Pacific Gas and Electric Company®

Barry S. Allen
Vice President, Nuclear Services

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

805.545.4888
Internal: 691.4888
Fax: 805.545.6445

June 22, 2015

PG&E Letter DCL-15-072

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

10 CFR 50.90

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

References:
1. PG&E Letter DCL-11-104, "License Amendment Request 11-07, Process Protection System Replacement," dated October 26, 2011 (ADAMS Accession No. ML11307A331)
2. PG&E Letter DCL-13-043, "Supplement to License Amendment Request 11-07, "Process Protection System Replacement," dated April 30, 2013 (ADAMS Accession No. ML13121A089)
3. PG&E Letter DCL-14-036, "Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement," dated April 30, 2014 (ADAMS Accession No. ML14121A002)

Dear Commissioners and Staff:

In Reference 1, Pacific Gas and Electric Company (PG&E) submitted License Amendment Request (LAR) 11-07 to request NRC Staff (Staff) approval to replace the Diablo Canyon Power Plant Eagle 21 digital process protection system (PPS) with a new digital PPS that is based on the Invensys Operations Management Tricon Programmable Logic Controller, Version 10, and the CS Innovations, LLC (a Westinghouse Electric Company), Advanced Logic System (ALS). In Reference 2, PG&E submitted a supplement to LAR 11-07.

This letter contains revisions to Reference 2. The revisions are due to changes to the PPS replacement design that have occurred and to provide additional clarification in several sections.

In Reference 3, PG&E provided to the response to the ALS plant-specific action items (PSAIs), except for PSAIs number 4, 5, 6, 8, 10, 20, and 22. This letter provides the

response to PSAIs number 4, 5, 6, 8, 10, 20, and 22. These responses address commitment number 4 contained in Attachment 1 to the Enclosure of Reference 3 to submit a response to ALS PSAIs number 4, 5, 6, 8, 10, 20, and 22.

This information does not affect the results of the technical evaluation or the significant hazards consideration determination previously transmitted in Reference 2.
In Reference 2, PG&E requested approval of the license amendments for Reference 1 by July 2014 and that they be made effective upon NRC issuance, to be implemented prior to entry into Mode 4 following completion of the Unit 1 Nineteenth Refueling Outage and the Unit 2 Nineteenth Refueling Outage. The Technical Specification (TS) 1.1 change proposed in Attachment 3 to the Enclosure of Reference 2 applies to both the current Eagle 21 process protection system and the proposed Tricon/Advanced Logic System process protection system upon installation, allowing the proposed TS 1.1 change to be implemented upon NRC approval. Therefore, PG&E requests approval of the license amendments for Reference 1 by December 2015 and that they be made effective upon NRC issuance, to be implemented within 120 days. These requested approval and implementation dates supersede those previously requested in Reference 2.

If you have any questions, or require additional information, please contact Mr. Philippe Soenen at (805) 545-6984.

This communication contains regulatory commitments (as defined by NEI 99 04). The commitments are contained in Attachment 1 to the enclosure.

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

Executed on June 22, 2015.

Sincerely,

Barry S. Allen
Vice President, Nuclear Services

kjse/4328/50271918
Enclosure
cc: Diablo Distribution
cc/enc: Marc L. Dapas, NRC Region IV
Thomas R. Hipschman, NRC Senior Resident Inspector
Siva P. Lingam, NRR Project Manager
Gonzalo L. Perez, Branch Chief, California Department of Public Health

Revisions to Supplement for License Amendment Request 11-07, "Process Protection System Replacement"

Pacific Gas and Electric Company (PG&E) Letter DCL-11-104, "License Amendment Request 11-07, Process Protection System Replacement," dated October 26, 2011, submitted License Amendment Request (LAR) 11-07 to request NRC Staff (Staff) approval to replace the Diablo Canyon Power Plant (DCPP) Eagle 21 digital process protection system (PPS) with a new digital PPS that is based on the Invensys Operations Management Tricon Programmable Logic Controller, Version 10, and the CS Innovations, LLC (CS Innovations) (a Westinghouse Electric Company), Field Programmable Gate Array (FPGA) based Advanced Logic System (ALS). PG&E submitted a supplement to LAR 11-07 in PG&E Letter DCL-13-043 on April 30, 2013.

This letter contains revisions to the supplement to LAR 11-07 (referred to as DCL-13-043 hereafter) due to PPS Replacement design changes that have occurred and to provide additional clarification to several sections. The DCL-13-043 section number, page number, change, and basis for change are provided.

Section 4.2.5.2, ALS Voting

The paragraph (DCL-13-043 Enclosure page 64)

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

is revised to

"The diverse "A" and "B" execution path outputs are combined in hardwired logic as shown in Figure 4-9 to ensure that the protective action is taken if directed by either path. A single failed path cannot prevent a protective action. If either ALS-102 CLB card identifies itself as failed, it enters the HALT mode and terminates RAB communication. The associated ALS-402 DO card then detects a double RAB timeout and sets its outputs to fail-safe state. If a ALS-402 DO card identifies itself as failed, it enters the HALT mode and its outputs fail as-is unless the fault condition that generated the failure prevents them from doing so."

Basis for Change

This revision is made to reflect the ALS platform functionality with regard to HALT mode implementation for the ALS-402 digital outputs, which is a fail as-is state versus a fail-safe state.

Section 4.2.13.2, FPGA-Based ALS Equipment Communications

The sentence (DCL-13-043 Enclosure page 89) "The ALS-102B broadcasts data via communications channel TxB1 to the nonsafety-related Gateway, which is common to all four Protection Sets" is revised to "The ALS-102 broadcasts data via communications channel TxB1 to the nonsafety-related Gateway, which is common to all four Protection Sets."

Basis for Change

There is both an A and a B chassis with an ALS-102 board, therefore the word "ALS-102B" is revised to "ALS-102" since either chassis will transmit TxB1 data to the Gateway Server and it is not a B chassis core function only.

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

The sentence (DCL-13-043 Enclosure page 91)

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

is being revised to

"The Tricon MWS is being designed to implement five application programs: (1) Invensys WonderWare™ InTouch™ PPS application; (2) Trilogger; (3) Tricon Diagnostic Monitor; (4) Startup Delayer Application; and (5) TriStation 1131 (TS1131) Developers Workbench."

