup. This evaluation verification and validation (V&V) activity was not included in the "Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Reference 118), and is expected to be a licensee activity which can be further inspected by the NRC for compliance with Regulatory Guide (RG) 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 2, July 2013 (Reference 73). Refer to Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation and Institute of Electrical and Electronics Engineers (IEEE) Std. 1012-1998, "IEEE Standard for Software

Verification and Validation" (Reference 74), for additional information regarding this evaluation item.

8. Perform a review of procedures that are to be used to control operation of the Tricon maintenance work station computers. Ensure that the use and limitations of use of the maintenance work station features are consistent with Section 3.1.7.1, "Maintenance Work Station," of this safety evaluation.

9. Verify that the licensee's software training plan for the Tricon subsystem is acceptable. Refer to Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems," Section B.3.1.7, "Software Training Plan (STrngP)" (Reference 46), for additional information regarding this evaluation item.

10. Verify that the licensee's software operations plan for the Tricon subsystem is acceptable. Refer to SRP BTP 7-14, Section B.3.1.8, "Software Operations Plan (SOP)" (Reference 46), for additional information regarding this evaluation item.

11. Ensure that the modification test plan specifies the necessary testing to be performed during and after installation of the Tricon PPS subsystem and that the test procedures are prepared, reviewed, approved, controlled, and performed under the existing operating procedures. Refer to Section 3.4.2.4, "Testing Activities," of this safety evaluation for additional information regarding this evaluation item.

12. Ensure the PPS design control package includes an update of the DCPP Final Safety Analysis Report Update (Reference 52) to reflect the modified Tricon PPS subsystem specific design bases. Refer to Section 3.9.1.12, "IEEE 603-1991, Clause 4.12, Special Design Basis," of this safety evaluation for additional information regarding this evaluation item.

13. Verify the licensee has developed and implemented measures to control the use of portable media such as universal serial bus (USB) flash drives or portable disk drives which can be connected to the Tricon maintenance work station or keyboard-video-mouse (KVM) switch.

14. Verify the licensee has developed and implemented measures to control access to the Maintenance and Test Facility.

15. For the Tricon maintenance work stations, verify the TriStation 1131 and maintenance work station application security level settings are set up by the licensee prior to installation of Tricon PPS equipment into the plant.

3.14.2 ALS Site Inspection Follow-up Items

1. Ensure that the procedures to be used for Advanced Logic System (ALS) subsystem configuration activities include controls for the connection of the ALS Test ALS Bus (TAB) communication link such that only channels being tested can be configured when other channels of the associated protection set are to remain operable during the activity. Refer to Section 3.7, "Communications," of this safety evaluation for additional information regarding this evaluation item.

2. Ensure that ALS TAB communication link operations are appropriate for testing activities such that no test is performed to render an ALS system safety function inoperable without first declaring the affected channel inoperable and entering the appropriate limiting condition for operation (LCO) for this condition. Refer to Section 4.2.1.2, "FPGA-Based ALS Platform," and 4.8.10, "ISG-04 Interdivisional Communications Staff Position No. 10," of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12). Refer to Section 3.7, "Communications," of this safety evaluation for additional information regarding this inspection item. The licensee has committed to place PPS channels out of service prior to changing any associated configuration parameters. Ensure procedures which include activities for changing configuration parameters include steps to declare the affected channel inoperable prior to operation of the ALS TAB communication link.

3. Perform a comparison of the required ALS subsystem configuration data to the installed logic configuration including ALS board part numbers, non-volatile memory part numbers and associated revision levels of the delivered plant PPS equipment. The intended system logic is recorded in the Diablo Canyon PPS ALS Board Configuration Drawings 5116-10201, 5116-30201, 5116-31101, 5116-32101, 5116-40201, 5116-40202, 5116-42101, 5116-42102. Refer to Section 3.4.1.7, "Software/Core Logic Configuration Management Plan," and 3.4.3.7, "System Build Documents," of this safety evaluation for additional information regarding this evaluation item.

4. Verify the PPS operating procedures and maintenance procedures are consistent with the design capability of the ALS PPS subsystem and plant technical specifications. Refer to Section 3.10.1.3.2, "IEEE 7-4.3.2-2003, Clause 5.5.2, Design for Test and Calibration," of this safety evaluation for additional information regarding this evaluation item.

5. Ensure the licensee performs an evaluation of the User Documentation (e.g., technical manuals, training material, procedural changes) associated with the ALS PPS subsystem prior to plant startup. This evaluation verification and validation (V&V) activity was not included in the ALS "Diablo Canyon PPS VV Plan," Revision 3, 6116-00003, November 2014 (Reference 135), and is expected to be a licensee activity which can be further inspected by the NRC for

compliance with Regulatory Guide (RG) 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 2, July 2013 (Reference 73). Refer to Section 3.4.1.6, "Software/Core Logic Verification & Validation Plan," of this safety evaluation and IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation" (Reference 74), for additional information regarding this evaluation item.

6. Perform a review of procedures that are to be used to control operation of the ALS maintenance work station computers. Ensure that the use and limitations of use of the maintenance work station features are consistent with Section 3.1.7.1, "Maintenance Work Station," of this safety evaluation.

7. Verify that the licensee's training plan for the ALS subsystem is acceptable. Refer to Section 3.4.1.7, "Software/Core Logic Configuration Management Plan," of this safety evaluation for additional information regarding this evaluation item.

8. Verify that the licensee's operations plan for the ALS subsystem is acceptable. Refer to Section 3.4.1.8, "Software/Core Logic Test Plan," of this safety evaluation for additional information regarding this evaluation item.

9. Ensure that the modification test plan specifies the necessary testing to be performed during and after installation of the ALS PPS subsystem and that the test procedures are prepared, reviewed, approved, controlled, and performed under the existing operating procedures. Refer to Section 3.4.2.4, "Testing Activities," of this safety evaluation for additional information regarding this evaluation item.

10. Ensure the PPS design control package includes an update of the DCPP Final Safety Analysis Report Update to reflect the modified ALS PPS subsystem specific design bases. Refer to Section 3.9.1.12, "IEEE 603-1991, Clause 4.12, "Special Design Bases," of this safety evaluation for additional information regarding this evaluation item.

11. Verify the licensee has developed and implemented measures to control the use of portable media such as universal serial bus (USB) flash drives or portable disk drives which can be connected to the ALS maintenance work station or keyboard-video-mouse (KVM) switch.

12. For the ALS maintenance work stations, verify the maintenance work station application security level settings are setup by the licensee prior to installation of PPS equipment into the plant.

13. Inspect cables interfacing to the rear of the ALS chassis. Upon system installation, ensure conformance with interface/boundary condition 2 as defined in Section 6.2, "Equipment Interface/Boundary Conditions Compliance

Information," of the "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235).

14. Inspect field cable Installation. Upon system installation, inspect external field cabling to ensure compliance with installation limitation 4 as defined in Section 6.3, "Installation Limitations Compliance Information," of the "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235).

15. Determine if electrostatic discharge precautions are being used during installation of PPS ALS equipment. During system installation, inspect to determine if ALS equipment is being handled in accordance with limitation 7 as defined in Section 6.3, "Installation Limitations Compliance Information," of the "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235).

16. The licensee is required to demonstrate the maximum temperature, including temperature rise, within each cabinet containing ALS components does not exceed the platform specification. This could not be confirmed during the safety evaluation because ALS equipment will not be in plant cabinets until site installation of the PPS is complete. Upon system installation, ensure the licensee performs a maximum temperature, including temperature rise test, to demonstrate compliance with installation limitation 8 as defined in Section 6.3, "Installation Limitations Compliance Information," of the "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235). See Section 3.5.1.1, "Temperature/Humidity," of this safety evaluation for additional details.

17. Inspect chassis ground-braid installations. Upon system installation, inspect ALS chassis ground connections to ensure compliance with installation limitation 9 as defined in Section 6.3, "Installation Limitations Compliance Information," of the "ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Reference 235).

18. Verify proper operation of the KVM switches. Upon system installation, review operating procedures to ensure proper steps for operation of the KVM switch are in place.

3.14.3 Licensee Site Inspection Follow-up Items

Perform a review of the licensee requirements traceability matrix. Confirm that licensee requirements tracing activities provide reasonable assurance that all licensee requirements are correctly implemented in the Diablo Canyon PPS.

3.15 Response Time Characteristics

In Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, Revision 5, "Guidance for Evaluation of Conformance to IEEE Std. 603," March 2007 (Reference 41), Section 5.5, "System Integrity," states that a special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the critical points of time identified as required by Clause 4 of IEEE 603. Standard Review Plan (SRP) Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance" (Reference 50), provides supplemental guidance on evaluating response time for digital computer-based systems, and discusses design constraints that allow greater confidence in the results analyses or prototype testing to determine real-time performance.

The accident analysis of design-basis events at nuclear power plants includes a determination of how soon the protective actions are needed to mitigate those design-basis events. In addition, 10 CFR 50.36(c)(1)(ii)(A) requires that the technical specifications include the limiting safety systems settings for nuclear reactors, selected so that the "automatic protective action will correct the abnormal situation before a safety limit is exceeded." Once the total time required for a protective action has been determined, licensees allocate portions of that time to elements of the protective system (i.e., the time required for the sensors to respond to changes in plant conditions, the time for rack/processing equipment, the time require for the actuation logic, and the time required for a valve to close or a pump to start).

Pacific Gas and Electric Company (PG&E, the licensee) defined the digital process protection system (PPS) response time requirements for the processing equipment and actuation logic in the PPS Interface Requirements Specification (Reference 98). The Tricon/Advanced Logic System (ALS) PPS response time requirements are the same as the response time requirements for the Eagle 21 PPS. Eagle 21 was installed as a form, fit, and functional replacement for the original 7100 analog protection system; however, the Trip Time Delay (TTD) function was added as a means to reduce the frequency of unnecessary feedwater-related reactor trips. This TTD function was evaluated by the NRC in the Eagle 21 safety evaluation dated October 7, 1993 (Reference 23), and was determined to be acceptable. The TTD function is included in the replacement PPS. The Diablo Canyon Power Plant (DCPP) Final Safety Analysis Report Update (FSARU) accident analysis also includes assumptions regarding the TTD function to account for this variable trip delay time when the reactor is operating below 50 percent power.

The basis for the PPS response time requirements is the accident analyses in Chapter 15 of the DCPP FSARU. Limiting trip setpoints assumed in accident analyses and the time delays assumed for each trip function are given in Table 15.1-2 of the FSARU. Several of the safety functions credited in the FSARU are reliant of the PPS and thus PPS time delays are a component of the overall assumed delay times listed. Additionally, Surveillance Requirement 3.3.1.16 requires that the licensee periodically verify reactor trip system response times to be within established limits. The NRC staff confirmed that the specified response times for the replacement PPS are consistent with the assumptions made in the DCPP FSARU.

The PPS is allocated a maximum response time of 409 milliseconds (ms). For functions that require reactor coolant system temperature signal processing, the response times for the ALS and Tricon subsystems are allocated to these systems as follows to meet the overall PPS response time requirement stated above:

ALS	175 ms	For resistance temperature detector (RTD) signal processing
Tricon	200 ms	
Contingency	34 ms	
Total PPS Allocation	409 ms	

The required response time of 409 milliseconds is also reflected in the PPS Functional Requirements Specification (Reference 126), Section 3.2.1.10. The Functional Requirements Specification defines this required parameter as being the time from input signal conditioner to conditioned output signal with all external transfer functions set to 1 and all externally adjustable time delays set to 0.0.

The PPS Functional Requirements Specification specifies that the digital system processor time base or loop-cycle time shall be measurable with an accuracy of +/- 0.1 percent of the utilized time base. This functional requirement provides the system user with the capability of monitoring and accessing the deterministic performance of the PPS during operation.

Tricon

Section 3.4.1, "Response Time," of the safety evaluation for the Tricon platform (Reference 29) states, in part, that "the actual response time for any particular system will depend upon the actual system configuration and may vary significantly from simple to complex systems." As such, the determination of the suitability of the Tricon programmable logic controller system response time characteristics for the DCPP PPS plant application is a plant-specific requirement.

