Pacific Gas and Electric Company®

Barry S. Allen
Site Vice President

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

805.545.4888
Internal: 691.4888
Fax: 805.545.6445

April 30, 2014

PG&E Letter DCL-14-036

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
Response to Request for Additional Information on License Amendment Request for Digital 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. Digital Instrumentation and Controls Digital I&C-ISG-06, "Task Working Group #6: Licensing Process, Interim Staff Guidance," Revision 1, January 19, 2011 (ADAMS Accession No. ML110140103).
3. NRC Letter "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.
4. NRC Letter "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Request For Additional Information Regarding Request for Replacement of the Digital Replacement of the Diablo Canyon Power Plant Eagle 21 Digital Process Protection System (PPS) With New Digital PPS (TAC NOS. ME7522 AND ME7523)," dated March 31, 2014 (ADAMS Accession No. ML14071A181).

Dear Commissioners and Staff:

In Reference 1, Pacific Gas and Electric Company 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. The LAR format and contents in Reference 1 are consistent with the guidance provided in Enclosure E and Section C.3, respectively, of Digital Instrumentation and Controls (I&C), Revision 1, of

Interim Staff Guidance Digital I&C-ISG-06, "Task Working Group #6: Licensing Process," (ISG-06) (Reference 2). In Reference 3, the Staff documented its acceptance of Reference 1 for review.

The NRC requested additional information to complete the review of Reference 1 in Reference 4. This letter responds to the additional information requested in Reference 4.

This information does not affect the results of the technical evaluation or the significant hazards consideration determination previously transmitted in Reference 1.

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

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 April 30, 2014.

Sincerely,

Barry S. Allen
Site Vice President

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

Enclosure
PG&E Letter DCL-14-036

Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement and Submittal of Revised Process Protection System Replacement System Quality Assurance Plan

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). The LAR 11-07 format and contents are consistent with the guidance provided in Enclosure E and Section C.3, respectively, of Digital Instrumentation and Controls (I&C), Revision 1, of Interim Staff Guidance (ISG) Digital I&C-ISG-06, "Task Working Group #6: Licensing Process." The Staff documented its acceptance of LAR 11-07 for review in the NRC Letter "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.

The Staff requested additional information to support the review of LAR 11-07 in NRC Letter "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). The request for additional information (RAI) is addressed below for RAIs 54 to 70. Each RAI begins with a reference to an open item (OI) that corresponds to the number of the item in the OI table that PG&E has discussed with the Staff during various public meetings. Response to RAIs 1 through 9, 11 through 13, and 15 through 20 were previously provided in PG&E Letter DCL-12-083, "Response to Request for Additional Information on License Amendment Request for Digital Process Protection System Replacement," dated September 11, 2012 (ADAMS Accession No. ML12256A308). RAIs 10 and 14 were not used, and therefore did not require a response. Response to RAIs 21 to 53 were previously provided in PG&E Letter DCL-13-048, "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," dated May 9, 2013 (ADAMS Accession No. ML13130A059).

NRC RAI 54

(Open Item 81) Channel level Bypass Functionality - The DCPP PPS design of the ALS subsystem, allows channel or specific function level configurability while the

remaining safety division functions remain operable. This design does not appear to meet the criteria of ISG-04 positions 10, which only allows for software configuration activities when the entire safety division (i.e., all channels and functions) is inoperable. Please provide a justification for this as an alternative means of meeting the regulatory requirements of Institute of Electrical and Electronics Engineers, Inc. (IEEE) standard IEEE 603-1991 clauses 5.7, 6.5, and 6.7.

PG&E Response to RAI 54

Digital I&C (DI&C) ISG-04 Position states, in part:

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

PG&E provided justification for alternatives to ISG-04 Position 10 for the PPS replacement design in Section 4.8.10 of the LAR Supplement contained in PG&E Letter DCL-13-043, "Supplement to License Amendment Request 11-07, 'Process Protection System Replacement," dated April 30, 2013. For the ALS subsystem, PG&E Letter DCL-13-043 Section 4.8.10 states:

> "Certain ALS data parameters can be modified during plant operation (with the subject instrument channel in bypass mode) or while the plant is shutdown. The non-safety MWS is used to perform these functions when the TAB [Test ALS Bus] is physically connected by means of the TAB access connector. TAB activation is alarmed at the ALS chassis and in the control room."
>
> "Placing an instrument channel in bypass mode for the purpose of changing addressable constants, setpoints, parameters, and other settings associated with a safety function will not affect the safety function of adjacent instrument channels in the same ALS chassis (i.e., ALS-A or ALS-B) that are not bypassed for maintenance. That is, instrument channels that are not bypassed for maintenance will continue to perform their safety functions without requiring that all instrument channels in the ALS chassis be bypassed or removed from service. The time for maintenance will be administratively controlled to require restoration of the ALS chassis within 30 days..."

It was PG&E's intent in PG&E Letter DCL-13-043 to keep an affected ALS Core Chassis in service during maintenance (i.e., while the TAB is connected) to avoid unnecessary Technical Specification (TS) Action entry when performing routine configuration activities such as parameter updates.

The ALS design provides two independent and diverse Core Chassis for each

protection set (i.e., division). This enables one ALS Core Chassis (i.e., Core A) in a protection set to have a safety channel function removed from service while the diverse, independent safety channel function in the unaffected ALS Core Chassis (i.e., Core B) continues to perform the safety function. TS Action entry would not be necessary, except as discussed in PG&E Letter DCL-13-043 Section 4.12:

> "For the condition that the ALS A or B core [chassis] is out of service, the protection function can still be performed and the channel is operable, however the redundancy and diversity of the ALS has been reduced and therefore the situation will be administratively controlled to require restoration of the ALS core within 30 days. For the condition that an ALS A or B core [chassis] is out of service in Protections Sets I and II, TS 3.3.3 Condition A will also need to be entered because the RCS [Reactor Coolant System] wide range [WR] temperature parameter provided by ALS to the Post Accident Monitoring Instrumentation RCS hot leg temperature, RCS cold leg temperature, and reactor vessel water level indication system parameters will be inoperable. If both the ALS A and B core [chasses] are out of service, then the protection function cannot be performed and the channel is inoperable and the appropriate TS Condition for the function will be entered."

Upon subsequent review, PG&E determined that the above discussion addresses the WR RCS temperature channels, which do not perform a safety actuation function, but does not address the safety functions and TS Actions associated with the narrow range (NR) temperature channels. To address this RAI, PG&E will limit ALS Core Chassis routine maintenance activities to ensure the safety channel function can still be performed.

As previously described in Section 4.8.10 of PG&E Letter DCL-13-043, PG&E will take an ALS Core Chassis out of service (OOS) when the TAB is connected. Section 4.2.13.5 of PG&E Letter DCL-13-043 discusses administrative controls for the ALS during calibration and surveillance activities and states that the maintenance workstation (MWS) functions, which use interactive TAB communications will be available: (1) only when the TAB is physically connected to the ALS MWS by qualified personnel under administrative controls; and (2) only on one ALS "A" or "B" subsystem (chassis) at a time.

Normally, taking a Core Chassis OOS would require entry into the TS Actions associated with the functions that depend on the safety channels being processed by the affected Core Chassis (i.e., TS 3.3.1 and TS 3.3.2). However, if the routine maintenance activity is being performed on a safety channel such as RCS Flow (therefore, not associated with NR resistance temperature detector (RTD) signal processing), then:

- TS 3.3.1 Condition E will not be entered for TS Table 3.3.1-1 Function number 6 (Overpower Delta Temperature (OPDT)) and TS Table 3.3.1-1 Function number

7 (Overtemperature Delta Temperature (OTDT)),

- TS 3.3.1 Condition X will not be entered for TS Table 3.3.1-1 Function number 14.b (Steam Generator (SG) Water Level – Low Low Trip Time Delay), and
- TS 3.3.2 Condition M will not be entered for TS Table 3.3.2-1 Function number 6.d.2 (Auxiliary Feedwater initiation on SG Water Level – Low Low Trip Time Delay).

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 OOS, as previously discussed in PG&E Letter DCL-13-043, Section 4.12, and the routine maintenance activity resulting in the OOS condition is not associated with NR RTD signal processing. If an ALS Core Chassis is OOS in Protection Sets I and II, TS 3.3.3 Condition A will be entered as a minimum per PG&E Letter DCL-13-043 Section 4.12.

If the routine maintenance activity that is being performed is associated with NR RTD signal processing within the affected ALS Core Chassis, TS 3.3.1 and TS 3.3.2 actions will be entered as appropriate. TS actions associated with the non-NR RTD channels in the OOS ALS Core Chassis do not need to be entered because the safety functions will continue to be performed by the other independent ALS Core Chassis.

This is a limited exception to ISG-04 Position 10 for the ALS subsystem. The justification for this limited exception is provided below.

WR T_{hot} and WR T_{cold} post-accident monitoring are performed by 2 RCS loops in Protection Sets 1 and 2 for a total of 8 channels. When one ALS Core Chassis is OOS, only 1 WR T_{hot} (TS Table 3.3.3-1 Function number 3) and 1 WR T_{cold} (TS Table 3.3.3-1 Function number 4) channel will be inoperable. TS 3.3.3 Condition A entry is not required for TS Table 3.3.3-1 Function number 3 (RCS Hot Leg Temperature – T_{hot} WR) and number 4 (RCS Cold Leg Temperature – T_{cold} WR), because minimum channel operability requirements are maintained. With a WR T_{hot} OOS, one reactor vessel level indication system channel (TS Table TS 3.3.3-1 Function number 6) is considered inoperable and TS 3.3.3 Condition A entry is required for Function number 6. These actions are described in PG&E Letter DCL-13-043 Section 4.12.

PG&E Letter DCL-13-043 Section 4.12 did not specifically address the NR RTD channels that are input to OPDT and OTDT (TS Table 3.3.1-1 Function numbers 6 and 7, respectively) and trip time delay (TS Table 3.3.1-1 Function number 14.b and TS 3.3.2-1 Function number 6.d.2). These channels require further consideration.