Basis for Change

The Windows XP operating system is no longer supported by Microsoft. The software to be used on the Tricon MWS does not need to be specified in the LAR since it is not part of the safety-related function of the PPS. The software used is contained in the vendor project specific documents.

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

The sentence (DCL-13-043 Enclosure page 94)

"The diversity design of the ALS enables either (but not both) Chassis "A" or Chassis "B" in a protection set to be bypassed for maintenance or testing while the other

chassis remains fully operational (although, in the bypassed condition, certain post-accident monitoring functions may not be available and need to be controlled administratively)."

is revised to

"The diversity design of the ALS enables one Chassis in a protection set to be bypassed for maintenance or testing while the other chassis remains fully operational (although, in the bypassed condition, certain post-accident monitoring functions may not be available and need to be controlled administratively)."

Basis for Change

Both the ALS Chassis "A" or Chassis "B" in a protection set can be bypassed at the same time and this will be performed during the refueling outages when the ALS is not required to be TS operable. Due to the nature of the ALS TAB wiring, only one chassis TAB can be connected at any time, therefore, only one chassis can have maintenance or testing in progress and the other chassis will remain fully functional.

The sentence (DCL-13-043 Enclosure page 95)

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

is revised to

"The ALS MWS uses the ALS Service Unit (ASU) that is described in Section 2.6.3 of the ALS Topical Report [15]. The ALS subsystem of the DCPP PPS replacement does not use a keyswitch to enable and disable external TAB communications as described in the ALS Topical Report. The TAB communications require a physical connect/disconnect other than a keyswitch (i.e., manual disconnect/connect at the connector)."

Basis for Change

The Windows XP operating system is no longer supported by Microsoft. The software to be used does not need to be specified in the LAR since it is not part of the safety-related function of the PPS. The software used is contained in the vendor project specific documents.

The ALS subsystem of the DCPP PPS replacement does not use a keyswitch to enable and disable external TAB communications. This information is added to Section 4.2.13.5 for clarification consistent with other LAR sections.

The sentence (DCL-13-043 Enclosure page 96)

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

is revised to

"The ASU application developed for the MWS, provided by PG&E, provides graphical user interfaces for displaying ALS system status on the MWS and for providing user controlled access to the ALS controllers for performing maintenance operations such as calibration."

Basis for Change

The ASU application software basis is not part of the safety-related function of the PPS and therefore does not need to be specified in the LAR. The software package used is documented in the vendor project specific documents.

The sentence (DCL-13-043 Enclosure page 96)

"These dedicated MWS serial ports receive ALS system status at a rate of 10Hz (i.e., once every 100 ms)." is deleted.

Basis for Change

The ports are expected to operate at 500 msec, however, this is not a required system response. The use of a status rate of 500 msec has been specified by the vendor and does not affect any safety related function and will not prevent an operator from viewing available data (too fast for human response). Therefore, the sentence is not required and is deleted.

The paragraph (DCL-13-043 Enclosure page 96)

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

records the ALS system status in a data class which contains methods that are called by different GUI to extract and display the specific ALS system status."

is revised to

"Upon establishing the dedicated serial port connection on the MWS, the ASU periodically spawns a software thread to receive, validate, and store the data received from the respective ALS-102 TxB2 communication link. Validation of the received data consists of checking the packet header contents, TxB2 Chassis ID, packet trailer performing a CRC check on the packet contents, and then comparing the calculated CRC with the CRC inside the TxB2 packet. If the data received by the parameter display application is invalid (i.e. invalid CRC), the ASU will first attempt to re-sync which will be transparent to the operator. If the ASU cannot re-sync, it will indicate as such via the TxB2 status indicator and all other status indications and data fields (fed by the TxB2) will go to their unknown/offline state. If the data received by the parameter display application is valid, the application records the data which can be accessed via methods that are called by different Graphical User Interface (GUI) to extract and display the specific ALS system status."

Basis for Change

The change provides additional detail on operation of the current ASU software based on input from the vendor.

Section 4.2.14, KVM Switch

The sentence (DCL-13-043 Enclosure page 98)

"An AV4PRO-VGA KVM switch is being specified for the PPS replacement. This KVM switch has ports for four computers (VGA video port, USB port, and audio port for each computer), a user console with a VGA video port, a USB keyboard port, and a USB mouse port), a user console with two switched USB ports (one for touchscreen and one for printer), and an options port." is deleted.

The paragraphs (DCL-13-043 Enclosure page 99)

"In addition Section 2.3.7of the IRS [29] states the AV4PRO-VGA KVM switch shall utilize the default switching mode, in which the video display, keyboard and mouse and the enumerated USB ports are all switched simultaneously. This specification prevents the enumerated ports from being switched separately from the KVM. The user console's two switched USB ports, which use enumerated switching, pass data straight through the KVM switch without interpretation. With operation of the KVM switch utilizing the default switching mode, if a keyboard is connected to the USB1 or USB2 port, the hotkeys cannot be used to perform switching, and USB1 and USB2 traffic cannot cause an inadvertent switch. The keyboard and mouse are

being designed to use the emulated switching function, not the enumerated switching function, and thus only the keyboard, mouse, and the button on the KVM switch can control the switch. A user console switched USB port is being used by the local printer for each protection set.

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

are revised to

"In addition Section 2.3.7of the IRS [29] provides specifications for the operation of a KVM switch in association with the MWS. The unused MWS and KVM switch ports will be addressed in accordance with the DCPP CSP [48]."

Basis for Change (pages 98 and 99)

The model and vendor of the KVM switch will be chosen during the PPS replacement design change implementation and may need to be changed due to obsolescence of the model specified in the supplement to LAR 11-07. The KVM switch is not a safety-related device. The required functions of the KVM switch are specified in Section 2.3.7.1 of the PPS Replacement Interface Requirements Specification, which states the KVM switch shall permit only connections between a single computer and the selected video display and peripheral devices. The unused KVM switch ports will be addressed in accordance with the DCPP Cyber Security Plan, as previously stated on page 99 of the Enclosure of PG&E Letter DCL-13-043. The KVM switch configuration is controlled under the PG&E document SCM 36-01, "Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Software Configuration Management Plan (SCMP)" that provides a process of change control and for software configuration management for the PPS replacement components.