To demonstrate the Tricon subsystem's ability to meet the PPS response time requirements, a DCPP PPS Time Response Calculation is documented in "Diablo Canyon Power Plant, Maximum TSAP Scan Time," Revision 1, 993754-1-817-P, dated April 9, 2012 (Reference 238). This calculation determined what the maximum Test System Application Program (TSAP) scan time would be for the DCPP PPS subsystem. This calculation accounted for the PPS specific system configuration and worst-case conditions for time-dependent data transfer associated with the Tricon safety functions being performed by the system. Relevant variables used to determine worst-case conditions were:

- Number of subsystem inputs and outputs to be processed
- Variations in design between individual PPS protection sets

- Number of protective functions being performed by the PPS application
- Dependence on ALS system processing for RCS temperature signal inputs

It was then determined that the applications for protection sets 1 and 2 were more limiting and were thus used as a basis for determining the maximum scan time for the system. The Tricon worst-case response time was then calculated by determining and adding the input, application execution, and output times of the PPS application together. The result was an overall maximum allowable scan time to ensure that the 200-millisecond allocation time assigned to the Tricon subsystem would not be exceeded.

Additionally, a 34-millisecond contingency time is allowed for the combined PPS Tricon and ALS system and half of that contingency time, or 17 milliseconds, was factored into the Tricon scan time calculation. The resulting maximum allowable scan time for the DCPP Tricon subsystem was then used as a basis for setting the TSAP scan time.

The performance requirements for the Tricon PPS subsystem applications are included in the PPS "Software Requirements Specification (SRS)," Revision 4, 993754-11-809-P, dated January 21, 2014 (Reference 166), "Software Requirements Specification (SRS), Protection Set II," Revision 2, 993754-12-809-P, dated October 17, 2012 (Reference 167), "Software Requirements Specification (SRS), Protection Set III," Revision 2, 993754-13-809-P, dated October 17, 2012 (Reference 168), and "Software Requirements Specification (SRS), Protection Set IV," Revision 2, 993754-14-809-P, dated October 17, 2012 (Reference 169). Section 3.4.1 of these SRS documents refers back to the "Diablo Canyon Power Plant, Maximum TSAP Scan Time," Revision 1, 993754-1-817-P, dated April 9, 2012 (Reference 238),[5] for application scan time requirements.

During the June 3-5, 2014, regulatory audit of Invensys (Reference 38), the NRC staff confirmed that the actual scan time setting for all Tricon PPS applications is set to a value less than the maximum TSAP calculated scan time. The NRC staff reviewed the relation between the specified time response requirements for PPS and the safety analysis response time assumptions listed in the DCPP FSARU Table 15.1-2. The NRC staff verified Tricon application scan times to be correctly set. The staff also reviewed the software verification scan time test results reported in operational testing to determine the longest scan-time duration. The results of these tests are in the "System Time Response Confirmation Reports," 993754-11-818-P, Revision 0, dated July 1, 2014 (Reference 201), 993754-12-818-P, Revision 0, dated December 1, 2014 (Reference 202), 993754-13-818-P, Revision 0, dated December 1, 2014 (Reference 203), and 993754-14-818-P, Revision 0, dated December 1, 2014 (Reference 204), which confirmed satisfactory scan time performance results.

[5] The "Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Reference 102), refers to the "Validation Test Specification (VTS)," Revision 1, 993754-1-812-P, dated April 4, 2014 (Reference 140), as being the Max Allowable Scan Time for the system instead of 993754-1-817-P, Revision 1 (Reference 238). The NRC staff verified that all four SRSs refer to the correct 993754-1-817-P, Revision 1, document; therefore, the error is in the SDD.

ALS

The ALS board access time is the fixed interval allocated to exchange data with an individual board using the Reliable ALS Bus protocol. Requirements within the "ALS Subsystem, System Design Specification," Revision 9, 6116-00011, September 2015 (Reference 127), and the "ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, May 2013 (Reference 163), specify the ALS subsystem frame time used for the DCPP PPS application.

Although the ALS platform establishes a fixed board access time, other aspects—including the number of times a board is accessed per frame, the number of boards accessed per frame, the sequence of board accesses per frame, and the frame time itself—are determined during the application-specific design phase. The number and type of input and output boards used in the DCPP PPS is established and will not change during system operation. Each DCPP PPS ALS subsystem contains the following platform components as defined in the DCPP PPS ALS System Design Specification:

- One ALS-302 digital input board
- Two ALS-402 digital output boards
- One ALS-311 RTD board
- One ALS-321 analog input board
- Two ALS-421 analog output boards
- One ALS-102 core logic board

Section 5.1 of the DCPP PPS ALS-102 FPGA Requirements Specification states that acquiring of input values from the ALS input boards, ALS-102 application processing, and output processing to the ALS output boards are performed during the acquire, process, and control phases of each frame. Furthermore, each of the system boards is accessed only one time during each frame.

The frame time is the interval between accessing each specific board so that information will have been read once from all system input boards and written once to all system output boards. All of these design aspects establish the fixed interval for each safety function performed.

The ALS system Time Base Frame Rate is a parameter for each of the ALS subsystems which can be monitored as a means of ensuring continued deterministic behavior of the system. Each of the ALS subsystems contain a feature that provides a time base frame rate output signal that can be measured by external test equipment to determine if the subsystems' timing performance is sufficient to support operational requirements of the system. The Time Base Frame Rate for the DCPP can be measured during system operation without affecting the systems' ability to perform its safety functions.

During the June 22-26, 2015, regulatory audit at the Westinghouse facilities (Reference 39), the NRC staff confirmed how ALS system Time Base Frame Rate is measured using the test points described in Section 3.6 of the ALS System Design Description.

The ALS platform provides design features to alert operators to the system's condition when the Reliable ALS Bus transaction time, board access time, or frame time is not met. The ALS boards within each ALS subsystem of the PPS also contain watchdog timers which automatically detect and annunciate the absence of a heartbeat signal from the associated field programmable gate array. The DCPP ALS system will activate alarms when a failure to meet timing is detected. This alarm will notify operators when timing is not being met so that corrective actions can be initiated.

The PPS's deterministic performance capabilities are evaluated in Section 3.17, "Deterministic System Behavior," of this safety evaluation. The response time testing of the PPS was performed as part of the system factory acceptance test. Based on the specification, analysis, deterministic system performance characteristics, and system response time performance test results, the NRC staff determined that the DCPP PPS meets all requirements for safety system response time performance.

3.16 System Setpoints Evaluation

The Diablo Canyon Power Plant (DCPP) process protection system (PPS) license amendment request does not introduce instrument allowable value changes for any of the reactor trip system or engineered safety feature actuation system functions in the proposed technical specification changes. A previous setpoints analysis was performed by the licensee for protection system functions processed by the PPS to address changes to setpoint input values for rack calibration accuracies, rack drift, temperature effects, and response time associated with the Eagle 21 PPS. The functional requirements of the replacement PPS are compatible with the Eagle 21 PPS for these parameters.

The methodology for calculating instrumentation allowable values is based on Westinghouse document "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," Revision 0, WCAP-17706-P, January 2013 (Reference 221). Section 3.9.3.8, "IEEE 603-1991, Clause 6.8, Setpoints," of this safety evaluation provides additional details on the NRC staff's evaluation of PPS setpoints and updated setpoint calculations.

3.17 Deterministic System Behavior

The review guidance of Standard Review Plan (SRP) Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 6.1, "Automatic Control" (Reference 41), identifies considerations that address digital computer-based systems for the evaluation of the automatic control capabilities of safety system command features. This review guidance advises that the evaluation should confirm that the system's real-time performance characteristics are deterministic and known. Standard Review Plan (SRP) Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance" (Reference 50), discusses design practices for computer-based systems that should be avoided. These practices include non-deterministic data communications, non-deterministic computations, interrupts, multitasking, dynamic scheduling, and event-driven design. The technical position further states that methods for controlling the associated risk to acceptable real-time performance should be described when such practices are employed.

The Electric Power Research Institute technical report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996 (Reference 101), provides specifications and guidance intended to achieve a deterministic execution cycle with deterministic behavior that ensures an application and its constituent tasks will be completed within specified time limits. In particular, EPRI TR-107330, Section 4.4.1.3, "Program Flow Requirements," specifies that, where scanning of the inputs and application program execution are performed in parallel, methods should assure the input scan and application program execution are completed each cycle.

The deterministic performance characteristics of each of the process protection system (PPS) subsystem platform's was evaluated by the NRC staff during the individual platform safety evaluations for the Triconex Approved Topical Report (Reference 29) and the Advanced Logic System Topical Report (Reference 30). Each of these evaluations concluded that there are application-specific parameters that could influence the systems' ability to perform in a deterministic manner. Therefore, the staff re-evaluated deterministic behavior characteristics for each subsystem within the context of the DCPP PPS application.

ALS

Only the ALS-102 core logic boards are subject to application-specific response time performance and deterministic behavior variation. All other ALS boards are generic and have been accepted by the NRC as components of the ALS generic platform. The ALS platform and architecture provide design features to ensure the ALS-102 core logic board will perform its functions to completion within the board access time and frame time. Timing aspects of the ALS subsystem are further evaluated in Section 3.15, "Response Time Characteristics," of this safety evaluation.

Tricon

Deterministic performance characteristics of the Tricon V10 platform were evaluated in Section 3.4.2, "Deterministic Performance" of the safety evaluation for the Triconex Approved Topical Report (Reference 29). The NRC staff reviewed specific details pertaining to determinism of the Tricon platform including the description of the software in Section 2.1.3, "Tricon System Software, of the topical report.

The Tricon programmable logic controller system's triple-redundant architecture is designed such that input signal processing, application-specific function performance, and output signal processing are performed by redundant sets of components operating in parallel to provide highly reliable safety functions. The complete scan cycle time for each Tricon subsystem is dependent on the specific application being executed by the processors. System deterministic performance characteristics can be influenced by several application-specific design parameters, which are accounted for in the PPS "Maximum TSAP Scan Time," Revision 1, 993754-1-817-P, dated April 9, 2012 (Reference 238). See Section 3.15, "Response Time Characteristics," of this safety evaluation for a more detailed evaluation of the Tricon response time calculation.

All Tricon PPS subsystem input, processing, and output functions are controlled by the process application program or Test System Application Program (TSAP). The PPS TSAP is designed to perform all of the PPS safety functions in each TSAP scan cycle. The cycle time for each TSAP scan cycle is established during system design and is not subject to changes during TSAP program execution.

Both the Tricon and the ALS platforms use internal backplane communications as a means of transferring data between application-controlling modules (processors for Tricon and the ALS-102 board for ALS) and the systems input and output modules. These backplane communications are fundamental components of each platform which are relied upon for deterministic and predictable performance of all safety system functions. These backplane communications interfaces are separate and independent from communications interfaces to external non-safety-related systems. Design details for each of these communications interfaces are described in the Triconex Approved Topical Report for Tricon (Reference 29) and the Advanced Logic System Topical Report for ALS (Reference 30), and each has been evaluated and determined to be acceptable by the NRC in the associated platform safety evaluation for these topical reports.

Based on the above, the NRC staff concludes that the DCPP PPS's real-time performance is deterministic and known, as documented by the system performance requirements and tests performed for validation of these requirements. Therefore, the NRC staff concludes that the DCPP PPS meets the criteria for deterministic and predictable performance and is acceptable.

3.18 Human Performance Review

3.18.1 Description of Operator Action(s) and Assessed Safety Significance

Pacific Gas and Electric Company (PG&E, the licensee) stated in its January 25, 2016, submittal (Reference 20), that the process protection system (PPS) is an automatic system that does not require operator involvement to perform its function to initiate a reactor trip and engineered safety features actuation. The PPS does not require manual intervention or acknowledgement of actuation commands to complete a protective function. The PPS replacement design is not adding any new or changed manual operator actions.