Effects of ALS NR RCS temperature analog output channel failures are bounded by fail high, fail low, and fail as-is. The failure is assumed to be caused by an

undefined interaction between the ALS service unit (ASU) and the ALS to which it is connected.

NR T_{cold1} is processed by ALS Core A Chassis and NR T_{cold2} is processed by ALS Core B Chassis. When a NR T_{cold} channel fails out of range high or out of range low, it will be detected and alarmed by the Tricon subsystem as PPS Trouble, as required by Section 3.2.5.5.5 of the Functional Requirements Specifications (FRS). The SQA-2 algorithm will automatically reject the failed signal and output the good signal to compute the loop average temperature (T_{avg}) and RCS temperature difference (Delta-T). The safety function will continue to be performed in this situation.

A condition in which a T_{cold1} or T_{cold2} channel fails as-is will not be detected while RCS temperatures are steady state. During transient RCS temperature conditions, the SQA-2 algorithm will alarm when a T_{cold1}/T_{cold2} deviation exceeds 2.0°F. The Tricon subsystem will identify this condition as RTD failure. As specified in the FRS Sections 3.2.1.5.1 and 3.2.1.16.5, this condition will result in Delta-T/T_{avg} (DTTA) function bistables being tripped and thus the safety function will be maintained.

The three T_{hot} Group A signals are processed by ALS Core A Chassis. The three T_{hot} Group C signals are processed by the ALS Core B Chassis. Assuming that all T_{hot} signals in one group fail the same way (i.e, fail low, fail high, or fail as-is), the occurrence of a NR T_{hot} failure out of range high or failure out of range low from the affected ALS Core Chassis will be detected and alarmed by the Tricon subsystem as PPS Trouble, as specified in Section 3.2.5.5.5 of the FRS. As long as there are two or more good input signals into the SQA-3 sensor quality algorithm, the Tricon subsystem will use the output of the SQA-3 algorithm to calculate T_{avg} and Delta-T. If the three T_{hot} signals in Group A or Group C have failed out of range, the output of the respective SQA algorithm will be rejected automatically and will not be used to compute T_{avg} and Delta-T. The safety function will continue to be performed in this situation.

NR T_{hot} Group A or Group C fail as-is input values are the same within the group. If one of the T_{hot} groups fails as-is from the affected ALS Core Chassis, the Tricon subsystem may not detect the condition and may continue to use the failed as-is signal to compute T_{avg} and Delta-T, which could compromise the safety function if the DTTA bistables are not considered. However, the DTTA bistables will be tripped by the Tcold1/Tcold2 deviation exceeding 2.0°F and thus the safety function will be maintained operable by the Tricon subsystem of the PPS.

Although the fail-as-is scenario for the Group A or Group C T_{hot} signals may not be detected and alarmed, the likelihood of this scenario is extremely low. Based on the design features required per Interface Requirement Specification (IRS) Section 2.7.2.4, the likelihood of this scenario is not more than minimally impacted if the TAB is connected as compared to the normal on-line configuration with the TAB

disconnected.

ISG-04 Position 10 states:

> "...A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function ... when the associated channel is inoperable."

Declaring an ALS Core Chassis inoperable normally requires entry into the TS Action associated with the functions that depend on the channels being processed by the affected Core Chassis; that is, TS 3.3.1 Condition E (TS Table 3.3.1-1 Function number 6 for OPDT and TS Table 3.3.1-1 Function number 7 for OTDT); Condition X Trip Time Delay (TS Table 3.3.1-1 Function number 14.b in Mode 1 or 2); and TS 3.3.2 Condition M (TS Table 3.3.2-1 Function number 6.d.2 in Modes 1, 2, or 3). It is not necessary to enter TS Conditions for the non-NR RTD channels because their safety function is maintained by the unaffected ALS Core Chassis.

When the routine maintenance activities are being performed on a non-NR RTD channel (e.g., RCS Flow) within the same ALS Core Chassis, the DTTA safety function is maintained operable by the Tricon subsystem and the unaffected ALS Core Chassis as explained above. Therefore, it is not necessary to enter TS 3.3.1 Condition E (TS Table 3.3.1-1 Function number 6 for OPDT and TS Table 3.3.1-1 Function number 7 for OTDT); Condition X Trip Time Delay (TS Table 3.3.1-1 Function number 14.b in Mode 1 or 2); and TS 3.3.2 Condition M (TS Table 3.3.2-1 Function number 6.d.2 in Modes 1, 2, or 3).

The ALS ASU interface offers equivalent protection to the dual processor/shared memory scheme described in ISG-04 Position 10. That is, the interface does not allow the core logic to be modified; it simply allows access to the non-volatile memory (NVM), which contains the configurable parameters. The safety function of the non-NR RTD channel being updated continues to be maintained by the unaffected ALS Core Chassis.

The routine maintenance activity will require the ALS Core Chassis to be removed from service for a very short period of time, estimated at less than one hour, by a trained technician using an approved DCPP procedure.

The action is performed infrequently, once per fuel cycle when coming out of an outage. During power operation, administrative controls allow updating configurable parameters in only one protection set at a time. The other three protection sets will continue to perform their safety function. In order to perform the parameter update, the TAB must be enabled, which will be alarmed as PPS Trouble (IRS 2.8.2.2)

In addition, the likelihood of the Group A or Group C T_{hot} fail as-is scenario occurring concurrent with a transient requiring these signals for mitigation is not significantly greater with the TAB connected versus the TAB disconnected.

In conclusion, PG&E requests NRC approval of a limited exception to ISG-04 Position 10 for the ALS subsystem. The exception to ISG-04 Position 10 is that when removing a single ALS chassis from service in any protection set to perform routine maintenance activities on an unrelated (not associated with NR RTD signal processing) channel, the following TS Conditions will ***not*** be entered:

- TS 3.3.1 Condition E for TS Table 3.3.1-1 Function number 6 (OPDT) and TS Table 3.3.1-1 Function number 7 (OTDT)
- TS 3.3.1 Condition X for TS Table 3.3.1-1 Function number 14.b (SG Water Level – Low Low Trip Time Delay)
- TS 3.3.2 Condition M for TS Table 3.3.2-1 Function number 6.d.2 (Auxiliary Feedwater initiation on SG Water Level – Low Low Trip Time Delay)

If the routine maintenance activity that is being performed ***is*** associated with NR RTD signal processing within the affected ALS Core Chassis, TS 3.3.1 and TS 3.3.2 actions ***will*** be entered as appropriate.

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 OOS, as previously discussed in PG&E Letter DCL-13-043 Section 4.12, and the routine maintenance activity resulting in the Core Chassis OOS condition is not associated with NR RTD signal processing. If an ALS Core Chassis is OOS in Protection Sets I and II, TS 3.3.3 Condition A ***will*** be entered as a minimum per PG&E Letter DCL-13-043 Section 4.12.

NRC RAI 55

(Open Item 88) ALS Documentation – Please explain the numbering scheme between the ALS Generic platform documents 6002-xxx01, 6002-xxx06 and application-specific documents 6116-10201. For example, there is no Document 6116-10206 for the DCPP PPS. Please explain why certain documents do not appear to have been created.

PG&E Response to RAI 55

Both the ALS 6002-10201 and 6002-10206 documents are ALS platform documents that are applicable to DCPP. The document numbering scheme is project-specific. The 6116-10201 document is specific to DCPP ("6116" is the DCPP PPS Replacement Project number designation) and is in addition to the ALS platform documents. Because the 6002-10201 document includes hardware design that is not duplicated for DCPP (the board is already designed), there is no need to replicate a board requirements document at the DCPP document level.

A summary of the documents is as follows:

1. 6002-10201 – Platform 102 Board Requirements (applies to the ALS platform and all applications)
2. 6002-10206 – Platform 102 Board FPGA Design Specification (applies to the ALS platform and all applications, with the exception of the sequencer definition which is application specific)
3. 6116-10201 - Diablo Canyon 102 Board FPGA Requirements (includes application specific information including sequencer definition)
4. 6116-10203 and 6116-10204 - Diablo Canyon 102 Board FPGA Design Specifications for ALS Core A and B

NRC RAI 56

(Open Item 100) IEEE 603, Section 5.2, Completion of Protective Action – Section 4.10.2.2 of the LAR states that "The design for the PPS replacement meets the requirements of IEEE 603-1991 Clause 5.2, Completion of Protective Action." The NRC has reviewed the PPS FRS and has found no system specifications for safety function logic that would ensure the completion of protective actions or that could be credited for meeting the criteria of Clause 5.2. Instead, it appears that the completion of protective action or latching functions are performed by external systems such as the Solid State Protection System (SSPS) that are not being impacted by the PPS replacement. Please provide an explanation of how this criterion is being satisfied for each RTS and ESFAS safety function and provide details of any PPS functions that are to be credited as a basis for meeting these criteria.

PG&E Response to RAI 56

The PPS compares plant parameters against protective setpoints and provides discrete actuation signals to the SSPS, whose logic is not affected by the PPS replacement. The PPS de-asserts the initiating signal when the monitored parameter no longer satisfies the trip condition. Reactor trip commands are carried to completion when the reactor trip circuit breakers trip because the breakers remain in the tripped condition until they are manually reset. Latching relays in the SSPS ensure that the following engineered safety feature functions are carried to completion once they are initiated, and require manual reset:

- Safety Injection – Feedwater Valve Closure
- Safety Injection (manual reset blocked for 30 seconds after initiation)
- Containment Isolation Phase A
- Containment Isolation Phase B
- Containment Ventilation Isolation (initiated by containment ventilation radiation monitor)
- Feedwater Isolation (Low T_{avg} and Reactor Trip)

- Spray Actuation

NRC RAI 57

(Open Item 104) Functional Requirements for Channel Bypass - The PG&E FRS Section 2.2.3.1 & 2, and 3.2.1.3.5 & 6 seem to indicate that channel bypass functions are only implemented for Containment Pressure High-High actuation of Containment Spray, and Turbine Impulse Pressure High P-13 actuation, however, the Function diagrams for Reactor Coolant System Flow signals, Pressurizer Pressure Reactor Trip, Safety Injection actuation, Power Operated Relief Valve (PORV) actuation P-11 also show manual bypass switch capability. Additionally, the detailed channel specifications for these functions (i.e. 3.2.7) do not provide any specifications for these channel bypass functions. Please explain why these channel bypass functions are not specified in the PPS FRS.