<u>Section 4.5.6.1, PG&E</u>

The sentence (DCL-13-043 Enclosure page 108)

"The PG&E SCMP [159] has been developed to establish and document a process of change control and software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test

Facility and for the remainder of its life cycle following installation at DCPP, including the Operation Phase and Maintenance Phase."

is revised to

"The PG&E SCMP [159] has been developed to establish and document a process of change control and software configuration management for the PPS replacement from the time the equipment arrives at the PG&E Test Facility and for the remainder of its life cycle following installation at DCPP, including the Operation Phase and Maintenance Phase."

Basis for Change

The test facility to be used for Site Acceptance Testing may or may not be located offsite from the DCPP facility. The "Test Facility," regardless of location, needs to have associated procedural controls to ensure a safe environment (SDOE). Therefore, the use of the term "Test Facility" is more appropriate and is used.

Section 4.5.7.1, PG&E

The sentence (DCL-13-043 Enclosure page 110)

"PG&E document SCM 36-01, "Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Software Configuration Management Plan (SCMP)" [159] has been developed using DCPP Procedure CF2.1D2 to establish and document a process of change control and for software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility and for the remainder of its life cycle following installation at DCPP."

is revised to

"PG&E document SCM 36-01, "Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Software Configuration Management Plan (SCMP)" [159] has been developed using DCPP Procedure CF2.1D2 to establish and document a process of change control and for software configuration management for the PPS replacement from the time the equipment arrives at the PG&E Test Facility and for the remainder of its life cycle following installation at DCPP."

Basis for Change

The test facility to be used for Site Acceptance Testing may or may not be located offsite from the DCPP facility. The "Test Facility", regardless of location, needs to have associated procedural SCMP. Therefore, the use of the term "Test Facility" is more appropriate and is used.

Section 4.7, Defense-in-Depth & Diversity

The sentence (DCL-13-043 Enclosure page 118)

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

is revised to

"Concern for ALS software CCF is addressed through incorporating additional design diversity in the FPGA-based hardware system as described in Section 4.2.5.2 to develop and implement the hardware."

Basis for Change

The reference to LAR Section 4.1.1 for the discussion of ALS diversity should be Section 4.2.5.2. The reference to use of qualified design practices and methodologies to develop the hardware is removed since these are not significant contributors to the diversity of the ALS subsystem.

Section 4.8.3, ISG-04 Interdivisional Communications Staff Position No. 3

The sentence (DCL-13-043 Enclosure page 123)

"Activation of the TAB access is alarmed both locally and in the control room."

is revised to

"Activation of the TAB access is alarmed in the control room."

Basis for Change

The ALS will not utilize a local audible alarm, instead a local Light Emitting Diode indication on the ALS-102 digital input board provides the status indication. This change provides consistency with other LAR sections.

Section 4.8.8, ISG-04 Interdivisional Communications Staff Position No. 8

The sentence (DCL-13-043 Enclosure page 129)

"To enable the TAB to the interface to the MWS requires the setting of a hardware key-lock switch which, when enabled, is alarmed locally and in the control room."

is revised to

"To enable the TAB to the interface of the MWS requires physically connecting the TAB data link which, when connected, is alarmed in the control room."

Basis for Change

The words "physically connecting" are used elsewhere in the LAR. The ALS subsystem of the DCPP PPS replacement does not use a keyswitch to enable and disable external TAB communications. The ALS will not utilize a local audible alarm, instead a local Light Emitting Diode indication on the ALS-102 digital input board provides the status indication. These changes provide consistency with other LAR sections.

Section 4.8.10, ISG-04 Interdivisional Communications Staff Position No. 10

The sentence (DCL-13-043 Enclosure page 144)

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

is revised to

"Changes to process values contained in ALS NVM and the calibration of ALS analog inputs and outputs are possible only when the TAB data link is physically connected and the TAB Enable DI is activated."

Basis for Change

The ALS subsystem used for the DCPP PPS replacement does not detect a data link but instead detects if the TAB Enable DI has gone true. The DI value is used by the ASU to allow access to displays that can change parameters. The ALS subsystem ALS-102 board used for the DCPP PPS replacement will not contain logic that blocks a safety channel bypass from occurring if the TAB is not enabled. Instead there is logic to prevent a virtual channel from going to VCB (OOS) if the associated ALS-402 channel is not in DOO. The ALS subsystem continues to meet ISG-04 Interdivisional Communications Staff Position No. 10 with this change because changes to process values contained in ALS nonvolatile memory (NVM) and the calibration of ALS analog inputs and outputs are possible only when the TAB data link is physically connected and the TAB Enable DI is activated.

The paragraph (DCL-13-043 Enclosure page 144)

"The ALS Reliability and FMEA document for the PPS replacement is CS Innovations Document 6116-00029, Revision 1, "Diablo Canyon PPS ALS Reliability

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

Basis for Change

The ALS subsystem of the DCPP PPS replacement does not use a keyswitch to enable and disable external TAB communications. Therefore, the text related to the keyswitch failing is not needed. The control of the TAB data link is controlled through plant administrative procedure requirements.

The sentence (DCL-13-043 Enclosure page 145)

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

is deleted and replaced with the new paragraph

"Replacement of a faulted board requires PG&E to load the associated NVM image to a spare board using the ALS Test and Configuration Tool (ATCT) tool described in PPS Project Document 6116-00011. This tool is an external device that is unable to be connected to the installed plant system. ALS subsystem board NVM images will be controlled by the PG&E SCMP. Use of the ATCT tool will be performed in accordance with approved plant procedures and the NVM image will be validated by post-maintenance testing."

This change impacts the Commitment 11 contained in Attachment 1 to the Enclosure of PG&E Letter DCL-13-043, dated April 30, 2013. The revised commitment is contained in Attachment 1 to the Enclosure.