In its letter dated December 26, 2011 (Reference 1), the licensee stated that the current Eagle 21 PPS is susceptible to credible software common-cause failures that could adversely affect automatic performance of the protection function and require manual operator action to be taken. The licensee also stated in its letter dated April 30, 2013 (Reference 12), that several manual actuations previously credited in the Eagle 21 PPS safety evaluation report to mitigate a Final Safety Analysis Report Update (FSARU) Chapter 15, "Accident Analyses," accident or event with a concurrent common-cause failure have been eliminated by the PPS replacement, due to the built-in diversity provided by the Advanced Logic System (ALS) equipment. Automatic mitigation functions would 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 events were to occur with a concurrent, postulated common-cause failure in the Eagle 21 PPS:

1. Loss of forced reactor coolant flow in a single loop above the permissive 8 indicated by 2/3 reactor coolant flow-low;

2. Accidental reactor coolant system depressurization, including steam generator tube rupture, steam line break, and loss-of-coolant accident indicated by low pressurizer pressure; and

3. Large-break loss-of-coolant accident and steam line break indicated by high containment pressure.

Thus, the PPS replacement automatically mitigates events that currently require manual protective action, should a common-cause failure disable the primary and backup protection functions. The use of built-in diversity in the design of the replacement PPS would eliminate the need for manual operator action to address software common-cause failure and preclude the need for an external diverse actuation system.

Automatic actuation of protective functions not adversely affected by common-cause failure is preferred where manual operator action would otherwise be required to mitigate a FSARU Chapter 15 accident or event with concurrent common-cause failure. This reduces the number of manual operator actions and lessens the burden on the operator.

Although the aforementioned manual operator actions are no longer credited in the PPS replacement, the operators will retain the ability to take the same manual actions, and do so by the same means as would be accomplished by the currently installed equipment, using the same human-system interface (HSI).

In accordance with the generic risk categories established in NUREG-1764, "Guidance for the Review of Changes to Human Actions," Revision 1, September 2007 (Reference 54), the elimination of credited manual operator actions during a postulated software common-cause failure in a PPS replacement reviewed herein is not considered "risk-important" due to the fact that it reduces the operators' workload during an accident, thereby reducing the overall risk. Because of its low risk importance, the NRC staff performed a "Level Three" review (i.e., the least stringent of the graded reviews possible under the guidance of NUREG-1764).

3.18.2 Operating Experience Review

In its letter dated January 25, 2016 (Reference 20), the licensee stated that PG&E personnel performed a review of industry operating experience for the PPS replacement Tricon and ALS technology, including a review and inspection of installed applications of the technology, and did not identify any human factors engineering-related issues.

The licensee stated that Diablo Canyon Power Plant (DCPP) has significant operating experience with the Tricon system as a result of installation of the technology in multiple non-safety-related control system applications (e.g., process control system, feedwater control system, and turbine control system). Only one prior operating experience issue at DCPP for the Tricon hardware was identified; it was associated with the use of an improper grounding method and was not a human factors engineering-related issue.

The licensee further stated that for the ALS subsystem portion of the PPS replacement design, Wolf Creek Generating Station installed the CS Innovations field programmable gate array-based ALS design in the main steam and feedwater isolation system (Reference 95). There have not been any actuation failures of the ALS hardware since it has been installed.

Based on PG&E's operating history of successful implementation of the Tricon subsystem portion of the PPS replacement design, and licensee's evaluation of relevant operating experience and its applicability to the changes proposed in this license amendment request, the NRC staff determined that the licensee's operating experience review is acceptable.

3.18.3 Task Analysis

The PPS is an automatic system that does not require operator involvement to perform its function to initiate a reactor trip and engineered safety features actuation. The PPS replacement design does not change any existing or add any new manual operator actions. As stated in Section 3.18.1 of this safety evaluation, the PPS replacement reduces the number of credited manual operator actions and thus lessens the burden on the operator.

In its request for additional information (RAI) 77(c) dated December 23, 2015 (Reference 237), the NRC staff requested the licensee to identify if the emergency operating procedures were affected by the proposed modification and, if so, to describe the changes that were required of the control room task analysis that had been previously completed as part of the Detailed Control Room Design Review. In RAI response dated January 25, 2016 (Reference 20), the licensee stated that no changes to the emergency operating procedures in connection with the PPS replacement were required. The licensee also described the changes required to alarm response procedures and operating procedures (see Section 3.18.5 of this safety evaluation for additional information).

Based on the licensee's statement that no changes were required to the emergency operating procedures and the description of changes required to alarm response procedures and one operating procedure (for each unit), the NRC staff concludes that the updates to the control room task analysis was not necessary and the licensee's treatment of this review element is acceptable.

3.18.4 Human-System Interface Design

In its letter dated October 26, 2011 (Reference 1), as supplemented by letters dated April 30, 2013 (Reference 12), and January 25, 2016 (Reference 20), the licensee stated that for the PPS replacement, the existing operator interface with the control panel mounted switches and indicators, as well as lights, controls, alarms, and annunciators will be maintained. Also, as part of the PPS replacement, an existing HSI unit in the control room that was previously installed for a process control system replacement project will be used for system health and status displays and provide detailed system diagnostic results when failure indication on the control panel occurs. This HSI unit will obtain PPS data through a connection to an existing plant data network non-safety Gateway computer that is installed in the plant. The DCPP HSI Development Guidelines Document will be utilized for the development of displays of PPS information on the HSI unit, which will be implemented during the development of the formal design change, following receipt by PG&E of the safety evaluation approving this change.

The existing Eagle 21 PPS four redundant protection sets will be replaced with four redundant and independent protection sets that receive input from sensors and provide output to two trains (Train A and Train B) of the solid state protection system. Each protection set in the PPS replacement contains a software-based Tricon V10 processor subsystem and a diverse safety-related CS Innovations ALS subsystem. Each of the four protection sets contains a separate non-safety-related maintenance work station for the Tricon subsystem and the ALS subsystem – a total of eight maintenance work stations for the PPS that will be installed in the PPS instrumentation cabinets. The non-safety-related Tricon maintenance work station will be used to maintain and configure the Tricon and to view data from Tricon. Likewise, the non-safety ALS maintenance work station will be used to maintain and configure the ALS.

Under operating plant conditions, the maintenance work station will display plant parameters and diagnostic information. The maintenance work station will be used for PPS information processing and local display, and to facilitate maintenance, such as modifying Tricon safety system parameters. Use of the maintenance work station is in accordance with site-specific administrative (procedural) and physical-access controls. The DCPP HSI Development Guidelines Document was used by the vendors to develop the display screens and operator interface with maintenance work stations. System trouble alarms will be generated by the PPS replacement on the main annunciator system (as is currently done with Eagle 21), and the maintenance work station will provide alarm monitor and other data display capabilities to allow determination of the specific cause of an alarm.

The chassis for the Tricon and ALS subsystems will be installed in normally closed PPS instrumentation cabinets that are manually opened to access the chassis. To support system monitoring, surveillances, troubleshooting, and maintenance, the chassis contain local controls, indicators, and status lights.

Based on the information provided above, the proposed modification does not alter the HSI in any significant way. Therefore, the NRC staff determined the use of the DCPP HSI Development Guidelines Document for the development of the display screens of PPS information on the HSI unit and maintenance work stations to be acceptable.

3.18.5 Procedure Design

In its letter dated January 25, 2016 (Reference 20), the licensee stated that the operational aspects of the digital PPS replacement are designed to be consistent with the existing digital Eagle 21 PPS, for nearly all operational aspects. There are no technical specification instrument setpoint changes required due to the PPS replacement and no revised surveillance intervals are being implemented as part of the PPS replacement project. The licensee identified that the following changes to operating procedures will be required:

- Alarm response procedures "AR PK" [Alarm Response Panel Key] series control panel procedures will be revised, to incorporate the use of the significant improvements in the diagnostic capabilities of the PPS replacement design. For example, when a control panel alarm occurs, the procedures will be updated to provide instructions for use of the HSI unit in the control room, to display the detailed system diagnostic results, to support determination of what specific failure occurred, and to support troubleshooting, repair, and return of the PPS to technical specification Operable status. The integrated PPS replacement system used for site acceptance testing will also be used to develop and verify operational procedures. An inspection follow-up activity item 1 was included in Section 3.18.8 of this safety evaluation, to confirm implementation of revisions to "AR PK" series of alarm response procedures.

- Operating Procedure (OP) AP-5, "Malfunction of Eagle 21 Protection Channel and Control," for each unit will need to be updated, to include the control panel and plant process computer information that will be provided when the instrumentation failures occur in the PPS replacement equipment, to facilitate diagnosis of the failure. An inspection follow-up activity item 2 was included in Section 3.18.8 below, to confirm implementation of revision to OP AP-5.

Emergency Operating Procedure (EOP) E-0, "Reactor Trip or Safety Injection," directs manual actions to initiate a reactor trip and safety injection signal if they do not occur automatically (i.e., in the case of a postulated failure of a PPS automatic actuation). The licensee stated that the PPS replacement design will not alter the current plant system level manual actions to initiate a reactor trip, safety injection, or other engineered safety features actuation. Therefore, no changes affecting operators will be required for EOP E-0 because these manual actions will not be changed due to the PPS replacement.

The licensee further stated that Surveillance Test Procedures for Instrumentation ("STP I-" series surveillance test procedures) for the channel check trip actuating device operational test, channel operability test, and channel calibrations will be revised, to incorporate the Tricon and ALS equipment component names and equipment-specific actions needed to perform the tests. The integrated PPS replacement system used for site acceptance testing will also be used to develop and verify maintenance procedures.

The NRC staff determined the plan to revise affected procedures to be acceptable, based on: (1) the description of limited changes to procedures, (2) PG&E's verification of the procedures during site acceptance testing, as described in Section 3.18.7 of this safety evaluation, and (3) implementation of inspection follow-up activity items 1 and 2, as described in Section 3.18.8 of this safety evaluation.

3.18.6 Training Program and Simulator Design

In its letter January 25, 2016 (Reference 20), the licensee stated that as part of the design change process, which uses the Systematic Approach to Training process for plant modifications, the required operator training needs to support the PPS replacement modification will be identified. Any necessary updates to the operator simulator training will be developed and implemented as needed, as part of the design change process. The integrated PPS replacement system used for site acceptance testing will also be used to perform training. An inspection follow-up activity item 3 was included in Section 3.18.8 of this safety evaluation, to verify development and implementation of operator simulator training.

The licensee further stated that modifications to the simulator computer code will be required, to model the operational characteristics of the PPS replacement system Tricon and ALS equipment. No physical changes to the simulator control board will be required for installation of the PPS replacement system.

The NRC staff determined that the licensee's plans for operator training and changes to the plant-specific simulator are acceptable.

3.18.7 Human Factors Verification and Validation

In its letters dated April 30, 2013 (Reference 12), and January 25, 2016 (Reference 20), the licensee stated that the integrated PPS replacement system used for site acceptance testing will be used to verify operational and maintenance procedures, as well as to perform training. An inspection follow-up activity item 4 was included in Section 3.18.8 of this safety evaluation, to ensure that operational procedures are verified and validated during the site acceptance testing, in accordance with the review criteria of NUREG-0711, "Human Factors Engineering Program Review Model," Revision 3, November 2012 (Reference 56).

The NRC staff determined the process for verification of operational procedures to be acceptable, based on: (1) the fact that the proposed PPS replacement design does not change any existing or add any new manual operator actions, (2) the human-system interface changes are minimal (as described in Section 3.18.4, "Human-System Interface Design," of this safety evaluation), (3) no physical changes to the simulator control board will be made, and

(4) implementation of inspection follow-up activity item 4, as described in Section 3.18.8 of this safety evaluation.

3.18.8 Human Performance Review - Site Inspection Follow-Up Items

This section includes recommended inspection activities to be addressed by the NRC during site acceptance testing, installation, startup testing, and operation of the DCPP PPS. The inspection activities are intended to verify selected licensee activities that are related to the human performance aspects of the safe operation of the PPS replacement system. These inspection items provide the context and basis for inspection activities and should be used in the development of the on-site inspection plans. These items include:

1. Ensure that "AR PK" series alarm response procedures for each unit were revised as necessary, to provide instructions for use of the human-system interface unit in the control room, to display the detailed system diagnostic results, and to support troubleshooting, repair, and return of the PPS to technical specification Operable status.

2. Ensure that Operating Procedure "OP AP-5" for each unit was revised as necessary, to include the control panel and plant process computer information that will be provided when the instrumentation failures occur in the PPS replacement equipment.

3. Verify that operator training needs to support the PPS replacement modification were identified, and any necessary updates to the operator simulator training were developed and implemented as needed, as part of the design change process.

4. Ensure that operational procedures are verified and validated during the site acceptance testing, in accordance with the review criteria of NUREG-0711, Revision 3 (Reference 56).

4.0 RESULTS OF NRC STAFF REVIEW

The results of the NRC staff evaluations are described below.