PG&E Response to RAI 57

Containment Pressure High-High actuation of Containment and Turbine Impulse Pressure High P-13 actuation channels are operating bypass functions implemented to satisfy TS. Manual bypass and trip switches are provided on all ALS protection functions for maintenance purposes. The switches are not part of the ALS protection logic, and therefore do not have detailed specifications contained in the FRS. However, the FRS contains specifications for monitoring of the switches.

The NRC approved ALS diversity scheme requirements that protective action initiated from either ALS diversity group (Core A Chassis or Core B Chassis) will cause the protective action and that neither diversity group may impede protective action initiated by the other core chassis. Without the bypass switch, if a ALS-402 discrete output card, for example, had to be replaced for maintenance, partial trip signals would be sent to the SSPS for all the de-energize to trip channels on the card. Both ALS Core A Chassis and ALS Core B Chassis implement all safety actuation functions. The manual bypass switches allow one ALS core chassis to be removed from service temporarily for maintenance and the associated partial trip signals to be blocked while leaving the other chassis fully able to perform its safety function.

However, RCS temperature signals are not fully implemented in both core chasses. The NRC approved diversity analysis addresses protective functions dependent upon the temperature signals. Similarly, manual trip switches allow any or all channels to be tripped for maintenance or other reasons.

NRC RAI 58

(Open Item 106) Please provide a description of how the information provided by the ALS Parameter Display system will be used to "support or enhance execution of the

safety function." In particular, explain how the continuous availability and use of this data is consistent with ISG-04, Position 1, Point 3.

PG&E Response to RAI 58

ISG-04, Position 1, Point 3 states in part, "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." Each ALS protection set contains its own non-safety ALS MWS and each ALS protection set does not receive any communication from outside its own division. This information is provided on page 123 of the LAR Supplement in PG&E Letter DCL-13-043.

The on-line non-safety communications, between the PPS controllers and their respective dedicated MWS units, improve the ability to maintain the PPS which improves the reliability of the PPS. In addition, the on-line ALS non-safety communications enable on-line surveillance testing, calibration, and maintenance. The risk of challenging plant safety systems by inadvertent actuation is reduced through the ability to test when in bypass rather than requiring test in a trip condition. The on-line ALS non-safety communications capability provide real-time, on-line data and status information on the Plant Data Network Gateway Computer and in the Control Room that are required to perform maintenance, calibration, and testing. Without the on-line data links from ALS to the MWS and the Plant Data Network Gateway Computer, only the control board indicators and recorders would be available to provide "window" indicator information for the PPS. System trouble alarms would still be generated by the PPS on the main annunciator system, but without the alarm monitor and other data display capabilities provided by the MWS, there would be no direct means to remotely determine the specific cause of an alarm. Lack of access to real-time, continuous, on-line PPS status data and diagnostic information would introduce a delay into PPS trouble identification and resolution, and substantially degrades the maintenance effectiveness and timeliness enabled by the diagnostic features built into the platforms and the application programs. The ability to make on-line use of the information provided by redundant, real-time data communications to the MWS and to the plant process computer improves PPS reliability and thus supports and enhances safety through providing timely diagnostic information and status details that assist performance of required trouble-shooting, maintenance, and surveillance activities. This information is provided on page 90 of the LAR Supplement in PG&E Letter DCL-13-043.

NRC RAI 59

(Open Item 94) ALS Plant Specific Action Items - Please provide documentation to identify how each applicable Plant Specific Action Item (PSAI) in the ALS Topical Report safety evaluation is being addressed for the PPS project. This document should include references to the LAR and supporting documents where PSAI's are addressed.

PG&E Response to RAI 59

The response to the ALS PSAIs 4, 5, 6, 8, 10, 20, and 22 requires additional input from Westinghouse on the detailed ALS design to fully address the PSAI. The documentation to identify how ALS PSAIs 4, 5, 6, 8, 10, 20, and 22 are being addressed for the PPS project will be submitted by August 30, 2014.

PSAI 1

Application-specific ALS-102 Requirements Specification(s) - An applicant or licensee referencing this SE [Safety Evaluation] should demonstrate it has provided application specification(s) to govern each unique ALS-102 FPGA logic program's development.

PG&E Response to PSAI 1

PG&E has provided application-specific requirement specifications to Westinghouse to govern ALS-102 FPGA logic program development design in the DCPP PPS Replacement FRS, Revision 9, and the IRS, Revision 9.

PSAI 2

Application Conformance to ALS Platform Development Process - An applicant or licensee referencing this SE 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 of this SE. When the application uses only a single FPGA design variant, this demonstration should identify the associated design variant (either "Core A" or "Core B") and include the production and configuration control of related life-cycle development products, including those identified in Table 3.2.5-1 for that design variant, where "xxxx" represents a project specific identifier or may directly refer to "6002" if that document may be used without application-specific modification.

PG&E Response to PSAI 2

Concern for ALS software common cause failure (CCF) in the DCPP PPS replacement is addressed through incorporating additional design diversity in the FPGA-based hardware system as described in Section 4.1.1 of the LAR Supplement contained in PG&E Letter DCL-13-043. The ALS Platform Development Process for the DCPP PPS utilizes both "Core A" and "Core B" design variants, rather than a single core design. Details on the development process used are contained in Sections 4.2.11, 4.3, 4.5.2.3, 4.5.3.3, 4.5.6, 4.10.2.3, and 4.11.1.1 of the LAR Supplement contained in PG&E Letter DCL-13-043.

Westinghouse Document No. 6002-00000, "ALS Management Plan," meets the guidance of Branch Technical Position (BTP) 7-14 Section B3.1.1 and defines the process used to manage the ALS platform development project and overall project life-cycle. The ALS Management Plan follows the Quality Assurance (QA) program as defined in the "Westinghouse Quality Management System."

Westinghouse Document No. 6116-00000, "Diablo Canyon PPS Management Plan," is the project specific procedure that meets the guidance of BTP 7-14 Section B3.1.1 and NRC Regulatory Guide (RG) 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," and defines the process used to manage the PPS Replacement project and overall product life-cycle. This plan follows the QA program used by Westinghouse as defined in the "Westinghouse Quality Management System," and defines the set of unique activities as defined in IEEE Standard 1058-1998, "IEEE Standard for Software Project Management Plans," for delivery of the ALS-based chassis portion of the PPS replacement system. The 6116-00000 document includes details on how the independent verification and validation (IV&V) team has an independent organizational reporting structure from the design and implementation team. The IV&V team has an independent organizational reporting structure from the design and implementation team.

To ensure quality requirements are met, Westinghouse Document No. 6002-00001, "ALS Quality Assurance Plan," was used. It provides definitions for the techniques, procedures, and methodologies which are used to assure quality in the design and test developments of the ALS platform.

The DCPP PPS replacement design does not use only a single FPGA design variant.

PSAI 3

Application Conformance to "Embedded Design Diversity" Development Process - When an applicant or licensee referencing this SE 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 of this SE. This demonstration should include the production and configuration control of the related life-cycle development products, including those identified in Table 3.2.5-1 for both "Core A" and "Core B."

PG&E Response to PSAI 3

The ALS Platform Development Process for the DCPP PPS replacement utilizes Embedded Design Diversity; that is, both Core A and Core B FPGA design variants. The FPGA design variants followed equivalent development processes to those described in Section 3.2.4 of the NRC Safety Evaluation.

Based on the DCPP project specific design development documents contained in Westinghouse Document No. 6116-00000, "Diablo Canyon PPS Management Plan," the development of the DCPP PPS replacement design of the ALS-102 Core Logic Board (CLB) included the following project specific documents equivalent to those in Table 3.2.5-1 of the NRC Safety Evaluation:

- Westinghouse Document No. 6116-10203, "Diablo Canyon PPS ALS-102 Core A FPGA Design Specification"
- Westinghouse Document No. 6116-10204, "Diablo Canyon PPS ALS-102 Core B FPGA Design Specification"
- Westinghouse Document No. 6116-00059, "Diablo Canyon Units 1 & 2 Process Protection System ALS Requirements Traceability Matrix" (covers Core A and Core B)
- Westinghouse Document No. 6116-10216, "Diablo Canyon PPS V&V Simulation Environment Specification" (covers Core A and Core B)
- Westinghouse Document No. 6116-10220, "Diablo Canyon PPS ASE-102 Core A FPGA Test"
- Simulation Environment Specification
- Westinghouse Document No. 6116-10225, "Diablo Canyon PPS ASE-102 Core B FPGA Test"
- Simulation Environment Specification
- Westinghouse Document No. 6116-10221, "Diablo Canyon PPS ASE-102 Core A FPGA Test"
- Design Specification
- Westinghouse Document No. 6116-10226, "Diablo Canyon PPS ASE-102 Core B FPGA Test"
- Design Specification
- Westinghouse Document No. 6116-10222, "Diablo Canyon PPS ASE-102 Core A FPGA Test"
- Case Specification
- Westinghouse Document No. 6116-10227, "Diablo Canyon PPS ASE-102 Core B FPGA Test"
- Case Specification
- Westinghouse Document No. 6116-70031, "Diablo Canyon System Test Case Specification" (covers Core A and Core B)
- Westinghouse Document No. 6116-70032, "Diablo Canyon Factory Acceptance Test Procedure" (covers Core A and Core B)
- Westinghouse Document No. 6116-70140, "Diablo Canyon PPS System Test Design Specification" (covers Core A and Core B)

- Westinghouse Document No. 6116-00050, "Diablo Canyon PPS Configuration Status Accounting" (covers Core A and Core B)
- Westinghouse Document No. 6116-00400, "Diablo Canyon PPS Configuration Management Summary Report" (covers Core A and Core B)
- Westinghouse Document No. 6116-00500, "Diablo Canyon PPS IV&V Summary Report" (covers Core A and Core B)
- Westinghouse Document No. 6116-71000, "Diablo Canyon System Test Report" (covers Core A and Core B)

PSAI 7

Response Time Performance - As discussed within Section 3.4.1, an applicant or licensee referencing this SE 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.