Basis for Change

The previous paragraph in DCL-13-043 states that PG&E will not possess the hardware and software tools required to reprogram the FPGA logic and that the ALS safety application logic changes must be performed by Westinghouse. The previous paragraph in DCL-13-043 also states the ALS-102 Core Logic Board (CLB) must be removed from the ALS chassis in order to change the FPGA safety application logic. Changes to the FPGA safety application logic require the board to be removed from the chassis and installed in an external device. The external device cannot be connected to the plant chassis. Since PG&E is not capable of changing the ALS safety application or FPGA programming and changes to the FPGA safety application logic cannot be made to the ALS CLB when it is installed in the chassis,

the sentence regarding modification of ALS FPGA application logic using approved DCPP procedures is unnecessary and is removed.

If a faulted ALS CLB needs to be replaced, PG&E will need to perform an initial configuration of the Westinghouse supplied spare CLB for the specific protection set. The configuration parameters are stored in NVM. The configuration is performed using the Westinghouse supplied ATCT tool, documented in Section 4.5 of the ALS subsystem Project Document 6116-00011, "ALS Spares Programming System," and the Westinghouse supplied unique NVM images for each board in every protection set. It is noted that the ATCT is not capable of downloading FPGA images. Use of the ATCT tool to place the required NVM image on the spare board is performed completely external to the installed plant system and will be in accordance with approved plant procedures. Once the NVM image is downloaded to the spare board, then the faulted board can be removed from the plant chassis and the new spare board installed. After the new spare board is installed, verifications of the NVM parameters and post-maintenance testing would need to be performed in accordance with approved plant procedures prior to declaring the chassis operable. A summary of this information is added in the new paragraph.

The sentence (DCL-13-043 Enclosure page 145)

"Certain ALS data parameters can be modified during plant operation (with the subject instrument channel in bypass mode) or while the plant is shutdown."

is revised to

"Certain ALS data parameters can be modified during plant operation or plant shutdown (with the subject instrument channel OOS)."

Basis for Change

An instrument Channel can be in Test-in-Bypass, Test-in-Trip, Manual Trip, or Bypass and still be able to modify plant parameters. It is necessary to have the Instrument Channel OOS (which requires Test-in-Trip or Test-in-Bypass on the ALS) in order to make any changes, whether operating or shutdown during any of these states. Therefore the use of term OOS is more complete than the term bypass mode.

<u>Section 4.8.11, ISG-04 Interdivisional Communications Staff Position No. 11</u>

The sentence (DCL-13-043 Enclosure page 147)

"Activation of the TAB access is alarmed both locally and in the control room."

is revised to

"Activation of the TAB access is alarmed in the control room."

Basis for Change

The ALS will not utilize a local audible alarm, instead a local Light Emitting Diode indication on the ALS-102 digital input board provides the status indication. This change provides consistency with other LAR sections.

The sentence (DCL-13-043 Enclosure page 147)

"Changes to process values contained in ALS NVM memory and the calibration of ALS analog inputs and outputs can only be performed when the TAB data link is physically connected and when the ALS detects that the TAB data link has been connected to the MWS."

is revised to

"Changes to process values contained in ALS NVM memory and the calibration of ALS analog inputs and outputs can only be performed when the TAB data link is physically connected to the MWS and the Enable DI is active."

Basis for Change

The ALS subsystem used for the DCPP PPS replacement will not employ the capability to detect that the TAB data link has been connected to the MWS. This capability is not required to meet ISG-04 Interdivisional Communications Staff Positions No. 11 because the ALS processors, in different Protection Sets, cannot communicate with processors in other Protection Sets.

The sentence (DCL-13-043 Enclosure page 147)

"The ALS-102 Core Logic Board (CLB) contains logic that blocks safety channel bypasses from occurring if the TAB is not enabled" is deleted.

Basis for Change

The ALS subsystem used for the DCPP PPS replacement will not employ this capability. This capability is not required to meet ISG-04 Interdivisional Communications Staff Positions No. 11 because the ALS processors in different Protection Sets cannot communicate with processors in other Protection Sets. The ALS-102 board logic is designed such that a virtual channel (ALS-102 channel) will not go to virtual channel bypass – OOS) unless the associated ALS-402 Solid State Protection System digital output channel is in the digital output override status (i.e., Test-in-Bypass or Test-in-Trip is established).

The sentence (DCL-13-043 Enclosure page 147)

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

Basis for Change

The ALS subsystem used for the DCPP PPS replacement will not employ this capability. This capability is not required to meet ISG-04 Interdivisional Communications Staff Positions No. 10 or 11. The ALS subsystem continues to meet ISG-04 Interdivisional Communications Staff Position No. 10 because changes to process values contained in ALS NVM, and the calibration of ALS analog inputs and outputs, are possible only when the TAB data link is physically connected and the TAB Enable DI is activated. The ALS subsystem continues to meet ISG-04 Interdivisional Communications Staff Position No. 11 because the ALS processors in different Protection Sets cannot communicate with processors in other Protection Sets.

The sentences (DCL-13-043 Enclosure page 148)

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

are revised to

"To enable the TAB interface of the MWS requires physically connecting the TAB data link which, when connected, is alarmed in the control room. The ALS-102 generates a Trouble Alarm to alert operations that the TAB data link between the ALS MWS and the ALS chassis is connected."

Basis for Change

The ALS subsystem used for the DCPP PPS replacement will not employ the capability to generate an ALS Communications Enable alarm status signal when the ALS chassis is enabled; instead it will generate a Trouble Alarm when the TAB data link between the ALS MWS and the ALS chassis is physically connected and the pins are made up to the digital input. The capability to generate an ALS

Communications Enable alarm status signal when the ALS chassis is enabled is not required to meet ISG-04 Interdivisional Communications Staff Positions No. 11 because the ALS processors in different Protection Sets cannot communicate with processors in other Protection Sets.

Section 4.10.3.7 Clause 6.7 Maintenance Bypass

The sentence (DCL-13-043 Enclosure page 197)

"Manual bypass switches are provided for each comparator output in the ALS as described in ALS System Design Specification [19], Section 3.3.4.2."

is revised to

"Manual bypass switches are provided by PG&E for each comparator output in the ALS as described in ALS System Design Specification [19]."

Basis for Change

It is added that PG&E is providing the manual bypass switches to clarify they are not provided by the vendor. The Project Document 6116-00011 (Reference 19 of DCL-13-043) has been revised and Section 3.3.4.2 no longer exists; therefore, the reference to the Section number is removed.