4.1 Digital Replacement of the Process Protection System – Design Review

Summary of Regulatory Compliance

This safety evaluation discussed the acceptability of the Tricon and ALS platforms as used in the DCPP PPS. The Overall Plant criteria defined in Section 3.1.2 of the DCPP FSARU, establish minimum requirements for the design of the DCPP nuclear power plants. Institute for Electrical and Electronics Engineers (IEEE) Std. 603-1991, "IEEE Standard Criteria for Safety

Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995 (Reference 32), is also incorporated in 10 CFR 50.55a(h)(2).

The regulatory guides and the endorsed industry codes and standards listed Section 2.2, "Regulatory Guidance," of this safety evaluation were used as guidelines in determining the acceptability of the methods used by the licensee to comply with the regulatory requirements listed in Section 2.1, "Regulatory Criteria," of this safety evaluation.

The NRC staff concludes that the design of the digital DCPP PPS is acceptable and meets the relevant requirements of 10 CFR 50.55(i), 10 CFR 50.55a(h), 10 CFR 50.62, and the overall plant criteria defined in Section 3.1.2 of the DCPP FSARU as discussed below.

Section 10 CFR 50.36, "Technical specifications," requires, in part; where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded. The NRC staff determined that the DCPP replacement PPS is in compliance with this requirement because the proposed DCPP Units 1, and 2, technical specification changes for the replacement PPS do not include instrumentation setpoint (allowable value) changes for any of the PPS functions. See Sections 3.16, "System Setpoints Evaluation," and 3.9.3.8, "IEEE 603-1991 Clause 6.8, Setpoints," of this safety evaluation for additional information on PPS setpoints.

Section 10 CFR 50.55(i), "Codes and Standards," requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The PPS hardware and software development processes are addressed by the licensee in Sections 4.3, 4.4, and 4.5 of the Enclosure to the licensee's letter dated April 30, 2013 (Reference 12), and are addressed by conformance with the codes and standards listed in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP). Sections 4.10 and 4.11 of the Enclosure to the licensee's letter dated April 30, 2012, address conformance with the principle standards associated with the development of digital instrumentation and control (I&C) safety systems. The NRC staff evaluated conformance of the PPS with these standards and the results of this evaluation are contained in Sections 3.9, "Conformance with IEEE Std. 603-1991, 'IEEE Standard Criteria For Safety Systems for Nuclear Power Generating Stations,'" and 3.10, "Conformance with IEEE Std. 7-4.3.2-2003, 'IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,'" of this safety evaluation. Both equipment vendors, Westinghouse and Invensys, used these codes and standards in the development of the ALS and Tricon platforms as well as the DCPP plant-specific PPS applications for them. Therefore, the DCPP PPSs are in conformance with this requirement.

As applicable to DCPP, paragraph 10 CFR 50.55a(h)(2) states that the "protection systems must be consistent with their licensing basis or may meet the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995." Compliance of the DCPP PPS with IEEE 603-1991 was evaluated by the NRC staff and the results of this evaluation are contained within Section 3.9 of this safety evaluation. The NRC staff determined the DCPP PPS to be compliant with the criteria of IEEE Std. 603-1991 as well as the correction sheet dated January 30, 1995, and therefore conforms to this regulatory requirement.

Section 10 CFR 50.62 contains requirements for anticipated transients without scram (ATWS). The replacement digital DCPP PPS did not modify or replace the existing ATWS equipment, and the licensee demonstrated that the existing equipment is diverse from the ALS and Tricon equipment used to implement the digital PPS. The NRC staff reviewed the diverse actuation systems, including ATWS, and determined the replacement PPS to be in conformance with this requirement. The NRC staff verified the applicant has provided sufficient information and that the results of the review support the following conclusions:

- The review of the instrumentation and control aspects of the DCPP PPS includes the reactor trip system (RTS) and engineered safety feature actuation system (ESFAS). The PPS detects plant conditions requiring the operation of RPS/ESFAS and/or auxiliary supporting features and other auxiliary features and initiates operation of the systems. The RPS trips the reactor following automatic initiation by the PPS and solid state protection system or manual initiation by the plant operator. The ESFAS initiate operation of the ESFAS functions following automatic initiation by the PPS and solid state protection system or manual initiation by the plant operator.

- The NRC staff concludes that the design of the DCPP PPS is acceptable and meets Criterion 12, 14, 15, 19, 21, 22, and 23 of the DCPP Overall Plant Requirements as defined in Section 3.1.2 of the DCPP FSARU; 10 CFR 50.34(f); and 10 CFR 50.55a(h)(2).

- The NRC staff conducted a review of the DCPP replacement PPS for conformance to the guidelines in the regulatory guides, industry standards, and SRP branch technical positions applicable to RTS and ESFAS systems. The NRC staff concludes the DCPP PPS conforms to all applicable quality guidelines for these systems. The NRC staff therefore concludes that the requirements of Criterion 1 of the DCPP FSARU 10 CFR 50.55(i) and 10 CFR 50.55a(h)(2) have been met.

- The review included the identification of those systems and components of the DCPP PPS designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the NRC staff concludes that the licensee has identified those systems and components consistent with the design bases for those systems. Section 3.5, “Equipment Environmental Qualification,” of this safety evaluation, addresses the qualification programs to demonstrate the capability of the systems and components needed to survive the above effects. Therefore, the NRC staff concludes that the identification of these systems and components satisfies the requirements of Criterion 2 and 40 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of DCPP replacement PPS status information, manual initiation capabilities, control capabilities, and provisions to support safe shutdown, the NRC staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation and control of RPS and ESFAS functions. The RPS and ESFAS controls appropriately support actions to operate the nuclear power unit safely under normal conditions and to achieve and maintain a safe condition under accident conditions. Therefore, the NRC staff concludes that the DCPP PPS design satisfies the requirements of Criterion 12, 14, and 15 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of DCPP replacement PPS, manual initiation capabilities and provisions to support reactor trip, the NRC staff concludes that the design condition of the reactor coolant pressure boundary are not exceeded as appropriate to assure adequate safety. Therefore, the NRC staff concludes that the DCPP PPS design satisfies the requirements Criterion 9 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of DCPP replacement PPS, manual initiation capabilities and provisions to support containment isolation, the NRC staff concludes that the containment isolation initiation function as appropriate to assure adequate safety. Therefore, the NRC staff concludes that the DCPP PPS design satisfies the requirements of Criterion 10 and 49 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of system functions, the NRC staff concludes the DCPP replacement PPS conforms to the requirements of IEEE Std. 603-1991 as well as the correction sheet dated January 30, 1995. The PPS setpoint methodology conforms to the guidance of Regulatory Guide (RG) 1.105, "Setpoints for Safety-Related Instrumentation," Revision 3, December 1999 (Reference 67). Based upon this review and coordination with those having primary review responsibility for the accident analysis, the NRC staff concludes that the DCPP PPS includes the provision to sense accident conditions and anticipated operational occurrences consistent with the accident analysis presented in Chapter 15 of the FSARU and evaluated in the safety evaluation. Therefore, the NRC staff concludes that the DCPP PPS satisfies the requirements of Criterion 14, 15, 20, 21, and 25 of Section 3.1.2 in the DCPP FSARU.

- The DCPP replacement PPS conforms to the guidelines for periodic testing in RG 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0, February 1972 (Reference 58), and RG 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995 (Reference 69). The bypassed and inoperable status indication conforms to the guidelines of

RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 1, February 2010 (Reference 59). The DCPP PPS conforms to the guidelines on the application of the single-failure criterion in IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 61), as supplemented by RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," Revision 2, November 2003 (Reference 60). Based on the review, the NRC staff concludes that the DCPP PPS satisfies the requirement of IEEE Std. 603-1991 with regard to the system reliability and testability. Therefore, the NRC staff concludes that the DCPP PPS satisfies these requirements of Criterion 19 of Section 3.1.2 in the DCPP FSARU.

- The DCPP replacement PPS conforms to the guidelines in RG 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, February 2005 (Reference 63), for the protection system independence. Based on the review, the NRC staff concludes that the DCPP PPS satisfies the requirement of IEEE Std. 603-1991 with regard to the system's independence. Therefore, the NRC staff concludes that the DCPP PPS satisfies the requirements of Criterion 20, 21, and 22 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of the failure modes and effects analysis for the replacement DCPP PPS, the NRC staff concludes that the system is designed to fail into a safe state if conditions such as disconnection of the system, loss of energy, or a postulated adverse environment are experienced. Therefore, the NRC staff concludes that the DCPP PPS satisfies the requirements of Criterion 26 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of the interfaces between the replacement DCPP PPS and plant operating control systems, the NRC staff concludes that the system satisfies the requirements of IEEE Std. 603-1991 with regard to control and protection system interactions. Therefore, the NRC staff concludes the DCPP PPS satisfies the requirements of Criterion 22 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of the replacement DCPP PPS, the NRC staff concludes that the system satisfies the protection system requirements for malfunctions of the reactivity control system such as accidental withdrawal of control rods. Chapter 15, "Accident Analyses," of the FSARU and safety evaluation address the capability of the system to ensure that fuel design limits are not exceeded for such events. Therefore, the NRC staff concludes that the DCPP PPS satisfies the requirements of Criterion 31 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of the replacement DCPP PPS, the NRC staff concludes that the system satisfies the protection system requirements initiation of the reactivity control system safety function. Therefore, the NRC staff concludes that the DCPP PPS satisfies the requirements of Criterion 19 and 20 of Section 3.1.2 in the DCPP FSARU.

- The NRC staff conducted a review of the digital replacement DCPP PPS for conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures. The NRC staff concludes that the digital DCPP PPS is testable and remains operable using either onsite or offsite power. The controls associated with redundant RPS or ESFAS are independent and satisfy the single-failure criterion and, therefore, meet the relevant requirements of Criterion 37, 44, 49, and 52 of Section 3.1.2 in the DCPP FSARU.

- The conclusions noted above are based upon the requirements of IEEE Std. 603-1991, with respect to the design of the replacement digital DCPP PPS. Therefore, the NRC staff determined that the DCPP PPS satisfies the requirements of 10 CFR 50.55a(h) as well as the correction sheet dated January 30, 1995.

- Based on the review of software and logic development plans and the review of the computer software and system logic development processes and design outputs, the NRC staff concludes that the digital subsystems which comprise the PPS meet the guidance of RG 1.152. Therefore, the special characteristics of digital systems have been adequately addressed, and the NRC staff concludes that the replacement digital DCPP PPS satisfies these requirements of Criterion 1 and 19 of Section 3.1.2 in the DCPP FSARU.

- Based on the review of the licensee's diversity and defense-in-depth analysis, the NRC staff concludes that the digital replacement DCPP PPS complies with the criteria for defense against common-cause failure in digital instrumentation and control systems. Therefore, the NRC staff concludes that adequate diversity and defense against common-cause failure have been provided to satisfy these requirements of Criterion 19, 20, 21, and 22 of Section 3.1.2 in the DCPP FSARU.

4.2 Human Performance Review

Based on the statements provided by the licensee that: (1) the existing operator interface, including that control panel mounted switches, indicators, status lights, alarms, and annunciators will be maintained; (2) that the changes to the human-system interface are minimal (such as the addition of non-safety-related maintenance work stations for the Tricon and Advanced Logic System subsystems and the development of additional display screens for display of process protection system information on an existing HSI unit in the control room); (3) that the operating procedures and training will be updated; and (4) successful completion of site inspection follow-up items identified in Section 3.18.8 of this safety evaluation, the NRC staff concludes that the changes proposed by the license amendment request are acceptable, from the human performance perspective.

4.3 Regulatory Commitments

The licensee made a number of commitments by letters dated October 26, 2011 (Reference 1), December 20, 2011 (Reference 2), April 2, 2012 (Reference 3), June 6, 2012 (Reference 5), September 11, 2012 (Reference 7), March 25, 2013 (Reference 11), April 30, 2013 (Reference 12), April 30, 2014 (Reference 16), and June 22, 2015 (Reference 19). The commitments are related to the following:

- Future submittals before approval of the license amendment request and has already been fulfilled.
- Procedural changes and administrative controls to be implemented after approval/implementation of the license amendment request.
- Explanation of design features incorporated in the design either to comply with the regulatory design requirements or follow guidance provided by regulatory guides and industry codes and standards.