PG&E Response to PSAI 7

Information on the response time performance for the DCPP PPS replacement ALS subsystem is contained in Section 4.2.12 of the LAR Supplement in PG&E Letter DCL-13-043. In accordance with the FRS, the time response of the PPS processing instrumentation (from input signal conditioner to conditioned output signal) shall not exceed 0.409 seconds. The response time for the ALS subsystem for the PPS replacement architecture is contained in Westinghouse Document No. 6116-00011, "Diablo Canyon Process Protection System, ALS System Design Specification." For the (temperature) channels shared with the ALS FPGA-based system, the 0.409 seconds is allocated between the ALS and the Tricon as stated in Section 1.5.8 of the IRS. The 0.409 seconds PPS processing instrumentation response time is allocated between the ALS and Tricon as follows:

- ALS: 0.175 seconds for RTD processing
- Tricon: 0.200 seconds
- Contingency: 0.034 seconds

Table 7-4 in Section 7.5 of Westinghouse Document No. 6116-00011 identifies the ALS board access sequence, provides a budget analysis associated with digital response time performance, and verifies the time response specifications are met.

As previously stated in PG&E Letter DCL-12-083, dated September 11, 2012, the ALS response time will be verified as part of the Factory Acceptance Test (FAT) and the results will be included in the FAT summary report to be submitted (see Commitment 33 in Attachment 1 to the Enclosure of PG&E Letter DCL-12-083).

Surveillance Requirement 3.3.1.16 for the reactor trip system (RTS) and 3.3.2.10 for the engineered safety features actuation system (ESFAS) instrumentation include requirements to verify instrumentation response time are within limits.

PSAI 9

Self-Diagnostics, Test and Calibration Capabilities - As discussed within Section 3.4.3, an applicant or licensee referencing this SE 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.

PG&E Response to PSAI 9.a

The ALS platform is being implemented in the PPS portion of the protection system which performs processing of the sensor signals.

The ALS platform is not being utilized in the SSPS logic portion of the protection system or the relay portion of the protection system. These portions of the protection system are not being changed as part of the PPS Replacement Project and these portions are tested separately on-line using channel operability tests (COTs), or during refueling outages using channel calibrations and trip actuation device tests.

The available ALS diagnostic programs and self-test capabilities, through periodic injection of simulated process data into the channel, allow the performance of the COT, without injection of an external simulated or actual signal into the channel. The ALS platform allows manual verification that the setpoints and tunable parameters are correct by displaying the current values on the ALS MWS during performance of the COT. The revised TS 1.1 COT definition, discussed in Section

4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, requires manual verification that the setpoints and tunable parameters are correct.

As described in Section 3.1.1.1 of the ALS Topical Report Submittal, the ALS platform self-test strategy is based on four simple and effective steps:

> Detect: The ALS platform detects faults in its circuits or connected field devices by running background tests on a regular interval, and by redundancy.
>
> Mitigate: The circuits causing the failure are isolated before the failure is allowed to propagate from an ALS board to another and from the ALS to other systems.
>
> Announce: The detected failure is announced using the ALS chassis alarm and an alarm on the Control Room main annunciator system (MAS) "window" indicator. The on-line ALS non-safety communications capability provide real-time, on-line data and status information on the PDN Gateway Computer and to the MWS. The use of the on-line ALS non-safety communications capability provides redundant, real-time results of the diagnostic and self test features that provide timely diagnostic information on instrument channel OPERABILITY and status details that assist in timely performance of required trouble-shooting and maintenance. In addition, the MWS can provide detailed status indication, such as indicating in which function the failure occurred and providing indication as to whether the system remains operable.
>
> React: The failure is announced using the system alarm and by other application specific means. The on-line ALS non-safety communications capability provides real-time, on-line data and status information on the Plant Data Network (PDN) Gateway Computer and to the MWS. The use of the on-line ALS non-safety communications capability provides timely diagnostic information and status details that assist in timely performance of required troubleshooting and maintenance. In addition, the MWS can provide detailed status indication to support troubleshooting and maintenance.

Section 2.8 of Westinghouse Document No. 6002-00011, "ALS Platform Specification," describes the built-in-self-test (BIST) used for exercising all critical functions within a board to ensure latent failures cannot buildup in the system and make it inoperable without knowledge of plant personnel. This section also describes the inherent self-test method used to quickly detect stuck or open failures.

Section 3.1.1.2 of the ALS Topical Report Submittal, discusses self-testing performed from the field input, through the ALS input board, ALS CLB, ALS output board, and the field output. Table 3.1-1 of the ALS Topical Report Submittal identifies the self-testing test intervals for each ALS board.

The ALS-311 input board BIST operation begins with providing a single dedicated multichannel analog to digital converter (ADC) for each input for the purpose of measuring the field input signal and for sampling the onboard diagnostic signal references. Westinghouse Document No. 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 input/output (I/0) boards. In the ALS used for the DCPP PPS replacement subsystem, any integrity BIST failure is alarmed at the system level and provided to the MAS. The ALS-321 input board BIST is the same as for the ALS-311 input board.

The ALS-402 output board BIST integrity checking is accomplished by continually monitoring a feedback signal tied to an output to verify the commanded state matches the feedback state. The technique used is described in Westinghouse Document No. 6002-40202, "ALS-402 Design Specification." To verify operability of the circuit beyond the circuit isolation barrier and verify operability of downstream wiring and devices (SSPS, etc.) in the DCPP PPS replacement, the ASU can be used to place the ALS-402 output in question into an override mode and can then be used to command the output to the desired state (i.e. open/close). If an ALS-402 board output fails its integrity BIST, a failure is alarmed at the system level and provided to the MAS. A failed ALS-402 board output is driven automatically to its predefined failsafe state. Therefore, verification of ALS-402 operability does not require an injected signal source.

In addition to the encoding diversity that occurs on ALS boards, the ALS-102 CLB uses several levels of checking internal memory to verify that no change in safety logic has occurred. In the configuration section of NVM on every board, a 32-bit checksum is run against the following address locations:

- Board ID
- Project ID
- Channel Configuration
- Linearization Coefficients

In addition, a 16-bit cycle redundancy check is run on every NVM memory address location. An ALS board that does not pass the NVM check will revert to the FAIL mode and the board will not operate.

The FPGA design uses the on-chip static random access memory (SRAM) blocks, and provisions are made that ensure that single event upsets of the SRAM content does not result in the board being incapable of performing its safety function.

The Actel ProASIC®3L device family used in the ALS contains SRAM blocks which are used by the ALS logic. When these SRAM blocks are used, redundancy checking, parity checking and cycle redundancy checks are employed to ensure that corruption of a memory cell does not cause the ALS board to enter a halt state. Persistent memory corruptions are announced.

The BIST integrity checking on the ALS-421 output board is accomplished in a similar manner as is performed on the ALS-402 board. As described in Westinghouse Document No. 6002-42102, "ALS-421 Design Specification," the ALS-421 output board uses the combination of a digital-to-analog and an ADC for command and feedback for an output. The ALS-421 output board performs a difference detection between the commanded output and the output feedback, and if the feedback value exceeds a defined plus/minus error percentage, the ALS-421 output board will report the channel as an error. If an ALS-421 board output fails its integrity BIST, a failure is alarmed at the system level and is provided to the MAS. A failed ALS-421 board output is driven automatically to its predefined failsafe state. As with the ALS-402 board, an ALS-421 board output of interest can be placed into an override mode and commanded to a known analog output level for the purposes of determining the operation of downstream devices (e.g., Tricon). Therefore, verification of ALS-421 operability does not require an injected signal source.

Section 4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, states that for the ALS subsystem, the platform self-tests and the application specific test and calibration functions will be verified during the FAT to ensure that the protection set safety function is not adversely affected by performance of either built-in or application specific test and calibration functions.

The TS required channel calibrations are normally performed during refueling outages (but they can be performed on-line). The channel calibrations are a complete check of the instrument loop, including the sensor. These tests verify that the ALS channel responds to a measured parameter within the necessary range and accuracy.

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.

PG&E Response to PSAI 9.b

PG&E is not requesting to eliminate current TS required periodic surveillance tests or revise current TS surveillance frequencies based on the diagnostic capabilities of the PPS replacement. The TS 1.1 COT definition is being revised for the ALS digital

channels, as discussed in Section 4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, to require the use of diagnostic programs to test the digital hardware instead of injection of a simulated signal into the channel. This change is based on the BIST features of the ALS platform. The above response to PSAI 9.a describes the self-test and diagnostic features of the ALS input board, CLB, and output board and how they are comprehensive enough to provide equivalent assurance to injection of a simulated signal into the channel to verify operability.

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.

PG&E Response to PSAI 9.c

In Section 4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, PG&E has proposed a change to the TS 1.1 definition for COT based on the diagnostic and self-test capabilities of the ALS subsystem. The changes to the COT definition in the TS require manual verification that the setpoints and tunable parameters are correct, and require injection of a 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 response to PSAI 9.a above describes the self-test and diagnostic features of the ALS input board, CLB, and output board and how they are comprehensive enough to provide equivalent assurance to injection of a simulated signal into the channel to verify operability.