Section 4.11.1.3.2 Clause 5.5.2 Design for Test and Calibration

The sentence (DCL-13-043 Enclosure page 222)

"The ALS provides test and calibration capability as described in Section 2.3.2 and Section 3 of the ALS Topical Report Submittal [15] and Sections 10.2 and 10.3 of the ALS System Design Specification [19]."

is revised to

"The ALS provides test and calibration capability as described in Section 2.3.2 and Section 3 of the ALS Topical Report Submittal [15] and Section 7 of the ALS System Design Specification [19]."

Basis for Change

The Project Document 6116-00011 (Reference 19 of DCL-13-043), has been revised and the reference to Sections 10.2 and 10.3 are no longer applicable for test and calibration capability. Therefore, the reference to the Section numbers is removed.

Section 4.12.1 TS 1.1 COT Definition Revision

The paragraph (DCL-13-043 Enclosure page 236)

"The ALS-311 input board BIST operation begins with providing a single dedicated multichannel ADC for each input for the purpose of measuring the field input signal and for sampling the onboard diagnostic signal references. Document 6002-31102, "ALS-311 Design Specification," Section 3.5, provides an example configuration and ADC channel assignment for an ALS-311 input board configured with an RTD input. In normal operation, the ADC will perform the sample loop. Disabled channels will not sample data, nor perform self-test functions. If an input fails the integrity BIST, this is reported via the integrity status bit located in the CSI20 message packet for analog boards, or in the integrity monitor register for digital I/O boards. In the ALS used for the DCPP PPS replacement subsystem, any integrity BIST failure is alarmed at the system level and provided to the MAS. The ALS-321 input board BIST is the same as for the ALS-311 input board."

is supplemented by the following

"The available ALS diagnostic programs and self-test capabilities provide for an onboard high and low reference signal to be periodically injected in the channel and therefore, allows the performance of the COT without injection of an external simulated or actual signal into the channel. Injection of an external simulated or actual signal is not required for the ALS-311 and ALS-321 boards as part of the COT."

Basis for Change

The current text does not make it clear that the ALS diagnostic programs and self-test capabilities are relied upon to meet the COT definition "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" and that no injection of an external simulated or actual signal into the channel is required during the surveillance to meet the proposed TS COT definition.

Section 4.13 Secure Development and Operational Environment

The sentence (DCL-13-043 Enclosure page 245)

"The offsite testing facility will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to be turned over to operations, per Section 3.1.5 of the security plan."

is revised to

"The testing facility will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to be turned over to operations, per Section 3.1.5 of the security plan."

This change impacts the Commitment 18 contained in Attachment 1 to the Enclosure of PG&E Letter DCL-13-043, dated April 30, 2013. The revised commitment is contained in Attachment 1 to the Enclosure.

Basis for Change

The test facility to be used for testing may or may not be located offsite from the DCPP facility. The testing, regardless of location, will be visited by the CSAT. Therefore, the use of the term "testing facility" is more appropriate.

Section 4.14 Tricon V10 Safety Evaluation Application Specific Action Items

The sentence (DCL-13-043 Enclosure page 248)

"The PG&E SCMP [159] has been developed to establish and document a process of change control and for software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility and for the remainder of its life cycle following installation at DCPP."

is revised to

"The PG&E SCMP [159] has been developed to establish and document a process of change control and for software configuration management for the PPS replacement from the time the equipment arrives at the PG&E Test Facility and for the remainder of its life cycle following installation at DCPP."

Basis for Change

The test facility to be used for testing may or may not be located offsite from the DCPP facility. Therefore, the use of the term "PG&E Test Facility" is more appropriate.

Section 4.15.1, Detailed Description of FAT and SAT for PPS Replacement Design

The sentence (DCL-13-043 Enclosure page 261)

"When the TAB is enabled, an alarm is activated locally and in the main control room."

is revised to

"When the TAB data link is physically connected, an alarm is activated in the main control room."

Basis for Change

The ALS will not utilize a local alarm, instead a local Light Emitting Diode indication on the ALS-102 digital input board provides the status indication. This change provides consistency with other LAR sections.

The paragraph (DCL-13-043 Enclosure pages 260)

"The ALS communications with its dedicated MWS are via the unidirectional TXB2 communication links from the ALS-102 board. The TXB2 communication links are electrically isolated at the ALS-102. Unidirectional communications provides functional isolation from the MWS. The unidirectional nature of the links will be verified at the FAT."

The last sentence, "The unidirectional nature of the links will be verified at the FAT," is deleted.

The related sentences describing the ALS subsystem FAT (on page 263 of the DCL-13-043 Enclosure) contained in Item 2 "The test will verify no inbound communications via the TXB1 channel to either ALS-102 "A" or "B"." and in Item 3 "The test will verify no inbound communications via the TXB2 channel to either ALS-102 "A" or "B"." are also deleted.

Basis for Change

The ALS-102 board connection is hardwired to not provide a receive wire. There is no testing that can be devised to prove unidirectional flow of data. Data received at the MWS is being verified.

The ALS platform design requirement document, 6002-10202, Revision 3, Item D017 requirement is that receive capability is physically disabled by hardware. The receiver is configured such that the transmit data is looped back for channel integrity testing. The communication channel shall be configured for unidirectional (transmit only) EIA-422 communication. Bidirectional communication shall be disabled in hardware. Page 98 of the Enclosure of DCL-13-043 states that the design, in effect, is the same as the data isolation that is achieved by a "broken wire."

Due to the hardware nature of this configuration, an attempt to inject/transmit data on the receive lines of the ALS will result in either a channel integrity error (incoming data does not match outgoing data) or possibly could result in damage to the board. The transmit lines of the serial card in the MWS are not physically connected to anything.

PG&E is unable to physically modify or configure the ALS-102 board to enable bidirectional communications and the MWS/ASU "TAB" functions access only the TAB serial port and are not configured via hardware to use the TxB2 serial port.

Therefore, there is no need to verify the unidirectional nature of the TXB2 communication links during the ALS FAT.