The NRC staff approval of the license amendment request did not rely on these commitments. The design features explained by the commitments were verified during the review process.

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the California State official was notified of the proposed issuance of the amendments. The State official had no comments.

6.0 ENVIRONMENTAL CONSIDERATION

The amendments change a requirement with respect to the installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendments involve no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendments involve no significant hazards consideration and there has been no public comment on such finding published in the *Federal Register* on June 7, 2016 (81 FR 36606). Accordingly, the amendments meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendments.

7.0 CONCLUSION

The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) there is reasonable assurance that such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendments will not be inimical to the common defense and security or to the health and safety of the public.

8.0 REFERENCES

1. Becker, J. R., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, PPS Replacement License Amendment Request," DCL-11-104, dated October 26, 2011 (Agencywide Documents Access and Management System (ADAMS) Package Accession No. ML113070457).

2. Becker, J. R., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Security-Related Information to Support Process Protection System Replacement, License Amendment Request 11-07," DCL-11-123, dated December 20, 2011 (ADAMS Accession No. ML113610541).

3. Becker, J. R., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Response to Items Contained in NRC Acceptance Review of License Amendment Request for Digital Process Protection System Replacement," DCL-12-030, dated April 2, 2012 (ADAMS Accession No. ML12094A072).

4. Becker, J. R., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Tricon V10 Time Response Calculation for the License Amendment Request for Digital Process Protection System Replacement," DCL-12-039, dated April 30, 2012 (ADAMS Accession No. ML12131A513).

5. Becker, J. R., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-12-050, dated June 6, 2012 (ADAMS Package Accession No. ML121700592).

6. Welsch, J. M., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Quality Assurance Plan and Revised Phase 1 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-12-069, dated August 2, 2012 (ADAMS Package Accession No. ML122220135).

7. Welsch, J. M., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement," DCL-12-083, dated September 11, 2012 (ADAMS Accession No. ML12256A308).

8. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Revised Phase 1 and Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-12-120, dated November 27, 2012 (ADAMS Package Accession No. ML130040687).

9. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Revised Phase 1 and Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-12-121, dated December 5, 2012 (ADAMS Accession No. ML12342A149).

10. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Setpoint Calculations, Setpoint Methodology, and Justification for Application of Technical Specification Changes in WCAP-14333 and WCAP-1 5376 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-13-016, dated March 7, 2013 (ADAMS Package Accession No. ML13267A127).

11. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Revised System Verification and Validation Plan and Tricon Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-13-028, dated March 25, 2013 (ADAMS Package Accession No. ML130930344).

12. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units and 2, Supplement to License Amendment Request 11-07, 'Process Protection System Replacement,'" DCL-13-043, dated April 30, 2013 (ADAMS Accession No. ML13121A089).

13. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement and Submittal of Revised PPS Replacement System Quality Assurance Plan," DCL-13-048, dated May 9, 2013 (ADAMS Accession No. ML13130A059).

14. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of CS Innovations Documents and Revised Software Configuration Management Plan for the License Amendment Request for Digital Process Protection System Replacement," DCL-13-061, dated May 30, 2013 (ADAMS Package Accession No. ML131540159).

15. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of CS Innovations Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-13-087, dated September 17, 2013 (ADAMS Accession No. ML13261A354).

16. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Tricon Revised Phase 1 and Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-14-034, dated April 24, 2014 (ADAMS Package Accession No. ML14205A031).

17. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement," DCL-14-036, dated April 30, 2014 (ADAMS Accession No. ML14121A002).

18. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Advanced Logic System Phase 2 Documents for the License Amendment Request for Digital Process Protection System Replacement," DCL-15-009, dated February 2, 2015 (ADAMS Accession No. ML15062A386).

19. Allen, B. S., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Revisions to Supplement for License Amendment Request 11-07, 'Process Protection System Replacement,'" DCL-15-072, dated June 22, 2015 (ADAMS Accession No. ML15173A469).

20. Welsch, J. M., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Response to Request for Additional Information and Submittal of Advanced Logic System Phase 2 Documents for the License Amendment Request for Process Protection System Replacement," DCL-16-011, dated January 25, 2016 (ADAMS Package Accession No. ML16049A006).

21. Welsch, J. M., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Tricon Phase 2 Documents for the License Amendment Request for Process Protection System Replacement," DCL-16-020, dated February 11, 2016 (ADAMS Package Accession No. ML16061A481).

22. Welsch, J. M., Pacific Gas and Electric Company, letter to U.S. Nuclear Regulatory Commission, "Diablo Canyon Units 1 and 2, Submittal of Documents for the License Amendment Request for Process Protection System Replacement," DCL-16-081, dated August 17, 2016 (ADAMS Accession No. ML16238A101).

23. Peterson, S. R., U.S. Nuclear Regulatory Commission, letter to Gregory M. Rueger, Pacific Gas and Electric Company, "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).

24. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, DI&C-ISG-06, "Task Working Group #6: Licensing Process, Interim Staff Guidance," Revision 1, dated January 19, 2011 (ADAMS Accession No. ML110140103).

25. Haynes, B., Invensys Operations Management, letter to U.S. Nuclear Regulatory Commission, "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).

26. Invensys Operations Management, Document No. 7286-545-1, Revision 4, "Triconex Topical Report," dated December 20, 2010 (ADAMS Accession No. ML110140443); Appendix A, "EPRI TR-107330 Requirements Compliance and Traceability Matrix," dated December 20, 2010 (ADAMS Accession No. ML110140445); Appendix B, Revision 4, "Application Guide," dated December 20, 2010 (ADAMS Accession No. ML110140446).

27. Erin, L., CS Innovations, LLC, letter to U.S. Nuclear Regulatory Commission, "CS Innovations ALS Topical Report and Supporting Documents Submittal," dated July 29, 2010 (ADAMS Accession No. ML102160471).

28. CS Innovations, Document 6002-00301, Revision 0, "Advanced Logic System Topical Report," dated July 30, 2010 (Proprietary information. Not publicly available.).

29. Invensys/Triconex, "Triconex Approved Topical Report, 7286-545-1-A, Revision 4: Nuclear Qualification of Tricon V10 Triple Modular Redundant (TMR) PLC System," dated May 15, 2012, includes U.S. Nuclear Regulatory Commission Safety Evaluation Report dated April 12, 2012 (ADAMS Accession No. ML12146A010).

30. Westinghouse Electric Company LLC, "Advanced Logic System Topical Report," Revision 4, 6002-00301-P-A, dated September 2013, includes U.S. Nuclear Regulatory Commission Safety Evaluation dated September 9, 2013 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13298A094.).

31. Wang, A. B., U.S. Nuclear Regulatory Commission, letter to John T. Conway, Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Acceptance Review of License Amendment Request for Digital Process Protection System Replacement (TAC Nos. ME7522 and ME7523)," dated January 13, 2012 (ADAMS Accession No. ML120120005).

32. Institute of Electrical and Electronics Engineers, IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet dated January 30, 1995, Piscataway, NJ.

33. Institute of Electrical and Electronics Engineers, IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Piscataway, NJ.

34. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance," Revision 1, dated March 6, 2009 (ADAMS Accession No. ML083310185).

35. Sebrosky, J. M., U.S. Nuclear Regulatory Commission, letter to Edward D. Halpin, Pacific Gas and Electric Company, "Request for Additional Information Regarding Digital Replacement of the Process Protection System Portion of the Reactor Trip System and Engineered Safety Features Actuation System (TAC Nos. ME7522 and ME7523)," dated August 7, 2012 (ADAMS Accession No. ML12208A364).

36. Sebrosky, J. M., U.S. Nuclear Regulatory Commission, letter to Edward D. Halpin, Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Report of Regulatory Audit on November 13-16, 2012, at the Invensys Operations Management Facility in Lake Forest. California, to Support Review of Digital Instrumentation and Control License Amendment Request (TAC Nos. ME7522 and ME7523)," dated March 4, 2013 (ADAMS Accession No. ML13018A149).

37. Rankin, J. K., U.S. Nuclear Regulatory Commission, letter to Edward D. Halpin, Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Regulatory Audit on February 11-14, 2013, at the CS Innovations Westinghouse Facility in Scottsdale, Arizona, for the Digital Update to the Process Protection System Amendment (TAC Nos. ME7522 and ME7523)," dated October 8, 2013 (ADAMS Accession No. ML13232A263).

38. Lingam, S. P., U.S. Nuclear Regulatory Commission, letter to Edward D. Halpin, Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Units 1 and 2 - Regulatory Audit Report for the June 3-5, 2014 Audit at the Invensys Operations Management Facility in Lake Forest, California, for the Digital Update to the Process Protection System License Amendment Request (TAC Nos. ME7522 and ME7523)," dated May 19, 2015 (ADAMS Accession No. ML15103A010).

39. Lingam, S. P., U.S. Nuclear Regulatory Commission, letter to Edward D. Halpin, Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Units 1 and 2 - Regulatory Audit Report for the June 22-26, 2015 Audit at the Westinghouse Facility in Warrendale, Pennsylvania, for the Digital Update to the Process Protection System License Amendment Request (TAC Nos. ME7522 and ME7523)," dated September 2, 2015 (ADAMS Accession No. ML15223A968).

40. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Revision 6, "Instrumentation and Controls," May 2010 (ADAMS Accession No. ML100740146).

41. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Appendix 7.1-C, Revision 5, "Guidance for Evaluation of Conformance to IEEE Std. 603," March 2007 (ADAMS Accession No. ML070550088).

42. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," March 2007 (ADAMS Accession No. ML070660327).

43. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-9, Revision 5, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," March 2007 (ADAMS Accession No. ML070550084).

44. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-11, Revision 5, "Guidance on Application and Qualification of Isolation Devices," March 2007 (ADAMS Accession No. ML070550080).

45. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-12, Revision 5, "Guidance on Establishing and Maintaining Instrument Setpoints," March 2007 (ADAMS Accession No. ML070550078).

46. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-14, Revision 5, "Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems," March 2007 (ADAMS Accession No. ML070670183).

47. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-17, Revision 5, "Guidance on Self-Test and Surveillance Test Provisions," March 2007 (ADAMS Accession No. ML070650075).

48. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-18, Revision 5, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," March 2007 (ADAMS Accession No. ML070550078).

49. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-19, Revision 6, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," July 2012 (ADAMS Accession No. ML110550791).

50. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-21, Revision 5, "Guidance on Digital Computer Real-Time Performance," March 2007 (ADAMS Accession No. ML070550070).

51. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 18, "Human Factors Engineering," Revision 2, March 2007 (ADAMS Accession No. ML070670253).

52. Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Units 1 and 2, Final Safety Analysis Report Update," Revision 22, May 2015 (ADAMS Package Accession No. ML16004A137).

53. U.S. Nuclear Regulatory Commission, NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980 (ADAMS Accession No. ML051400209).

54. U.S. Nuclear Regulatory Commission, NUREG-1764, "Guidance for the Review of Changes to Human Actions," Revision 1, September 2007 (ADAMS Accession No. ML072640413).

55. U.S. Nuclear Regulatory Commission, NUREG-0700, "Human-System Interface Design Review Guidelines," Revision 2, May 2002 (ADAMS Accession No. ML021700373).

56. U.S. Nuclear Regulatory Commission, NUREG-0711, "Human Factors Engineering Program Review Model," Revision 3, November 2012 (ADAMS Accession No. ML12324A013).

57. U.S. Nuclear Regulatory Commission, NRC Information Notice 97-78, "Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times," dated October 23, 1997 (ADAMS Accession No. ML031050065).

58. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0, February 1972 (ADAMS Accession No. ML083300530).

59. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 1, February 2010 (ADAMS Accession No. ML092330064).

60. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Revision 2, November 2003 (ADAMS Accession No. ML033220006).

61. Institute of Electrical and Electronics Engineers, IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Piscataway, NJ.

62. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.62, "Manual Initiation of Protection Actions," Revision 1, June 2010 (ADAMS Accession No. ML092530559).

63. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, February 2005 (ADAMS Accession No. ML043630448).

64. Institute of Electrical and Electronics Engineers, IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Piscataway, NJ.

65. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Revision 1, June 1984 (ADAMS Accession No. ML003740271).

66. Institute of Electrical and Electronics Engineers, IEEE Std. 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Piscataway, NJ.

67. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation," Revision 3, December 1999 (ADAMS Accession No. ML993560062).

68. Instrument Society of America, Part 1 of ISA-S67.04-1994, and ANSI/ISA-67.04-01-2006, "Setpoints for Nuclear Safety-Related Instrumentation," Research Triangle Park, NC.

69. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995 (ADAMS Accession No. ML003739468).

70. Institute of Electrical and Electronics Engineers, IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," Piscataway, NJ.

71. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Revision 3, July 2011 (ADAMS Accession No. ML102870022); Revision 2, January 2006 (ADAMS Accession No. ML053070150).

72. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.153, "Criteria for Safety Systems," Revision 1, June 1996 (ADAMS Accession No. ML003740022).

73. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 2, July 2013 (ADAMS Accession No. ML13073A210).

74. Institute of Electrical and Electronics Engineers, IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation," Piscataway, NJ.

75. Institute of Electrical and Electronics Engineers, IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits," Piscataway, NJ.

76. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (ADAMS Accession No. ML003740102).

77. Institute of Electrical and Electronics Engineers, IEEE Std. 828-1990, "IEEE Standard for Software Configuration Management Plans," Piscataway, NJ.

78. Institute of Electrical and Electronics Engineers, IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management," Piscataway, NJ.

79. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, July 2013 (ADAMS Accession No. ML13003A216).

80. Institute of Electrical and Electronics Engineers, IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation," Piscataway, NJ.

81. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (ADAMS Accession No. ML003740108).

82. Institute of Electrical and Electronics Engineers, IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing," Piscataway, NJ.

83. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (ADAMS Accession No. ML003740094).

84. Institute of Electrical and Electronics Engineers, IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications," Piscataway, NJ.

85. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997 (ADAMS Accession No. ML003740101).

86. Institute of Electrical and Electronics Engineers, IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," Piscataway, NJ.

87. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Revision 1, October 2003 (ADAMS Accession No. ML032740277).

88. Institute of Electrical and Electronics Engineers, IEEE Std. 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," Piscataway, NJ.

89. U.S. Department of Defense, Military Standard MIL-Std.-461E-1999, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," Philadelphia, PA.

90. International Electrotechnical Commission, IEC 61000-3, "Electromagnetic Compatibility (electromagnetic capability) - Part 3: Limits," IEC 61000-4, "Electromagnetic Compatibility (electromagnetic capability) - Part 4: Testing and Measurement Techniques," IEC 61000-6, "Electromagnetic Compatibility (electromagnetic capability) - Part 6: Generic Standards," Geneva, Switzerland.

91. Institute of Electrical and Electronics Engineers, IEEE Std. C62.41-1991, "IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits," Piscataway, NJ.

92. Institute of Electrical and Electronics Engineers, IEEE Std. C62.45-1992, "IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits," Piscataway, NJ.

93. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.209, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," Revision 0, March 2007 (ADAMS Accession No. ML070190294).

94. Institute of Electrical and Electronics Engineers, IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Piscataway, NJ.

95. Singal, B. K., U.S. Nuclear Regulatory Commission, letter to Rick A. Muench, Wolf Creek Nuclear Operating Company, "Wolf Creek Generating Station - Issuance of Amendment Re: Modification of the Main Steam and Feedwater Isolation System Controls (TAC No. MD4839)," dated March 31, 2009 (ADAMS Accession No. ML090610317).

96. Stang, J., U.S. Nuclear Regulatory Commission, letter to Dave Baxter, Duke Energy Carolinas LLC, "Oconee Nuclear Station, Units 1, 2, and 3, Issuance of Amendments Regarding Acceptance of the Reactor Protective System and Engineered Safeguard Protective System (RPS/ESPS) Digital Upgrade (TAC Nos. MD7999, MD8000, and MD8001)," dated January 28, 2010 (ADAMS Accession No. ML100130944).

97. Pacific Gas and Electric Company, "Diablo Canyon Power Plant, Topical Report: Process Protection System Replacement, Diversity & Defense in Depth Assessment," Revision 1, August 2010 (ADAMS Accession No. ML102580725).

98. Pacific Gas and Electric Company, "Diablo Canyon Power Plant Units 1 & 2, Process Protection System (PPS) Replacement, Interface Requirements Specification, Nuclear Safety Related (Non-Proprietary)," Revision 7, dated October 23, 2012 (ADAMS Accession No. ML13004A470).

99. Pacific Gas and Electric Company, "Process Protection System Controller Transfer Functions Design Input Specification," Revision 4, dated November 13, 2013 (ADAMS Accession No. ML16049A012).

100. CS Innovations, LLC, "Diablo Canyon Units 1 and 2 Process Protection System, ALS-ASU Communication Protocol," Revision A, 6116-00100, August 2012 (Proprietary information. Not publicly available.).

101. Electric Power Research Institute, TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996, Palo Alto, CA (http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=TR-107330).

102. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Design Description (SDD)," Revision 0, 993754-11-810-P, dated February 25, 2013 (Proprietary information. Not publicly available.).

103. Invensys Operations Management, "Pacific Gas and Electric Co., Nuclear Safety-Related Process Protection System Replacement Project, Project Traceability Matrix," Revision 1, 993754-1-804-P, dated October 17, 2012 (Proprietary information. Not publicly available.)

104. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Independent Verification and Validation Summary Report," Revision 1, 6116-00500, October 2015 (Proprietary information. Not publicly available.).

105. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Management Plan," Revision 8, 6116-00000, September 2015 (Proprietary information. Not publicly available.).

106. Pacific Gas and Electric Company, "DCPP Procedure CF2, Revision 8, 'Computer Hardware, Software and Database Control,'" dated October 26, 2011 (ADAMS Accession No. ML13308B832).

107. Pacific Gas and Electric Company, "DCPP Procedure CF2.1D2, Revision 10, 'Software Configuration Management for Plant Operations and Operations Support,'" dated October 26, 2011 (ADAMS Accession No. ML13308B834).

108. Pacific Gas and Electric Company, "DCPP Procedure CF2.1D9, Revision 2, 'Software Quality Assurance for Software Development,'" dated October 26, 2011 (ADAMS Accession No. ML13308B835).

109. Pacific Gas and Electric Company, "Diablo Canyon Power Plant Process Protection System (PPS) Replacement, 'Concept, Requirements, and Licensing Phase 1, Project Plan,'" Revision 1, dated October 26, 2011 (ADAMS Accession No. ML15099A062).

110. Pacific Gas and Electric Company, "Process Protection System (PPS) Replacement, System Quality Assurance Plan (SyQAP), Nuclear Safety Related," Revision 1, dated May 9, 2013 (ADAMS Accession No. ML13130A059).

111. Pacific Gas and Electric Company, "Diablo Canyon Power Plant Process Protection System (PPS) Replacement, System Verification and Validation Plan (SyVVP), Nuclear Safety Related," Revision 1, dated February 19, 2013 (ADAMS Accession No. ML13093A312).

112. Invensys/Triconex, NTX-SER-09-21, "Nuclear Systems Integration Program Manual," Revision 1, dated July 9, 2010 (Proprietary information. Not publicly available.).

113. Invensys/Triconex, NTX-SER-09-21, "Summary of the Invensys Project Procedures Manual for Safety-Related Work," Revision 0, NTX-SER-09-21, dated August 31, 2009 (Proprietary information. Not publicly available.).

114. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Project Management Plan (PMP)," Revision 3, 993754-1-905-P, dated December 18, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13093A316.).

115. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Development Plan (SDP)," Revision 2, 993754-1-906-P, dated December 18, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13093A317.).

116. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Configuration Management Plan (SCMP)," Revision 1, 993754-1-909-P, dated December 18, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13093A318.).

117. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Integration Plan (SIntP)," Revision 1, 993754-1-910-P, dated October 14, 2011 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML11319A072.).

118. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Verification and Validation Plan (SVVP)," Revision 3, 993754-1-802-P, dated December 18, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13093A313.).

119. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Safety Plan (SSP)," Revision 1, 993754-1-911-P, dated October 13, 2011 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML11319A071.).

120. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Project Quality Plan (PQP)," Revision 1, 993754-1-900-P, dated March 2, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13004A473.).

121. Institute of Electrical and Electronics Engineers, IEEE Std. 1058-1998, "IEEE Standard for Software Project Management Plans," Piscataway, NJ.

122. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Quality Assurance Plan," Revision 0, 6116-00001, May 2014 (Proprietary information. Not publicly available.).

123. Westinghouse Electric Company LLC, "Advanced Logic System, Advanced Logic System Design Tools," Revision 13, 6002-00030, May 2015 (Proprietary information. Not publicly available.).

124. Pacific Gas and Electric Company, "Diablo Canyon Power Plant Units 1 and 2, Process Protection System (PPS) Replacement, System Quality Assurance Plan (SyQAP), Nuclear Safety Related," Revision 0, dated October 26, 2011 (ADAMS Accession No. ML15099A063).

125. Westinghouse Electric Company LLC, "ALS Quality Assurance Plan," Revision 9, 6002-00001-P, dated October 25, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML12332A250.).

126. Pacific Gas and Electric Company, "Diablo Canyon Power Plant Units 1 & 2, Process Protection System (PPS) Replacement, Functional Requirements Specification, Revision 7 (Non-Proprietary)," October 2012 (ADAMS Accession No. ML13004A469).

127. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, ALS Subsystem, System Design Specification," Revision 9, 6116-00011, September 2015 (Proprietary information. Not publicly available.).

128. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Regulatory Guide 1.152 Conformance Report," Revision 0, 993754-1-913-P, dated September 6, 2011 (Proprietary information. Not publicly available.).

129. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Quality Assurance Plan (SQAP)," Revision 1, 993754-1-801-P, dated March 14, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13004A471.).

130. Institute of Electrical and Electronics Engineers, IEEE Std. 730-1998, "IEEE Standard for Software Quality Assurance Plans," Piscataway, NJ.

131. U.S. Nuclear Regulatory Commission, NUREG/CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems," dated June 11, 1993 (http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6101/cr6101.pdf).

132. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Safety Analysis," Revision 9, 993754-1-915-P, dated December 9, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A460.).

133. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Software Safety Plan," Revision 2, 6116-10020, January 2015 (Proprietary information. Not publicly available.).

134. Westinghouse Electric Company LLC, "ALS V&V Plan," Revision 8, 6002-00003-P, January 2013 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13108A088.).

135. Westinghouse Electric Company LLC, "Automation and Field Services Independent Verification and Validation, Diablo Canyon PPS VV Plan," Revision 3, 6116-00003, November 2014 (Proprietary information. Not publicly available.).

136. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Test Plan," Revision 4, 6116-00005, October 2014 (Proprietary information. Not publicly available.).

137. Invensys/Triconex, "Tricon V10.5.2, V&V Test Report," Revision 1.1, dated January 14, 2011 (Proprietary information. Not publicly available.).

138. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety Related Process Protection System Replacement, Diablo Canyon Power Plant, Validation Test Plan (VTP)," Revision 2, 993754-1-813-P, dated December 18, 2012 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13093A315.).

139. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Verification Test Plan (SVTP)," Revision 1, 993754-868-P, dated April 3, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML14205A039.).

140. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Validation Test Specification (VTS)," Revision 1, 993754-1-812-P, dated April 4, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML14205A040.).

141. Westinghouse Electric Company LLC, "ALS, ALS Diversity Analysis," Revision 2, 6002-00031, January 2013 (Proprietary information. Not publicly available.).

142. Westinghouse Electric Company LLC, "ALS Platform FPGA VV Test Plan," Revision 9, 6002-00018, February 2013 (Proprietary information. Not publicly available.).

143. Pacific Gas and Electric Company, "SCM 36-01, Revision 1, Process Protection System Replacement Software Configuration Management Plan (SCMP)," dated March 18, 2013 (ADAMS Accession No. ML13154A047).

144. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Engineering Department Manual, Configuration Management," Revision 8.0, EDM 20.00, dated October 28, 2009 (Proprietary information. Not publicly available.).

145. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Triconex Engineering Procedure, Software Configuration and Change Control," Revision 1.4, EDM 24.00, dated April 8, 2005 (Proprietary information. Not publicly available.).

146. Westinghouse Electric Company LLC, "Advanced Logic System, ALS Configuration Management Plan," Revision 11, 6002-00002-P, March 2015 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML15314A705.).

147. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, ALS Subsystem Configuration Management Report, Release 4.2.0 for Baseline 6116-00401 Rev. 4," Revision 7, 6116-00400, October 2015 (Proprietary information. Not publicly available.).

148. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Configuration Management Baseline Report," Revision 4, 6116-00401, October 2015 (Proprietary information. Not publicly available.).

149. Westinghouse Electric Company LLC, "ALS Test Plan," Revision 4, 6002 00005, dated March 1, 2013 (Proprietary information. Not publicly available.).

150. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, System Test Design Specification," Revision 5, 6116 70030, June 2015 (Proprietary information. Not publicly available.).

151. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Diablo Canyon PPS VV Simulation Environmental Specification," Revision 2, 6116-10216, September 2015 (Proprietary information. Not publicly available.).

152. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, V&V Requirements Phase Summary Report," Revision 1, 993754-1-860-P, dated October 30, 2012 (Proprietary information. Not publicly available.).

153. CS Innovations, LLC, "Diablo Canyon PPS ALS Reliability Analysis and FMEA," Revision 1, 6116-00029, dated May 15, 2012 (Proprietary information. Not publicly available.).

154. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, V&V Design Phase Summary Report, PPSI," Revision 3, 993754-11-861-P, dated January 15, 2016 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A464.).

155. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, V&V Implementation Phase Summary Report, PPSI," Revision 1, 993754-11-862-P, dated August 7, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A465.).

156. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, V&V Implementation Phase Summary Report, PPSII-IV," Revision 1, 993754-12-862-P, dated January 15, 2016 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A468.).

157. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set I, Factory Acceptance Test Report," Revision 3, 993754-11-854-1-P, dated January 14, 2016 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A459.).

158. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set II, Factory Acceptance Test Report," Revision 0, 993754-12-854-1-P, dated December 12, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A471.).

159. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set III, Factory Acceptance Test Report," Revision 0, 993754-13-854-1-P, dated December 12, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A477.).

160. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set IV, Factory Acceptance Test Report," Revision 0, 993754-14-854-1-P, dated December 12, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A475.).

161. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, ALS Subsystem Requirements Traceability Matrix," Revision 3, 6116-00059, November 2014 (Proprietary information. Not publicly available.).

162. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Factory Acceptance Test Report," Protection Set I, Revision 0, 6116-70033; Protection Set II, Revision 0, 6116-70034; Protection Set III, Revision 0, 6116-70035; and Protection Set IV, Revision 0, 6116-70036, August 2015 (Proprietary information. Not publicly available.).

163. Westinghouse Electric Company LLC, "Diablo Canyon Units 1 and 2, Process Protection System, ALS-102 FPGA Requirements Specification," Revision 1, 6116-10201, Revision 1, May 2013 (Proprietary information. Not publicly available.).

164. Westinghouse Electric Company LLC, "Diablo Canyon Units 1 and 2, Process Protection System, Diablo Canyon PPS ALS-102 Core A FPGA Design Specification," Revision 0, 6116-10203, May 2013 (Proprietary information. Not publicly available.).

165. Westinghouse Electric Company LLC, "Diablo Canyon Units 1 and 2, Process Protection System, Diablo Canyon ALS-102 Core B FPGA Design Specification," Revision 0, 6116-10204, dated April 18, 2013 (Proprietary information. Not publicly available.).

166. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Requirements Specification (SRS)," Revision 4, 993754-11-809-P, dated January 21, 2014 (Proprietary information. Not publicly available.).

167. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Requirements Specification (SRS), Protection Set II," Revision 2, 993754-12-809-P, dated October 17, 2012 (Proprietary information. Not publicly available.).

168. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Requirements Specification (SRS), Protection Set III," Revision 2, 993754-13-809-P, dated October 17, 2012 (Proprietary information. Not publicly available.).

169. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Requirements Specification (SRS), Protection Set IV," Revision 2, 993754-14-809-P, dated October 17, 2012 (Proprietary information. Not publicly available.).

170. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Failure Modes and Effects Analysis," Revision 1, 993754-1-811-P, dated February 21, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML14205A037.).

171. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Reliability Analysis," Revision 0, 993754-1-819-P, dated October 11, 2013 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML14205A038.).

172. U.S. Department of Defense, MIL-HDBK-217F, Notice 2, "Military Handbook: Reliability Prediction of Electronic Equipment," February 1995 (http://everyspec.com/MIL-HDBK/MIL-HDBK-0200-0299/download.php?spec=MIL-HDBK-217F_NOTICE-2.014590.PDF).

173. U.S. Department of Defense, MIL-HDBK-338B, "Military Handbook: Electronic Reliability Design Handbook," October 1998 (http://everyspec.com/MIL-HDBK/MIL-HDBK-0300-0499/download.php?spec=MIL-HDBK-338B.015041.pdf).

174. Institute of Electrical and Electronics Engineers, IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," Piscataway, NJ.

175. Institute of Electrical and Electronics Engineers, IEEE Std. 577-2004, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities," Piscataway, NJ.

176. Pacific Gas and Electric Company, "PPS Seismic Qualification," dated August 8, 2016 (ADAMS Accession No. ML16238A105).

177. Pacific Gas and Electric Company, "System Level Failure Modes & Effects Analysis (FMEA)," Document No. 15-0681-FMEA-001, Revision 1, March 2016 (ADAMS Accession No. ML16238A103).

178. Lingam, S. P., U.S. Nuclear Regulatory Commission, letter to Edward D. Halpin, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Issuance of Amendments Regarding Transition to a Risk-Informed, Performance-Based Fire Protection Program in Accordance with 10 CFR 50.48(c) (CAC Nos. MF2333 and MF2334)," dated April 14, 2016 (ADAMS Accession No. ML16035A441).

179. U.S. Nuclear Regulatory Commission, NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," June 1996 (ADAMS Accession No. ML063470583).

180. Institute of Electric and Electronics Engineers, ANSI/IEEE Std. 381-1977, "IEEE Standard Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations," Piscataway, NJ.

181. Invensys Operations Management, "Environmental Test Report," Document No. 9600164-525, Revision 0, dated July 17, 2007 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML100192034).

182. Westinghouse Electric Company LLC, "ALS EQ Plan," Revision 8, 6002-00004, December 2012 (Proprietary information. Not publicly available).

183. Westinghouse Electric Company LLC, "ALS Platform EQ Summary Report," Revision 2, 6002-00200, January 2013 (Proprietary information. Not publicly available).

184. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, Advanced Logic System and Line Sense Module Equipment Qualification Summary Report," Revision 0, EQ-QR-120-PGE, September 2014 (Proprietary information. Not publicly available.)

185. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.100, Revision 3, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," September 2009 (ADAMS Accession No. ML091320468); Revision 2, June 1988 (ADAMS Accession No. ML003740293).

186. Institute of Electric and Electronics Engineers, IEEE Std. 344-2004, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Station," Piscataway, NJ.

187. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.61, Revision 1, "Damping Values for Seismic Design of Nuclear Power Plants," March 2007 (ADAMS Accession No. ML070260029)

188. Pacific Gas and Electric Company, "System Level Requirements Traceability Matrix (RTM)," Document No. 15-0681-RTM-001, March 2016 (ADAMS Accession No. ML16238A104).

189. Institute of Electric and Electronics Engineers, IEEE Std. 344-1987, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Station," Piscataway, NJ.

190. Bamford, P., U.S. Nuclear Regulatory Commission, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Request for Additional Information Regarding Digital Replacement of the Process Protection System Portion of the Reactor Trip System and Engineered Safety Features Actuation System (TAC Nos. ME7522 and ME7523)," dated March 31, 2014 (ADAMS Accession No. ML14071A181).

191. Electric Power Research Institute, TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 2, November 2000, Palo Alto, CA (http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001000603).

192. Boger, B. A., U.S. Nuclear Regulatory Commission, letter to Carl Yoder, Electric Power Research Institute, "Review of EPRI Utility Working Group Topical Report TR-102323, 'Guidelines for Electromagnetic Interference Testing in Power Plants,'" dated April 17, 1996 (ADAMS Legacy Accession No. 9605070359).

193. Electric Power Research Institute, TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 1, January 1997, Palo Alto, CA (http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=TR-102323-R1).

194. U.S. Nuclear Regulatory Commission, Staff Requirements Memorandum, SECY-93-087 – Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993 (ADAMS Accession No. ML003708056).

195. U.S. Nuclear Regulatory Commission, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994 (ADAMS Accession No. ML071790509).

196. Markley, M. T., U.S. Nuclear Regulatory Commission, letter to John T. Conway, Pacific Gas and Electric Company, "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)," dated April 19, 2011 (ADAMS Accession No. ML110480845).

197. U.S. Nuclear Regulatory Commission, NUREG/CR-7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," February 2010 (ADAMS Accession No. ML100880143).

198. Hughes, K. K., Westinghouse Electric Company LLC, "Response to NRC RAI 73 (Open Item 129)," dated January 5, 2016 (Proprietary information. Not publicly available.).

199. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety Related Process Protection System Replacement, Diablo Canyon Power Plant, 'DI&C-ISG-04 Conformance Report,'" Document No. 993754-1-912, Revision 0, dated September 6, 2011 (Proprietary information. Not publicly available.).

200. Westinghouse Electric Company LLC, "Diablo Canyon PPS ISG-04 Matrix, Nuclear Safety Related," 6116-00054, Revision 0, dated November 9, 2012 (Proprietary information. Not publicly available.).

201. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set I, System Time Response Confirmation Report," Revision 0, 993754-11-818-P, dated July 1, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A461.).

202. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set II, System Time Response Confirmation Report," Revision 0, 993754-12-818-P, dated December 1, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A466.).

203. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set II, System Time Response Confirmation Report," Revision 0, 993754-13-818-P, dated December 1, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A469.).

204. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Protection Set IV, System Time Response Confirmation Report," Revision 0, 993754-14-818-P, dated December 1, 2014 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML16061A473.).

205. U.S. Nuclear Regulatory Commission, NUREG/CR-6082, "Data Communications," August 1993 (ADAMS Accession No. ML063530379).

206. Institute of Electrical and Electronics Engineers, IEEE Std. 384-1981, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Piscataway, NJ.

207. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, V10 Tricon Reference Design Change Analysis," Revision 0, 993754-1-916-P, dated March 19, 2012 (ADAMS Accession No. ML12222A099.).

208. Invensys/Triconex, "Tricon V10.5.2 Release, Software Release Definition," 6200003-226, Revision 1.0, dated December 10, 2010 (Proprietary information. Not publicly available.).

209. Invensys/Triconex, "Tricon V10.5.2, Engineering Project Plan," Revision 1.4, 9100346-001, dated December 2, 2010 (Proprietary information. Not publicly available.).

210. Invensys/Triconex, "Technical Advisory Bulletin #183, Intermittent Inter-Leg Register Faults on Specified Tricon I/O Modules," Revision 1, 9791006-183, dated February 21, 2011 (ADAMS Accession No. ML13093A435).

211. Invensys/Triconex, "Tricon PAN 25 Fix, Engineering Project Plan," Revision 1.2, 9100428-001, dated October 12, 2011 (Proprietary information. Not publicly available.).

212. Invensys/Triconex, "Tricon PAN25 Master Test Report," Revision 1.0, dated October 12, 2011 (Proprietary information. Not publicly available.).

213. Invensys/Triconex, "Tricon V10.5.3, Software Release Definition," Revision 1.0, 6200003-230, dated September 28, 2011 (Proprietary information. Not publicly available.).

214. Invensys/Triconex, "Product Alert Notice #25—Potential Safety Issue," Revision 2, 9791010-025, dated October 12, 2011 (ADAMS Accession No. ML13093A437).

215. Invensys /Triconex, "TriStation v4.9.0 and Safety Suite Apps, Engineering Project Plan," Revision 1.3, 9100359-001, dated June 13, 2011 (Proprietary information. Not publicly available.).

216. Invensys/Triconex, "TriStation 1131 V4.9.0 Test Report," Revision 0.4, dated May 16, 2011 (Proprietary information. Not publicly available.).

217. Invensys/Triconex, "TriStation 1131 v4.9.0.117 SRD Software Release Definition," Revision 1.2, 6200097-038, dated August 23, 2011 (Proprietary information. Not publicly available.).

218. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Appendix 7.0-A, "Review Process for Digital Instrumentation and Control Systems," March 2007 (ADAMS Accession No. ML070660258).

219. Richards, S. A., U.S. Nuclear Regulatory Commission, letter to J. Troy 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)," dated December 11, 2001 (ADAMS Accession No. ML013470433).

220. Westinghouse Electric Company LLC, "Westinghouse Setpoint Calculations for the Diablo Canyon Power Plant Digital Replacement Process Protection System," Revision 0, WCAP-17696-P, January 2013 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13267A133.).

221. Westinghouse Electric Company LLC, "Westinghouse Setpoint Methodology as Applied to the Diablo Canyon Power Plant," Revision 0, WCAP-17706-P, January 2013 (Proprietary information. Not publicly available. Non-proprietary version at ADAMS Accession No. ML13267A134.).

222. Institute of Electrical and Electronics Engineers, IEEE Std. 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," Piscataway, NJ.

223. Institute of Electrical and Electronics Engineers, IEEE Std. 577-1976, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations," Piscataway, NJ.

224. U.S. Nuclear Regulatory Commission, Regulatory Issue 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," dated August 24, 2006 (ADAMS Accession No. ML051810077).

225. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Branch Technical Position (BTP) 7-3, Revision 5, "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service," March 2007 (ADAMS Accession No. ML070550091).

226. Technical Specification Task Force (TSTF) Traveler TSTF-493-A, Revision 4, "Clarify Application of Setpoint Methodology for LSSS Functions," dated January 5, 2010 (ADAMS Accession No. ML100060064).

227. Institute of Electrical and Electronics Engineers, IEEE Std. 828-1998, "IEEE Standard for Software Configuration Management Plans," Piscataway, NJ (Not endorsed by the NRC Staff).

228. Electric Power Research Institute, TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996 (ADAMS Accession No. ML103360462).

229. Invensys/Triconex, "Reliability/Availability Study for the Tricon Version 10 Programmable Logic Controller," Revision 0, 9600164-532, dated May 23, 2007 (Proprietary information. Not publicly available.).

230. Invensys/Triconex, "Tricon v10 Software Qualification Report," Revision 0, 9600164-535, dated August 5, 2009 (Proprietary information. Not publicly available.).

231. Invensys/Triconex, "Critical Digital Review of the Triconex Tricon V10.2.1," Revision 1, 9600164-539, dated August 4, 2009 (Proprietary information. Not publicly available.).

232. U.S. Nuclear Regulatory Commission, NUREG-1431, "Standard Technical Specifications, Westinghouse Plants," Volume 1, "Specifications," and Volume 2, "Bases," April 2012 (ADAMS Accession Nos. ML12100A222 and ML12100A228, respectively).

233. Westinghouse Electric Company LLC, "Advanced Logic System, ALS Security Plan," Revision 3, 6002-00006, May 2014 (Proprietary information. Not publicly available.).

234. U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," January 2010 (ADAMS Accession No. ML090340159).

235. Westinghouse Electric Company LLC, "Pacific Gas & Electric, Diablo Canyon Process Protection System, ALS Subsystem Equipment Qualification Evaluation," Revision 2, 6116-00204, July 2015 (Proprietary information. Not publicly available.).

236. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance," Revision 2, dated June 5, 2009 (ADAMS Accession No. ML091590268).

237. Lingam, S. P., U.S. Nuclear Regulatory Commission, e-mail to Kenneth Schrader, Pacific Gas and Electric Company, "Diablo Canyon 1 and 2 – RAIs for Digital Replacement of the Process Protection System LAR (TAC Nos. ME7522 and ME7523)," dated December 23, 2015 (ADAMS Accession No. ML15357A382).

238. Invensys/Triconex, "Pacific Gas and Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Maximum TSAP Scan Time," Revision 1, 993754-1-817-P, dated April 9, 2012 (Proprietary information. Not publicly available.).

239. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Section 7.8, Revision 5, "Diverse Instrumentation and Control System," March 2007 (ADAMS Accession No. ML070650035).

240. U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Chapter 7, Section 7.9, Revision 5, "Diverse Instrumentation and Control System," March 2007 (ADAMS Accession No. ML070650036).

241. Essig, T., U.S. Nuclear Regulatory Commission, letter to Joseph Naser, Electric Power Research Institute, "Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR-107330, Final Report, 'Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-related Applications in Nuclear Power Plants,'" dated July 30, 1998 (ADAMS Accession No. ML12205A265).

Principal Contributors:

Richard Stattel, NRR/DE/EICB
Samir Darbali, NRR/DE/EICB
Rossnyev Alvarado, NRR/DE/EICB
Victoria Huckabay, NRR/DRA/AFPB

Date: December 21, 2016

LIST OF ACRONYMS

Acronym	**Term**
AC	Alternating Current
ADAMS	Agencywide Document Access and Management System
ALS	Advanced Logic Systems
AMSAC	ATWS Mitigating System Actuation Circuitry
ANS	American Nuclear Society
AR PK	Alarm Response Panel Key
ASU	ALS Service Unit
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CAPAL	Corrective Action, Prevention and Learning
CCF	Common Cause Failure
CFR	*Code of Federal Regulations*
COMBUS	Communications Bus
COT	Channel Operational Test
CSA	Configuration Status Accounting
CSI	CS Innovations
D3	Diversity and Defense-in-Depth
DC	Direct Current
DCM	Design Criteria Memorandum
DCPP	Diablo Canyon Power Plant
DI&C	Digital Instrumentation and Controls
DPRAM	Dual-Port Random Access Memory
DTT	De-energize To Trip
EDM	Engineering Department Manual
EIA	Electronics Industries Association
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EOP	Emergency Operating Procedure
EPRI	Electric Power Research Institute
EQ	Equipment Qualification
ESFAS	Engineered Safety Features Actuation System
ETP	External Termination Panel
ETT	Energize To Trip
FAT	Factory Acceptance Test
FBD	Function Block Diagram
FMEA	Failure Modes and Effects Analysis
FPGA	Field-Programmable Gate Array
FRS	Functional Requirement Specification
FSARU	Final Safety Analysis Report Update
GDC	General Design Criterion/Criteria
GHz	GigaHertz
HICRc	Highly-Integrated Control Rooms – Communications Issues
HSI	Human-System Interface
HTML	Hyper Text Markup Language
Hz	Hertz

Acronym	**Term**
I&C	Instrumentation and Control
I/O	Input and Output
ICN	Interim Change Notice
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IN	Information Notice
IOCCOM	Combined Input Output Communications and Com Processor
IOM	Invensys Operations Management (Tricon V10 vendor)
IP	Internet Protocol
IRS	Interface Requirement Specification
ISA	Instrument Society of America
ISG	Interim Staff Guidance
IV&V	Independent Verification and Validation
KHz	KiloHertz
krad	Kilorad
KVM	Keyboard-Video-Mouse (peripheral device).
LAR	License Amendment Request
LCO	Limiting Condition for Operation
LSM	Line Sense Module
LSSS	Limiting Safety System Setting
LWR	Light-Water Reactor
mA	Milliampere
MHz	MegaHertz
MIL-STD	Military Standard
ms	Millisecond
MWS	Maintenance Work Station
NGAI	Next Generation Analog Input
NGDO	Next Generation Digital Output
NRC	U.S. Nuclear Regulatory Commission
NSR	Non-Safety-Related
NVM	Non-Volatile Memory
OBE	Operating Basis Earthquake
OP	Operating Procedure
OPDT	Over Power Delta Temperature
OTDT	Over Temperature Delta Temperature
PAN	Product Alert Notice
PDN	Packet Data Network
PDS	Predeveloped Software
PG&E	Pacific Gas and Electric Company (the licensee)
PHA	Preliminary Hazard Analysis
PLC	Programmable Logic Controller
PMP	Project Management Plan
PPM	Project Procedures Manual
PPS	Process Protection System
PSAI	Plant-Specific Action Item
PTM	Project Traceability Matrix

Acronym	**Term**
QAM	Quality Assurance Manual
QAP	Quality Assurance Plan
QPM	Quality Procedures Manual
RAB	Reliable ALS Bus
RAI	Request for Additional Information
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RFI	Radio-Frequency Interference
RG	Regulatory Guide
RH	Relative Humidity
RIS	Regulatory Issuance Summary
RMS	Root Mean Squared
RPS	Reactor Protection System
RS	Recommended Standard (Used for identifying communications protocols such as RS-422, and RS-485)
RSA	Rivest Shamir Adleman
RTD	Resistance Temperature Detector
RTM	Requirements Traceability Matrix
RTS	Reactor Trip System
RXM	Remote Extender Module
SCMP	Software Configuration Management Plan
SDD	Software Design Description
SDOE	Secure Development and Operational Environment
SDP	Software Development Plan
SDS	Software Design Specification
SIDR	System Integration Deficiency Report
SIL	Software Integrity Level
SIntP	Software Integration Plan
SMP	Software Management Plan
SQAP	Software Quality Assurance Plan
SR	Safety-Related
SRD	Software Release Definition
SRP	Standard Review Plan
SRS	Software Requirements Specification
SSE	Safe Shutdown Earthquake
SSP	Software Safety Plan
SSPS	Solid State Protection System
Std.	Standard
STP	Software Test Plan
STS	Standard Technical Specifications
SVTP	Software Verification Test Plan
SVVP	Software Verification and Validation Plan
SyQAP	System Quality Assurance
SyVVP	System Verification and Validation Plan
TAB	Test ALS Bus
T_{ave}	Average Reactor Coolant Temperature
TCM	Tricon Communication Module

Acronym	**Term**
TFS	Transfer Functions Design Input Specification
TMI	Three Mile Island
TMR	Triple Modular Redundant or Triple Mode Redundancy
TR	Technical Report
TS	Technical Specification
TSAP	Test System Application Program
TSTF	Technical Specification Task Force
TTD	Trip Time Delay
USB	Universal Serial Bus
UV	Undervoltage
V	Volt
V&V	Verification and Validation
VAC	Volts Alternating Current
VDC	Volts Direct Current
VTP	Validation Test Plan
VTS	Validation Test Specification
WEC	Westinghouse Electric Company

The NRC staff has determined that the related safety evaluation contains proprietary information pursuant to Title 10 of the *Code of Federal Regulations* Section 2.390. The proprietary version of the safety evaluation is provided in Enclosure 3. Accordingly, the NRC staff has also prepared a non-proprietary version of the safety evaluation, which is provided in Enclosure 4.

The Notice of Issuance will be included in the Commission's next regular biweekly *Federal Register* notice.

Sincerely,

/RA/

Balwant K. Singal, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

Enclosures:
1. Amendment No. 227 to DPR-80
2. Amendment No. 229 to DPR-82
3. Safety Evaluation (proprietary)
4. Safety Evaluation (non-proprietary)

cc w/o Enclosure 3: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL4 Reading
RidsACRS_MailCTR Resource
RidsNrrDeEicb Resource
RidsNrrDorlLpl4 Resource
RidsNrrDraAphb Resource
RidsNrrDssSrxb Resource
RidsNrrDssStsb Resource
RidsNrrLAJBurkhardt Resource
RidsNrrPMDiabloCanyon Resource
RidsRgn4MailCenter Resource
RStattel, NRR/DE/EICB
SDarbali, NRR/DE/EICB
RAlvarado, NRR/DE/EICB
JWhitman, NRR/DSS/SRXB
CTilton, NRR/DSS/STSB
VHuckabay, NRR/DRA/APHB

ADAMS Accession No. ML16134A320 (Proprietary); ML16139A008 (Non-proprietary) *via email

OFFICE	NRR/DORL/LPL4-1/PM	NRR/DORL/LPL4-1/LA	NRR/DE/EICB/BC*	NRR/DSS/STSB/BC*	NRR/DRA/APHB/BC*
NAME	BSingal	JBurkhardt	MWaters	AKlein	SWeerakkody
DATE	9/23/16	9/23/16	10/14/16	10/6/16	10/6/16
OFFICE	NRR/DSS/SRXB/BC*	OGC – NLO*	NRR/DORL/LPL4/BC	NRR/DORL/LPL4/PM	
NAME	EOesterle	DRoth	RPascarelli	BSingal	
DATE	10/13/16	11/2/16	12/21/16	12/21/16	

OFFICIAL RECORD COPY