The TS required channel calibrations are normally performed during refueling outages (but they can be performed on-line). The channel calibrations are a complete check of the instrument loop, including the sensor. These tests verify that the ALS channel responds to a measured parameter within the necessary range and accuracy and would identify that the ALS diagnostic and self-test capabilities are not functioning properly.

Section 4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, states that for the ALS subsystem, the platform self-tests and the application specific test and calibration functions will be verified during the FAT to ensure that the protection set safety function is not adversely affected by performance of either built-in or application specific test and calibration functions. These tests will ensure the DCPP PPS replacement ALS subsystem does not exhibit unjustified intermediate errors without reported failures that could adversely affect a safety function.

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.

PG&E Response to PSAI 9.d

Section 12.1.2 of the ALS Topical Report discusses the board level Failure Modes and Effects Analysis (FMEA) performed on each of the ALS boards. The effect of single failure for the DCPP PPS replacement ALS application level is contained in Westinghouse Document No. 6116-00029, "Diablo Canyon PPS ALS Reliability Analysis and FMEA." Failures in the application-specific diagnostic or self-test features are bounded by the failures considered in Table 4-4 of Westinghouse Document No. 6116-00029, and therefore have no impact on the safety function due to the diversity and redundancy included in the ALS design.

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.

PG&E Response to PSAI 9.e

The TS 1.1 COT definition is being revised for the ALS digital channels, as discussed in Section 4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, to require the use of diagnostic programs to test the digital hardware instead of injection of a simulated signal into the channel. With this change, a COT can be performed on the ALS channels without connecting the TAB and declaring the channel inoperable. This significantly limits the number of entries into TS Required Actions compared to the current Eagle 21 PPS.

The PPS replacement architecture provides two individual MWSs in each protection set. One MWS is dedicated to the Tricon, and the other MWS is dedicated to the ALS. A MWS within a given protection set communicates only with the controllers to which it is connected in its own protection set. A MWS cannot communicate with, modify, or affect the operation of the MWS from another protection set, nor can a MWS within a given protection set communicate with, modify, or affect the operation of a safety controller in another Protection Set.

Section 4.2.13.5 of the LAR Supplement contained in PG&E Letter DCL-13-043 discusses administrative controls for the ALS during calibration and surveillance activities and states the MWS functions that use interactive TAB communications will

be available: (1) only when the TAB is physically connected to the ALS MWS by qualified personnel under administrative controls; and (2) only on one ALS "A" or "B" subsystem (chassis) at a time. During this time, the other three protection sets will continue to perform their safety function. In order to perform the parameter update, the TAB must be enabled, which will be alarmed as PPS Trouble.

In addition, as stated in Section 4.8.10 of the LAR Supplement contained in PG&E Letter DCL-13-043, activation of the TAB communication link is monitored by the ALS subsystem and administratively controlled through physically disconnecting the communication link when the TAB is not in use. Communication between the ALS MWS and the ALS via the TAB are not possible when the TAB is disconnected. The TAB is connected infrequently under procedural control by trained personnel, and only when required during surveillance testing, maintenance, and troubleshooting while the channel is placed in the bypass mode and declared OOS.

f. Conformance to 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 RGs 1.22 and 1.118.

PG&E Response to PSAI 9.f

Conformance to RG 1.22, "Periodic Testing of Protection System Actuation Functions," Revision 0, and RG 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, is described below. In summary, the PPS replacement design provides the capabilities for test and calibration while retaining the equipment's ability to accomplish its safety function, to support tripping or bypassing individual functions per channel when TS limiting conditions for operation are not met, and to provide continuous indication of these compensatory actions in the control room.

RG 1.22

Position 1
The protection system should be designed to permit periodic testing to extend to and include the actuation devices and actuated equipment.
a. The periodic tests should duplicate, as closely as practicable, the performance that is required of the actuation devices in the event of an accident.
b. The protection system and the systems whose operation it initiates should be designed to permit testing of the actuation devices during reactor operation.

The PPS replacement is a digital replacement for the existing digital Eagle 21 PPS at DCPP. The capability for testing and calibration of the PPS replacement is not significantly different from that of the existing Eagle 21 PPS.

The ALS platform is not being utilized in the SSPS logic portion of the protection system or the relay portion of the protection system. These portions of the protection system are not being changed as part of the PPS Replacement project, and are tested separately on-line using COTs or during refueling outages using channel calibrations and trip actuation device tests.

The PPS replacement permits any individual instrument channel to be maintained and calibrated in a bypassed condition, and when required, tested during power operation without initiating a protective action at the system level. This is accomplished without lifting electrical leads or installing temporary jumpers. The PPS replacement permits periodic testing during reactor power operation without initiating a protective action from the channel under test. The ALS subsystem is capable of being tested during power operation through use of simulated signal inputs into a channel that can be applied using measuring and test equipment.

Position 2
Acceptable methods of including the actuation devices in the periodic tests of the protection system are:
a. Testing simultaneously all actuation devices and actuated equipment associated with each redundant protection system output signal;
b. Testing all actuation devices and actuated equipment individually or in judiciously selected groups;
c. Preventing the operation of certain actuated equipment during a test of their actuation devices;
d. Providing the actuated equipment with more than one actuation device and testing individually each actuation device. Method a. set forth above is the preferable method of including the actuation devices in the periodic tests of the protection system. It shall be noted that the acceptability of each of the four above methods is conditioned by the provisions of regulatory positions 3 and 4 below.

The DCPP protection system design allows individual testing of the RTS, ESFAS, and SSPS portions of the protection system. External hardwired switches are provided on all PPS replacement trip and actuation outputs to support testing of each redundant PPS channel in each protection set. The switches may be used for SSPS input relay testing or to trip or actuate the channel manually if needed. Activation of the external trip switches is indicated in the control room through the SSPS partial trip indicators. Actuation of bypass switches for ALS subsystem is indicated in the control room through the MAS and is administratively controlled.

Position 3
Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation:
a. Positive means should be provided to prevent expansion of the bypass condition to redundant or diverse systems, and

b. Each bypass condition should be individually and automatically indicated to the reactor operator in the main control room.

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. Actuation of bypass switches for the ALS subsystem is indicated in the control room through the MAS.

Position 4
Where actuated equipment is not tested during reactor operation, it should be shown that:
a. There is no practicable system design that would permit operation of the actuated equipment without adversely affecting the safety or operability of the plant;
b. The probability that the protection system will fail to initiate the operation of the actuated equipment is, and can be maintained, acceptably low without testing the actuated equipment during reactor operation, and
c. The actuated equipment can be routinely tested when the reactor is shut down.

The DCPP PPS replacement ALS equipment is designed to be tested during reactor operation.

RG 1.118

Conformance with the requirements of IEEE Std. 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," provides a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to periodic testing of electric power and protection systems if the following exceptions are complied with:

Position 1
The definitions of "safety systems," "safety function," and "safety group" in IEEE Std. 603-1991,1 "Criteria for Safety Systems for Nuclear Power Generating Stations," are used instead of the definitions in IEEE Std. 338-1987.

IEEE Standard 603-1991 [21], Clause 5.7 states:
Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987 [3]. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

(1) appropriate justification shall be provided (for example, demonstration that no practical design exists),
(2) acceptable reliability of equipment operation shall be otherwise demonstrated, and
(3) the capability shall be provided while the generating station is shut down.

Section 4.10.2.7 of the LAR Supplement contained in PG&E Letter DCL-13-043, addresses how the DCPP PPS replacement complies with IEEE Standard 603-1991, Clause 5.7 and IEEE Std 338-1987.

The PPS Replacement design is safety related Class I equipment for the portions required to perform the safety function.

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 the ALS subsystem. The requirement for periodic testing is addressed by required TS 3.3.1 and TS 3.3.2 COTs and channel calibrations surveillance requirements. The PPS replacement COTs can be performed on-line and are supported by the bypass capability built into the design. The channel calibrations are performed on-line using the bypass capability of the channel or during refueling outages when the PPS is not required to be operable. Calibration and testing is performed according to approved procedures that establish specific surveillance techniques and surveillance intervals intended to maintain the high reliability of the PPS replacement.

The PPS replacement design allows on-line testing for troubleshooting or maintenance without disconnecting wires, installing jumpers, or otherwise modifying the installed equipment. Simulated signal inputs into a channel can be applied using measuring and test equipment. During performance of testing or maintenance of the PPS replacement, it may be necessary to place the individual channel into the bypass mode.

Administrative procedures will provide appropriate guidance in the event a portion of the PPS replacement is in bypass or is manually tripped. These procedures are augmented by automatic indication at the system level that the system is in bypass or that a portion of the protection system and/or the systems actuated or controlled by the protection system is tripped.

Section 3.2 of the ALS Topical Report describes the ALS design to support periodic surveillance testing, channel calibration and maintenance on a particular channel, while retaining the capability to accomplish the intended safety functions on the remaining channels. Section 3.4 of the ALS Topical Report describes the ALS design to support calibration of an analog I/O channel using the ASU and calibrated external test

equipment. Section 12.1.8 of the ALS Topical Report describes the ALS platform compliance with IEEE Standard 603-1991, Clause 5.7.

Position 2
Both Sections 5(15) and 6.4(5) of IEEE Std. 338-1987 are replaced by the following:

Procedures for periodic tests shall not require makeshift test connections except as follows:

(1) Temporary jumper wires may be used with safety systems that are provided with facilities specifically designed for the connection of portable test equipment. These facilities shall be considered part of the safety system and shall meet all the requirements of IEEE Std. 338-1987.
(2) Removal of fuses or opening a breaker is permitted only if such action causes trip of the associated channel or actuation of the logic of the associated load group.
(3) Test procedures or administrative controls shall provide for verifying the open circuit or verifying that temporary connections are restored after testing.

Section 4.10.2.7 of the LAR Supplement contained in PG&E Letter DCL-13-043, addresses the capability for testing and calibration of the PPS replacement. The PPS replacement provides enhanced self-testing and diagnostic functions that reduce likelihood of undetected failures in the ALS subsystem. These self-testing and diagnostic functions do not impact the PPS replacement design that supports testing without disconnecting wires, installing jumpers, or otherwise modifying the installed equipment. The PPS replacement design supports injection of simulated signal inputs into a channel that can be applied using measuring and test equipment. The PPS replacement bypass and trip switches to support testing are permanent plant equipment.