The sentence (DCL-13-043 Enclosure page 263)

"4. The ALS FAT configuration will include the MWS provided by PG&E, KVM switch, printer, KVM and media converters."

is revised to

"4. The ALS FAT configuration will include the MWS provided by PG&E."

This change impacts Commitment 25 contained in Attachment 1 to the Enclosure of PG&E Letter DCL-13-043, dated April 30, 2013 (Reference 2). The revised commitment is contained in Attachment 1 to the Enclosure.

Basis for Change

These components do not have an impact on the ALS subsystem. The testing of the PPS replacement KVM switch and media converters was performed as part of the Tricon FAT and will be performed as part of the SAT, as previously stated on page 264 of Attachment 1 to the Enclosure of PG&E Letter DCL-13-043. Additional testing of the KVM and media converters during the ALS FAT is not necessary. The printer is being removed from the PPS replacement design as discussed in the subsection titled "Removal of Printer from ALS MWS and Tricon MWS" below.

The paragraph (DCL-13-043 Enclosure pages 263 and 264)

"5. Bidirectional EIA-485 TAB communication between ALS Chassis "A" and Chassis "B" and ASU software running on the ALS MWS can take place only if the communication links are physically connected and enabled. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected and enabled."

is revised to

"5. Bidirectional EIA-485 TAB communication between ALS Chassis "A" and Chassis "B" and ASU software running on the ALS MWS can take place only if the communication links are physically connected which enables the DI. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected."

Basis for Change

The ALS subsystem used for the DCPP PPS replacement does not detect that a communication link is "enabled" but instead detects if the TAB Enable DI has gone true. The DI value is used by the ASU to allow access to displays that can change parameters. TAB communication between the MWS and the ALS is possible only when the TAB communication link between the ALS chassis and the MWS is physically connected. Therefore, there is no need for a test requirement associated with a communication link being "enabled."

Removal of Printer from ALS MWS and Tricon MWS

The capabilities of the ALS MWS and Tricon MWS software and screen layouts will eliminate the need to have a printer for the ALS MWS and Tricon MWS in each protection set. Therefore, the printer will be removed from the PPS replacement design. Therefore, reference to a printer is removed from the following LAR Sections (pages):

3.2.2, Figure 3-3 (page 18)
3.2.2.3 (page 19)
4.2.13, Figure 4-12 (page 87)
4.2.13, Figure 4-13 (page 88)
4.2.14, (pages 98, 99)
4.8.10 (page 143)
4.11.1.3 (page 225)
4.15.1 (pages 260, 262)
4.15.2 (page 263)
4.15.3 (page 264)

This change impacts the Commitments 5, 24, 25, and 26 contained in Attachment 1 to the Enclosure of PG&E Letter DCL-13-043, dated April 30, 2013. The revised commitments are contained in Attachment 1 to the Enclosure.

Response to ALS Plant-Specific Action Items (PSAI) 4, 5, 6, 8, 10, 20, and 22

In PG&E Letter DCL-14-036, "Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement," dated April 30, 2014, PG&E provided the response to the ALS PSAIs to address Request for Additional Information Number 59, except for PSAIs 4, 5, 6, 8, 10, 20, and 22. The ALS PSAIs are contained in Section 4.2 of the NRC Safety Evaluation for the ALS Topical Report 6002-00301, dated September 9, 2013. The response to the PSAIs 4, 5, 6, 8, 10, 20, and 22 is contained below.

PSAI 4

ALS Platform Boundary/Interface Conditions and Installation Limitations - An applicant or licensee referencing this SE should address its conformance to or deviations from the manufacturer identified boundary/interface conditions and installation limitations within the "ALS Platform EQ Summary Report" (see Reference 51, Section 7). An applicant or licensee referencing this SE 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.

PG&E Response to PSAI 4

The ALS Platform Document 6002-00200, Revision 2, "ALS Platform EQ Summary Report," (Reference 51 contained in the NRC Safety Evaluation for the ALS Topical Report 6002-00301) has been updated to Revision 4.

The interface/boundary conditions specified in Section 7.1 of 6002-00200 apply to the PPS ALS subsystem. Conformance for the interface/boundary conditions for the DCPP PPS replacement is documented in Section 6.2 of 6116-00204, Revision 1, "ALS Subsystem Equipment Qualification Evaluation."

The installation limitations specified in Section 7.2 of 6002-00200 apply to the PPS replacement ALS subsystem. Conformance is documented in Section 6.3 of 6116-00204.

PSAI 5

ALS Platform Application Restrictions - An applicant or licensee referencing this SE should address its adherence to the manufacturer identified application restrictions within the "ALS Application Guidance" (see Reference 41). An applicant or licensee referencing this SE 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.

PG&E Response to PSAI 5

The ALS Platform Document 6002-00008, Revision 4, "ALS Application Guidance," (Reference 41 contained in the NRC Safety Evaluation for the ALS Topical Report 6002-00301) has been updated to Revision 6 (note: Platform Document 6002-00008 is being revised again as a result of completion of additional ALS equipment qualification testing).

The PPS ALS subsystem adherence to the ALS platform application restrictions specified in Platform Document 6002 00008, Revision 6, is described in Appendix D of Project Document 6116-00011, Revision 7, "ALS Subsystem System Design Specification."

PSAI 6

Demonstration of Equipment Qualification - An applicant or licensee referencing this SE should demonstrate the equipment qualification testing documented and evaluated within this SE 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 NVM 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.

PG&E Response to PSAI 6

The DCPP PPS Project Document 6116-00204, Revision 1, "ALS Subsystem Equipment Qualification Evaluation," documents an evaluation of the PPS ALS subsystem with respect to the equipment qualification testing that was documented and evaluated under the ALS platform safety evaluation. Section 3 of Project Document 6116-00204 specifically documents the application-specific NVM configurations for the ALS circuit boards and the evaluation of the configurations.

The DCPP PPS Project Document 6116-00204, Section 8, concludes 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 (LSM). The LSM was not tested under the platform equipment qualification testing that was documented and evaluated under the ALS platform safety evaluation. The LSM has been qualified by testing to the requirements specified in Section 12 of the PPS Project Document 6116-00011, Revision 7, "ALS Subsystem System Design Specification."

This qualification is documented in PPS Project Document EQ QR-120-PGE, Revision 0, "Advanced Logic System and Line Sense Module Equipment Qualification Summary Report."

PSAI 8

Deterministic Performance - As discussed within Section 3.4.2, an applicant or licensee referencing this SE 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 SE should also verify the application-specific logic does not introduce non-deterministic computation or non-deterministic digital data communications.

PG&E Response to PSAI 8

The PPS ALS subsystem design is consistent with the discussion in Section 3.4.2 of the ALS NRC safety evaluation.

The DCPP PPS Project Document 6116-10203, Revision 5, "ALS-102 Core A FPGA Software Design Specification," Section 5.5, identifies the sequence and timing of the reliable ALS bus (RAB) transaction (board access) assignments during each frame. Table 5.5-1 of 6116-10203 specifies each sequencer step.

The DCPP PPS Project Document 6116-10204, Revision 4, "ALS-102 Core B FPGA Design Specification," Subsection 4.4.3, identifies the sequence and timing of RAB transaction (board access) assignments during each frame. Table 4.4-2 of 6116-10203 specifies each sequencer step.

The DCPP PPS Project Document 6116-00011, Revision 7, "ALS Subsystem System Design Specification," Requirement R1000, and Project Document 6116-10201, Revision 5, "ALS-102 FPGA Requirements Specification," Requirement R5000, specify the ALS subsystem frame time as 10 milliseconds.

The ALS platform-specific self-diagnostic fault conditions are supplemented by an application-specific ALS-102 board double RAB timeout fault condition. The DCPP PPS Project Document 6116-00011, Subsection 7.2.2, and the associated tables, describe these fault conditions and specify their assignment to the plant failure alarm (for faults that adversely affect the ability of the PPS ALS subsystem to perform its safety system function) or the plant trouble alarm (for faults that indicate ALS subsystem degradation but do adversely affect the ability of the PPS ALS subsystem to perform its safety system function).

The ALS-102 board FPGA application-specific logic is deterministic in all respects. It does not introduce conditions that require the associated finite state machines (FSMs) to wait for responses from unreliable sources (e.g. look-up tables).

Furthermore, ALS Procedures 9006-00043, Revision 6, "ALS Core A FPGA Build Procedure" and 9006 00071, Revision 1, "ALS Core B FPGA Build Procedure" require use of "safe encoding" methods to ensure that undefined FSM state transitions result in reset to a valid (defined) state, thereby preventing nondeterministic behavior.

Finally, the simulation testing of the Register Transfer Level code included predictive models that are based on the interface requirements specified in ALS Platform Documents 6002-00010, Revision 18, "ALS Platform Requirements Specification," and 6002-10201, Revision 5, "ALS-102 Requirements Specification," as well as the requirements specified in the DCPP PPS Project Document 6116-10201. The use of these models results in test failure if non-deterministic behavior is present in the design. No failures were identified in the final production code. A description of these models and the test results are presented in DCPP PPS Project Document 6116-00500, Revision 0, "Diablo Canyon PPS VV Summary Report" and other documents referenced therein.

PSAI 10

Failure Mode and Effects Analysis - As discussed within Section 3.5, an applicant or licensee referencing this SE 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 nonsafety 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.

PG&E Response to PSAI 10

PG&E has prepared a system level Failure Modes and Effects Analysis (FMEA) document to demonstrate the application-specific use of the ALS platform.

PSAI 20

IEEE Std 603-1991 Compliance – As discussed within Section 3.10 of this SE, 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 SE should identify the approach taken to meet each applicable clause of IEEE Std 603-1991. The applicant or licensee should consider its plant-specific design basis because the "ALS Topical Report" scope is limited. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. Therefore, an applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std 603-1991 clause to its application-specific ALS-based safety system or component. As described within Section 3.10 of this SE, 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.

PG&E Response to PSAI 20

The conformance of the ALS subsystem portion of the proposed PPS replacement design to the IEEE Standard 603-1991 clauses is contained in Section 4.10 of the Supplement to LAR 11-07, dated April 30, 2013.

PSAI 22

IEEE Std 7-4.3.2-2003 Compliance – As discussed within Section 3.11 of this SE, although the NRC staff determined the ALS platform supports meeting various sections and clauses of IEEE Std 7-4.3.2-2003, an applicant or licensee referencing this SE should identify the approach taken to meet each applicable clause of IEEE Std 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis, because the "ALS Topical Report" scope is limited. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std 7-4.3.2-2003 clause to its application-specific ALS-based safety system or component. As further described within Section 3.11 of this SE, 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.

PG&E Response to PSAI 22

The conformance of the ALS subsystem portion of the proposed PPS replacement design to the IEEE Standard 7-4.3.2-2003 clauses is contained in Section 4.11 of the Supplement to LAR 11-07, dated April 30, 2013.

Regulatory Commitments

List of New Commitments

Commitment # 1

ALS subsystem board NVM images will be controlled by the PG&E SCMP. Use of the ATCT tool will be performed in accordance with approved plant procedures and the NVM image will be validated by post-maintenance testing.

Commitment # 2

The testing facility will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to be turned over to Operations, per Section 3.1.5 of the Security Plan.

Commitment # 3

The Tricon FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 rnA DC analog temperature input signals from ALS; these signals will be generated by a loop simulator or equivalent test equipment.
2. The FAT will verify bidirectional nonsafety NET2-port communications from Tricon TCM1 and TCM2 to the Tricon MWS through the two Ethernet media converters, and Ports A and B of the two port aggregator network taps.
3. The FAT will verify continued multicast transmission from TCM1 and TCM2 in the event of MWS network communication failure.
4. The Tricon FAT configuration will include the MWSs, port aggregator network tap, network switches, KVM switch, and KVM and media converters.
5. The FAT will verify no inbound communication path from Port 1 of the port aggregator network tap to either Port A or Port B exists.
6. The FAT will verify outbound communications from Port 1 of the port aggregator network tap.

Commitment # 4

The ALS FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 rnA DC analog temperature output signals to Tricon: This interface will be monitored by external equipment to verify conversion and scaling. The ALS analog temperature output channels will be terminated with 250 ohm resistors to simulate the Triconex external termination assembly

(ETA) panel. Voltage across the resistors will be measured to verify analog output function.