Position 3
The description for a logic system functional test, as noted in Section 6.3.5 of IEEE Std. 338-1987, implies that the sensor is included. A logic system functional test is to be a test 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, to verify operability.

The TS 1.1 COT definition is being revised for the ALS digital channels, as discussed in Section 4.12.1 of the LAR Supplement contained in PG&E Letter DCL-13-043, to require the use of diagnostic programs to test the digital hardware as close to the sensor input to the process racks as practical. This change is based on the BIST features of the ALS platform. The response to PSAI 9.a above describes the self-test and diagnostic features of the ALS input board, CLB, and output board and how they are comprehensive enough to provide equivalent assurance to injection of a simulated signal into the channel to verify operability.

The ALS platform is not being utilized in the SSPS logic portion of the protection system or the relay portion of the protection system. These portions of the protection system are not being changed as part of the PPS replacement project and are tested separately on-line using COTs or during refueling outages using channel calibrations and trip actuation device tests.

PSAI 11

Reliability and Availability Analysis - As discussed within Section 3.6, an applicant or licensee referencing this SE 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.

PG&E Response to PSAI 11

The PG&E FRS specified requirements for system reliability and states 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. A project specific DCPP PPS replacement ALS reliability analysis is contained in Westinghouse Document No. 6116-00029, "Diablo Canyon PPS ALS Reliability Analysis and FMEA." The reliability results are well within the reliability goals applicable for a safety-related protection system. In addition, as stated in Section 4.12.3 of the LAR Supplement contained in PG&E Letter DCL-13-043, a separate evaluation has been performed to support application of the existing TS and TS surveillance test intervals, that is contained in the Westinghouse Document, "Justification for the Application of Technical Specification Changes in WCAP-14333 and WCAP-15376 to the Tricon/ALS Process Protection System." The Westinghouse document provides a qualitative comparison of features important to the reliability of the Tricon and ALS subystems and the Eagle 21 system, and concludes the reliability is acceptable for the PPS replacement design based on the additional redundancy, diversity, and self-testing features that have been utilized.

As discussed in Section 4.7 of the LAR Supplement contained in PG&E Letter DCL-13-043, PG&E has performed a Diversity and Defense-in-Depth study of the PPS replacement in accordance with BTP 7-19, "Guidance for Evaluation of D3 in Digital Computer Based Instrumentation and Control Systems," Revision 5, March 2007, as well as the supplemental guidance provided by DI&C-ISG-02, "Task Working Group

#2: D3 Issues, Interim Staff Guidance," Revision 2, dated June 5, 2009. This has been approved by the NRC in a safety evaluation report (ADAMS Accession No. ML110480845).

The PG&E FRS specified requirements for system test and calibration, including that capability shall be provided for testing at power in either test in bypass mode (where the partial trip/actuation outputs associated with the channel in test are maintained in the non-tripped/non-actuated condition) or test in trip mode (where the partial trip/actuation outputs associated with the channel in test are maintained in the tripped/actuated condition).

PSAI 12

Application-specific ALS-102 Digital Communications - As discussed within Section 3.7.2.1, an applicant or licensee referencing this SE 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 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.

PG&E Response to PSAI 12

PG&E has specified ISG-04 be considered for the PPS replacement design, including the ALS subsystem. The LAR Supplement contained in PG&E Letter DCL-13-043, Sections 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.7, 4.8.18, 4.8.19, and 4.8.20 describe how the ALS subsystem meets ISG-04 staff points 2, 3, 4, 5, 7, 18, 19, and 20, respectively.

Also, application-specific ALS-102 Digital Communications between the safety-related ALS processor, its non-safety MWS, including compliance with applicable ISG-04 Interdivisional Communication points, and the Gateway Computer have been addressed in the responses to the following open item (RAI's):

68 (RAI 46)
69 (RAI 47)
71 (RAI 49)
73 (RAI 44)
96 (RAI 67)
106 (RAI 63)

PSAI 13

Application-specific TAB Communications - As discussed within Section 3.7.2.1, an applicant or licensee referencing this SE 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 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.

PG&E Response to PSAI 13

PG&E has specified in the IRS that ISG-04 be considered for the PPS replacement design, including the ALS subsystem. The LAR Supplement contained in PG&E Letter DCL-13-043, Sections 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.7, 4.8.8, 4.8.11, 4.8.12, and 4.8.18 describe how the ALS subsystem meets ISG-04 staff points 1, 2, 3, 4, 5, 7, 8, 11, 12, and 18 , respectively. For ISG-04 staff point 10, PG&E has requested a limited exception, as described in Section 4.8.10 of the LAR Supplement contained in PG&E Letter DCL-13-043 and the response to RAI 54 contained in this letter, based on the redundant and diverse feature of the ALS and administrative controls.

PSAI 14

Application-specific ALS-601 Digital Communications - As discussed within Section 3.7.2.1, an applicant or licensee referencing this SE 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 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.

PG&E Response to PSAI 14

As stated in the LAR Supplement contained in PG&E Letter DCL-13-043, Section 4.2.4.3, the PPS replacement application does not utilize the ALS-601 Communications Board.

PSAI 15

Application-specific Command Prioritization - As discussed within Section 3.7.2.2, an applicant or licensee referencing this SE 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 staff points 1 through 10 under the NRC staff position for command prioritization.

PG&E Response to PSAI 15

As stated in the LAR Supplement contained in PG&E Letter DCL-13-043, Section 4.8, the PPS replacement application does not utilize command prioritization.

PSAI 16

Application-specific Multidivisional Control and Display Stations - As discussed within Section 3.7.2.3, an applicant or licensee referencing this SE 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 Staff Position 3 for multidivisional control and display stations.

PG&E Response to PSAI 16

As stated in the LAR Supplement contained in PG&E Letter DCL-13-043, Section 4.8, the PPS replacement application does not utilize multidivisional control and display stations.

PSAI 17

Secure Development Environment for Applications - As discussed within Section 3.8, an applicant or licensee referencing this SE 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.

PG&E Response to PSAI 17

Section 4.13 of the LAR Supplement, contained in PG&E Letter DCL-13-043, discusses how the development environment of the ALS subsystem meets the criteria of RG 1.152.

Westinghouse Document No. 6002-00006, "ALS Security Plan," meets the guidance of NRC RG 1.152 and establishes the secure development and operational environment for the ALS portion of the PPS replacement design.

On September 24 through 26, 2012, the PG&E Cyber Security Supervisor accompanied members of the PG&E Quality Verification group to examine the ALS design and production facilities and examined the code production practices and the

development environment. They determined that a secure development environment in accordance with NRC RG 1.152, Revision 3, is being used.

PSAI 18

Secure Operational Environment - As discussed within Section 3.8, an applicant or licensee referencing this SE 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.

PG&E Response to PSAI 18

Section 4.13 of the LAR Supplement contained in PG&E Letter DCL-13-043 discusses how the operational environment of the ALS subsystem meets the criteria of RG 1.152.

PG&E DCPP Procedures CF2, Revision 8, "Computer Hardware, Software and Database Control," and CF2.ID2, Revision 10, "Software Configuration Management for Plant Operations and Operations Support," provide the DCPP station control procedures for software configuration management throughout the remaining life cycle phases under the control of PG&E after development and delivery of the software from the vendor to PG&E.

PG&E Document No. SCM 36-01, "Diablo Canyon Power Plant Units 1 & 2 Process Protection System (PPS) Replacement Software Configuration Management Plan (SCMP)," has been developed to establish and document a process of change control and software configuration management for the PPS replacement from the time the equipment arrives at the offsite PG&E Project Integration and Test Facility and for the remainder of its life cycle following installation at DCPP, including the operation phase and maintenance phase. The change management process includes software changes and aspects of PPS replacement component configuration necessary to meet secure operational environment and cyber security requirements.

Modification to the PPS Replacement components produced by the vendors, Westinghouse and Invensys, will be performed by the vendors. Verification and validation (V&V) will be controlled by the vendor's V&V plans created for the PPS replacement project (Document No. 6116-00003, "DCPP ALS V&V Plan," for Westinghouse and Triconex Document No. 993754-1-802, "PPS Replacement DCPP SWP," for Invensys).

PSAI 19

Demonstration of Adequate Diversity – As discussed within Section 3.9, an applicant or licensee referencing this "ALS Topical Report" SE should identify the approaches

specified to provide built-in diversity and mitigations against common cause failures (CCFs) 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.

PG&E Response to PSAI 19.a

Section 4.2.5.2 of the LAR Supplement contained in PG&E Letter DCL-13-043, discusses the use of embedded design diversity for the ALS subsystem used for the PPS replacement. The embedded design diversity is used for all safety functions processed by the ALS, including all channels used in each of the four protection sets.

The ALS platform development process for the DCPP PPS replacement utilizes Embedded Design Diversity with both Core "A" and Core "B." The arrangement of the independent designs is illustrated in LAR Figure 3-2. The IRS provides specific details, including I/O signal assignments that are contained in Appendices 4.1 through 4.4.

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.

PG&E Response to PSAI 19.b

Core diversity is used for all ALS processed functions in the PPS replacement, but no application-specific comparison checks are required for the design.

c. Fail Safe Behavior - Specifications should identify application-specific fail-safe behavior that should result from any comparison check mismatch.

PG&E Response to PSAI 19.c

Core diversity is used for all ALS processed functions in the PPS replacement, but no specific comparison checks are required for the design. As described in Section 4.2.5.2 of the LAR Supplement contained in PG&E Letter DCL-13-043, the diverse Core A and Core B execution path outputs are combined in hardwired logic 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 board 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.