2. Unidirectional only, nonsafety EIA-422 communications from the ALS-102 "A" and ALS-102 "B" TXB 1 channels: The TXB 1 channels will be monitored during the ALS FAT to verify data protocol.
3. Unidirectional only, nonsafety EIA-422 communications to the ALS MWS from the ALS-102 "A" and ALS-102 "B" TXB2 channels: The TXB2 channels will be monitored during ALS FAT to verify data protocol.
4. The ALS FAT configuration will include the MWS.
5. Bidirectional EIA-485 TAB communication between ALS Chassis "A" and Chassis "B" and ASU software running on the ALS MWS can take place only if the communication links are physically connected which enables the DI. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected.

Commitment # 5

1. The PG&E SAT will be performed on an integrated system, including the Tricon and ALS subsystems, MWSs, port aggregator network tap, network switches, KVM switch, KVM and media converters.
2. The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT.
3. The SAT will verify interfaces that cannot be tested at the Tricon or ALS FAT, including, in part, verification of information that is transmitted to the Gateway computer and the control board display.
4. Additional testing of communications between the Tricon and its MWS (including network failure) will be performed at the SAT.
5. The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

List of Revised Commitments

Commitments 5, 11, 18, 24, 25, and 26, listed below, previously made in PG&E Letter DCL-13-043, dated April 30, 2013, are superseded by this letter and are removed. Commitments 11, 18, 24, 25, and 26 are revised by changes contained in this letter. The revisions are included as new Commitments 1, 2, 3, 4, and 5 respectively above.

Commitment # 5

The local printer for each protection set will also be controlled by the PG&E SCMP.

Commitment # 11

Modification of ALS FPGA application logic will always be performed using approved

DCPP procedures and will normally not be done with the plant online.

Commitment # 18

The offsite testing facility will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to be turned over to Operations, per Section 3.1.5 of the Security Plan.

Commitment # 24

The Tricon FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 rnA DC analog temperature input signals from ALS; these signals will be generated by a loop simulator or equivalent test equipment.
2. The FAT will verify bidirectional nonsafety NET2-port communications from Tricon TCM1 and TCM2 to the Tricon MWS through the two Ethernet media converters, and Ports A and B of the two port aggregator network taps.
3. The FAT will verify continued multicast transmission from TCM1 and TCM2 in the event of MWS network communication failure.
4. The Tricon FAT configuration will include the MWSs, port aggregator network tap, network switches, KVM switch, printer, and KVM and media converters.
5. The FAT will verify no inbound communication path from Port 1 of the port aggregator network tap to either Port A or Port B exists.
6. The FAT will verify outbound communications from Port 1 of the port aggregator network tap.

Commitment # 25

The ALS FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 rnA DC analog temperature output signals to Tricon: This interface will be monitored by external equipment to verify conversion and scaling. The ALS analog temperature output channels will be terminated with 250 ohm resistors to simulate the Triconex ETA panel. Voltage across the resistors will be measured to verify analog output function.
2. Unidirectional only, non-safety EIA-422 communications from the ALS-102 "A" and ALS-102 "B" TXB 1 channels: The TXB 1 channels will be monitored during the ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB1 channel to either ALS-102 "A" or "B".
3. Unidirectional only, nonsafety EIA-422 communications to the ALS MWS from the ALS-102 "A" and ALS-102 "B" TXB2 channels: The TXB2 channels will

be monitored during ALS FAT to verify data protocol. The test will verify no inbound communications via the TXB2 channel to either ALS-102 "A" or "B".

4. The ALS FAT configuration will include the MWS, KVM switch, printer, KVM and media converters.
5. Bidirectional EIA-485 TAB communication between ALS Chassis "A" and Chassis "B" and ASU software running on the ALS MWS can take place only if the communication links are physically connected and enabled. The test will verify there is no communication between the ALS chassis and the ASU if the communications cables are not physically connected and enabled.

Commitment # 26

1. The PG&E SAT will be performed on an integrated system, including the Tricon and ALS subsystems, MWSs, port aggregator network tap, network switches, KVM switch, printer, KVM and media converters.
2. The physical connection of the temperature channels from the ALS to the Tricon will be verified during the SAT.
3. The SAT will verify interfaces that cannot be tested at the Tricon or ALS FAT, including, in part, verification of information that is transmitted to the Gateway computer and the control board display.
4. Additional testing of communications between the Tricon and its MWS (including network failure) will be performed at the SAT.
5. The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

Abbreviations and Acronyms

Acronym	Definition
ADC	Analog to Digital Converter
ALS	Advanced Logic System
ASU	ALS Service Unit
ATCT	ALS Test and Configuration Tool
BIST	Built-In-Self-Test
CCF	Common Cause Failure
CLB	Core Logic Board
COT	Channel Operability Test
CRC	Cycle Redundancy Checks
CSAT	Cyber Security Assessment Team
CSP	Cyber Security Plan
DCPP	Diablo Canyon Power Plant
DI	Discrete Input
DO	Discrete Output
DOO	Digital Output Overide
EPROM	Erasable Programmable Read Only Memory
EQ	Environmental Quality
FAT	Factory Acceptance Test
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FSM	Finite State Machines
GUI	Graphical User Interface
I/O	Input/Output
IEEE	Institute of Electrical and Electronic Engineers
IRS	Interface Requirements Specification
KVM	Keyboard-Video-Mouse
LAR	License Amendment Request
LSM	Line Sense Module

Acronym	Definition
MFC	Microsoft Foundation Class
MWS	Maintenance Workstation
NVM	Nonvolatile Memory
OOS	Out of Service
PDN	Plant Data Network
PG&E	Pacific Gas and Electric Company
PPS	Process Protection System
PSAI	Plant-Specific Action Items
RAB	Reliable ALS Bus
RTD	Resistance Temperature Detector
SAT	Site Acceptance Test
SCMP	Software Configuration Management Plan
SDOE	Secure Development and Operational Environment
SE	Safety Evaluation
TAB	Test ALS Bus
TS	Technical Specification
VCB	Virtual Channel Bypass
VV	Verification and Validation