PPS Replacement FRS, Rev 9, Sections 3.2.1.16.3 thru 3.2.1.16.6 specify preferred failure states for analog and discrete outputs. The preferred failure state for analog and discrete ALS outputs is specified in 6116-00011 Appendix A through Appendix D, if the output can be set.

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.

PG&E Response to PSAI 19.d

The DCPP PPS design includes systems that provide diversity for the PPS including the Nuclear Instrumentation System and the Anticipated Transient Without Scram Mitigation System. These systems are being retained for use with the PPS replacement. Section 4.7 of the LAR Supplement contained in PG&E Letter DCL-13-043, discusses the Diversity and Defense-in-Depth study for the PPS replacement. The PPS replacement Diversity and Defense-in-Depth study credits these systems to ensure the PPS safety functions are performed for all required failures to be considered.

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 CCFs, which are described in Section 3.3 of the "ALS Diversity Analysis" (Reference 46), 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 BTP 7-19 and DI&C-ISG-02, as applicable.

PG&E Response to PSAI 19.e

Section 4.7 of the LAR Supplement contained in PG&E Letter DCL-13-043, discusses the Diversity and Defense-in-Depth study for the PPS replacement, that was performed in accordance with guidance in BTP 7-19, "Guidance for Evaluation of D3 in Digital Computer Based Instrumentation and Control Systems," Revision 5, March 2007, and DI&C-ISG-02, "Task Working Group #2: D3 Issues, Interim Staff Guidance," Revision 2, dated June 5, 2009. The PPS replacement Diversity and Defense-in-Depth study addresses ALS software CCF through incorporating core diversity as well as additional, embedded design diversity in the FPGA-based hardware system and using qualified design practices and methodologies to develop and implement the hardware. The diverse ALS subsystem cannot be affected by a CCF that affects the Tricon subsystem. The proposed PPS provides sufficient

design diversity to automatically mitigate DCPP Final Safety Analysis Report Update Chapter 15 events.

f. Identification of Echelons of Defense – Applicant or licensee D3 Analysis should identify the echelon(s) of defense (i.e., control, RTS, ESFAS, and monitoring and display) within the plant that each ALS platform-based I&C function is assigned.

PG&E Response to PSAI 19.f

The Diversity and Defense-in-Depth study for the PPS replacement identifies the control, RTS, ESFAS, and monitoring and display information that are associated with the functions that are assigned to the ALS subsystem.

g. Diverse Manual Control Features - When manual controls are not provided as discrete hardwired components connected to the safety equipment at a point downstream of the plant's digital I&C safety system outputs, the applicant or licensee 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.

PG&E Response to PSAI 19.g

The DCPP protection system design utilizes existing manual controls in the Main Control Room. The PPS monitors plant parameters and generates initiating signals to the existing non-software based SSPS, which performs coincident logic functions and generates reactor trip signals and actuation signals to ESF devices. Manual controls are located downstream of the SSPS. Neither the SSPS nor the existing manual controls are affected by the PPS replacement; that is, the PPS replacement project does not alter the system level manual actuation configuration at DCPP. Sections 4.10.3.2.1, 4.10.3.2.2, and 4.10.3.2.3 of the LAR Supplement contained in PG&E Letter DCL-13-043 describe compliance of the PPS replacement manual controls with IEEE 603 Article 6.2.1, 6.2.3, and 6.2.2, respectively.

Further, as described in Section 4.2 and Figure 4-3 of the LAR Supplement, the DCPP SSPS has discrete hardwired manual switches that are not being modified by the PPS replacement design and will be available. These switches are downstream of the ALS output boards, which provide initiation signals to the SSPS as described above. Therefore, this PSAI is not applicable to the PPS replacement ALS subsystem.

PSAI 20

IEEE Std 603-1991 Compliance – As discussed within Section 3.10 of this safety evaluation, although the NRC staff determined that the ALS platform supports satisfying various sections and clauses of IEEE Std 603-1991, an applicant or

licensee that references this safety evaluation should identify the approach taken to fully satisfy 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. As such, this safety evaluation 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 safety evaluation, the applicant or licensee should demonstrate that the plant-specific and application-specific use of the ALS platform fully satisfies 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

Section 4.10 of the LAR Supplement contained in PG&E Letter DCL-13-043 discusses how the ALS subsystem meets the applicable clauses of IEEE Standard 603-1991.

PSAI 21

Demonstration of Sufficient Isolation - An applicant or licensee referencing this SE should identify all safety/nonsafety interfaces and interdivisional interfaces, and 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, as endorsed by RG 1.75 and in accordance with BTP 7-11, and DI&C-ISG-04, 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 covered by this SE.

PG&E Response to PSAI 21

Sections 4.2.13.2 and 4.2.13.3 of the LAR Supplement contained in PG&E Letter DCL-13-043 describe the ALS equipment communications and communications with the non-safety ALS MWS. There are no communication paths between redundant safety divisions in the ALS portion of the PPS replacement.

The EIA-422 ALS communication channel from each ALS chassis to the Gateway Computer is isolated, serial, one-way, as described in Section 2.2.1.3 of the ALS Topical Report and Section 3.9 of the ALS-102 Design Specification. The TxB1 communications channel does not receive any data, handshaking, or instructions

from the Gateway Computer. The ALS-102 CLB communication channel TxB1 is a communication link where the receive capability is physically disabled by hardware as described in Document No. 6002-10202, "ALS-102 Design Specification." The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 CLB is electrically incapable of receiving information from outside the ALS-102 via the Transmit Busses TxB1 and TxB2. Thus, the ALS does not require use of an isolation device to prevent communication back to the ALS from the Gateway Computer.

The EIA-422 TxB2 communication channel that transmits data to the non-safety-related MWS is also serial, one-way with no handshaking. The third ALS serial communications channel enables TAB functions between ASU maintenance software in the MWS and the ALS controller. This EIA-485 communication path is normally disabled, with two-way communications permitted only when the TAB communication link is physically connected between the TAB and the ALS MWS. Communications are not possible on the TAB if the communication link is physically disconnected.

Section 4.2.3.2 and 4.2.3.3 of the LAR Supplement contained in PG&E Letter DCL-13-043 describe the ALS I/O modules. The input channels are protected against electrostatic discharge (ESD) and surge voltages using transient voltage suppressors. Generally, all input channels are galvanically isolated from the ALS logic and the barriers can withstand more than 1500 Volts (V) root mean squared (rms) difference between the field domain and the digital domain.

The output channels are protected against ESD and surge voltages. All output boards have galvanic isolation between the channels and the ALS logic, and can withstand a minimum of 1500 V rms.

Section 4.2.13 of the LAR Supplement contained in PG&E Letter DCL-13-043 describes the ALS-102 CLB isolation. The Class 1E/non-1E data communication for the ALS-1 02 CLB is described in Sections 2.2.1.3 and 5.3.2 of the ALS Topical Report, and in Position 2 of Document No. 6116-00054. The electrical isolation of the transmit busses is performed by magnetic couplers located on the ALS-102 CLB. The TxB isolators are described in Section 3.9.1 of Document No. 6002-10202, "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 of the LAR Supplement contained in PG&E Letter DCL-13-043, 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," and will be documented in a supplemental test report to be issued at a future date.

PG&E will verify that the maximum test voltages applied to the ALS-102 during ALS qualification testing envelope the maximum credible voltages for the Non-Class 1E interfaces with the DCPP PPS.

PSAI 23

IEEE Std 1012-1998 Compliance – As discussed within Section 3.11.2.3.3 of this SE, although the NRC staff determined the ALS platform IV&V processes support various sections and clauses of IEEE Std 1012-1998, an applicant or licensee referencing this SE 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 this SE 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.

PG&E Response to PSAI 23

Section 4.5.6.3 of the LAR Supplement contained in PG&E Letter DCL-13-043 describes the software V&V performed for the ALS subsystem. Westinghouse Document No. 6116-00003, "DCPP ALS V&V Plan," defines the techniques, procedures, and methodologies that will be used to provide independent V&V in the design and test development of the FPGA design and test activities for the PPS replacement project. The ALS V&V Plan, Appendix A, contains an IEEE-1012 compliance table to describe how the criteria of the 1998 version of IEEE-1012 are implemented for the PPS replacement ALS subsystem.

NRC RAI 60

(Open Item 99) Virtual Channel - CSI document 6116-00054, "Diablo Canyon PPS ISG-04 Matrix", responses to ISG-04 Position 1, points 4 and 10 describe the use of Virtual Channel. Furthermore, the response to point 10 states that virtual channels are described in 6002-10206, "ALS-102 FPGA Design Specification" and their use in the ALS PPS subsystem are described in 6116-10201, "DC PPS ALS-102 FPGA Requirements Specification." However, the 6002-10206 document only provides general information on how a virtual channel can be used (for which implementation will be application specific). This information cannot be referenced in the DCPPS safety evaluation because it has not been docketed. In addition, this information is too generic, and it does not describe how Virtual Channels are used in the ALS

platform portion of the DCPPS replacement system. Thus, the staff requires detailed information on how virtual channels will be used for the DCPPS.

When trying to search and trace the requirement for the use of virtual channel, the Staff could not find information in either 6116-00011, "ALS PPS System Design Specification", or 6002-00010, "ALS Platform Requirements Specification". ALS document 6116-10201 only lists virtual channel in Table 6-7, which does not provide any description about use of ALS virtual channels for DC PPS replacement system. Thus, it is not clear what the original requirement is for this function, and how the design is being implemented for the DCPPS replacement system.

Please describe the ALS Virtual Channels, requirements, design specification, and how they are used for the ALS portion of the DCPPS replacement system. In addition, clarify the use of virtual channels to address points 4 and 10 of ISG-04, specifically for setpoint modification.

PG&E Response to RAI 60

A virtual channel is a set of logic functions on the ALS-102 board that provides filtering, scaling and data storage. The data can then be applied to comparator logic for processing output trip signals or for conversion to an output signal for indication. The resultants of the logic are applied to output slave boards that provide the interface with plant systems.

The ALS-102 board may assign logic paths within the system a virtual channel number. This assignment is used to allow the logic path to be placed into different operating modes, and to enable the writing of set points associated with the logic path by placing the virtual channel into calibrate mode. If the virtual channel can be controlled via the TAB interface the virtual channel must be placed into override mode which will allow the TAB to assume control of the virtual channel. The design of the custom system application will determine how many virtual channels are implemented, and which operating modes it can support (Section 3.2.3 of Document No. 6002-10206, "ALS-102 FPGA Design Specification").

Details on implementation of the virtual channels in the DCPP PPS replacement design are contained in Section 3 of Document No. 6116-10201, Revision 2, "Diablo Canyon Units 1 and 2 Process Protection System ALS-102 FPGA Requirements Specification."

A total of 18 Virtual Channels are processed by the ALS-102 logic, each having independent sets of configuration parameters and data registers. Each provides independent management of the logic path within one Reliable ALS bus (RAB) Time Frame. Each virtual channel supports a different set of I/O configurations. There are 13 individual process inputs to the ALS-102 board logic that form the 18 virtual channels. For each comparator function there is an associated virtual channel that

supports current loop analog inputs. Comparator resultants are applied to an output slave board for setting contact status and some channels also provide processing for 4-20 milliampere (mA) outputs. The remaining 7 virtual channels provide signal conditioning of RTD input values which are processed for 4-20 mA analog outputs. There are no comparator associated functions for these 7 virtual channels. Filtering and scaling are implemented on the input slave board (ALS-311).

Virtual channel logic functions are depicted in Appendix B of Document No. 6116-00011, "ALS PPS System Design Specification." The table below (reference Document No. 6116-10201, Table 3.2-6 ALS-102 "FPGA Requirements Specification") contains the virtual channel functionality, including which protection set is enabled (EN) for each channel, of the ALS-102 board for the Diablo Canyon PPS application.

The NVM holds the parameters necessary for the ALS-102 board to perform its required functions. The NVM contains an entry that has an enable bit for each of the 18 virtual channels. During the power-on configuration startup state, the ALS-102 board loads this entry from NVM and stores it into a local register. This register will determine which virtual channels are enabled and which are not. If a channel is not enabled, it will not process data, or set the error flags. If the contents of the NVM are corrupted, an error flag is set and the board will enter the halt state. The power on configuration startup state functions are described in more detail in Section 3.2.6.1 of Document No. 6116-10201, Revision 2.

If the logic path is enabled, the logic functions associated with each virtual channel (depicted in Appendix B of Document No. 6116-00011, "ALS PPS System Design Specification") are implemented while in Normal Mode.

When a virtual channel is in Normal mode, the channel data for the ALS-321 board is converted from current into engineering units (EU) and the results are stored in the Instrument Data Registers. The channel data for the ALS-311 board is filtered and converted to EU by the slave board, however, that input is also stored to the Instrument Data Register on the ALS-102 board.

A virtual channel can support the following ALS operating modes (see Section 3.2.3 of Document No. 6002-10206 and Section 2.1.7.1 of Document No. 6116-10201, "FPGA Requirements Specification"):

- Normal – The virtual channel processes its associated functional logic.
- Bypass – in this mode the channel is OOS – alarmed and the filtered/scaled value in the instrument data register is held at its last state (effectively As-Is). Note: this is an ALS-102 function and not to be confused with a Station (TS) "Bypass" which is directly associated with the state in which the contact output to SSPS is being maintained.

Virtual Channel I/O Configuration

VCH #	Virtual Channel Name	Protection Set				IO Channels		
		I	II	III	IV	Analog Input	Analog Output	Digital Output
1	RCS Flow Loop 1	EN	EN	EN	—	321-1/1	421-1/1 (A only)	402-2/1
2	RCS Flow Loop 2	EN	EN	EN	—	321-1/2	421-1/2 (A only)	402-2/2
3	RCS Flow Loop 3	EN	EN	EN	—	321-1/3	421-1/1 (B only)	402-2/3
4	RCS Flow Loop 4	EN	EN	EN	—	321-1/4	421-1/2 (B only)	402-2/4
5	PZR Pressure Low Reactor Trip	EN	EN	EN	EN	321-1/5	—	402-2/5
6	PZR Pressure High P-11	EN	EN	EN	—	321-1/5	—	402-2/6
7	PZR Pressure High Reactor Trip	EN	EN	EN	EN	321-1/5	—	402-2/7
8	PZR Pressure Low-Low SI	EN	EN	EN	EN	321-1/5	—	402-2/8
9	PZR Pressure High PORV	EN	EN	EN	EN	321-1/5	—	402-2/9
10	Containment Pressure High SI, Phase A Isolation	—	EN	EN	EN	321-1/6	—	402-2/10
11	Containment Pressure High-High Containment Spray, Phase B Isolation, Steamline Isolation	EN	EN	EN	EN	321-1/6	—	402-2/11
12	WR T_{HOT}	EN	EN	—	—	311-1/1	421-2/1	—
13	WR T_{COLD}	EN	EN	—	—	311-1/2	421-2/2	—
14	NR T_{COLD}	EN	EN	EN	EN	311-1/3	421-2/3	—
15	NR T_{HOT1}	EN	EN	EN	EN	311-1/4	421-2/4	—
16	NR T_{HOT2}	EN	EN	EN	EN	311-1/5	421-2/5	—
17	NR T_{HOT3}	EN	EN	EN	EN	311-1/6	421-2/6	—
18	PZR Vapor Temperature	—	—	—	EN A only	311-1/7	421-2/7 (A Only)	—

- Override – the channel is in ALS Bypass (OOS) and allows the Station (via 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; it does not override the slave board modes of operation.
- Calibrate – The channel is in ALS Bypass (OOS) and it allows updates to the tunable parameters in the NVM.

Regardless of the operating mode, a TAB read of the data registers will provide their current value. 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 (OOS) before being changed to Calibrate or Override (i.e., Normal to ALS Bypass to Calibrate or, Normal to ALS Bypass to Override mode). It is not possible to transit from either Override or Calibrate modes directly to Normal without returning to ALS Bypass mode. This ensures that any modifications or signal injection status can be verified/validated prior to returning the virtual channel to normal (inservice) operation. It also will ensure that the calibrate mode is exited for one virtual channel prior to establishing calibrate for another virtual channel.

For virtual channels with associated comparators, they shall not enter ALS-102 Bypass mode unless its corresponding digital output channel is in Digital Output Override mode (DOO) as depicted in Appendix B of Document No. 6116-00011. This ensures that the contact status to SSPS is held either in the non-Trip condition (Test-in-Bypass – Station TS Bypass condition - alarmed) or in the Trip condition (Test-in-Trip) to ensure that the virtual channel will not cycle the input to SSPS. The DOO mode of operation is an ALS-402-2 board function, independent from the ALS-102 virtual channel Modes.

The virtual channel Operating mode is stored in the NVM (reference Document No. 6116-10201, Rev 2 Section 3.2.6.3) 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 (OOS) mode and then be placed into Calibrate mode. During testing, the ALS-102 Board will identify the operating mode of the virtual channel using the Channel Operating Mode Register.

Functional logic diagrams that describe the PPS functions in terms of ALS components and functionality, and describe the virtual channels, are contained in Appendix B of Document No. 6116-00011, "ALS System Design Specification."

For the ALS-102 CLB TxB communications, Document No. 6116-00100 includes descriptions of the protocol used by the TxB1/TxB2 data stream, the contents of the data at the byte level and the format of the data included in the data stream. The data contained in the TxB originates from various data registers, described in the virtual channel section above, in the CLB of the ALS-102. The data is marshaled by the Finite State Machine (FSM) that processes the virtual channel to an independent FSM that processes the TxB communications via a unidirectional core specific mechanism. The Comm-Channel FSM periodically moves data to the ALS-102 communication channel interface module where it is then transmitted over the physical bus.

The two ALS-102 CLB TxB communication channels, as specified in Document No. 6002-10203 and 6002-10204, are identical in construction to an ALS-601 channel (Document No. 6002-60103 and 6002-60104), but have limited capability. The configuration settings in NVM consist of per-channel control settings for channel EN, baud rate, parity enable, parity type (even, odd), and number of stop bits (1, 2). The ALS-102 TxB communication channels, unlike the ALS-601 channels, do not have control settings for direction (RX, TX), transmit type (byte, packet), clone select, and clone enable. The ALS-102 TxB communications channels therefore operate in transmit-only, byte mode, with cloning disabled. Each channel is provided with an up-to 256x10-byte (first in first out) FIFO memory for buffering communication data passed between the register interface and the external communication interface. Transmit channels pass data from their channel data register to the channel's communication interface outputs buffering the data through the FIFO memory and providing channel integrity verification through the otherwise unused receive interface. The register transfer level (RTL) 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 Document No. 6116-00100, "Diablo Canyon Units 1 and 2 Process Protection System ALS-ASU Communication Protocol," is gathered by and written from the ALS-102's CLB into the communication channel interface module's register interface. This is a one way interface. The RTL that performs the data gathering and writing is a project specific implementation (Document No. 6116-10203, "Diablo Canyon PPS ALS-102 Core A FPGA Design Specification," and Document No. 6116-10204, "Diablo Canyon PPS ALS-102 Core B FPGA Design Specification").

In Core A, the sequencer marshals the data defined in Table 3-1 of Document No. 6116-00100 to the communication channel interface from the following sources: RAM for NVM data (including the virtual channel data: setpoint, dead-band, sensor input range minimum/maximum values, coefficients, and miscellaneous data), engineering units registers for processed input channel data in engineering units, and status registers for channel health and status. The marshalling is governed by a FSM to control a multiplexer of all the data sources. It is independent of the FSM that governs the loading of the virtual channel data from NVM (described in Section 6.2 of Document No. 6116-10201) to RAM (Parameter FSM, described in Section

6.10 of Document No. 6116-10203) and the safety function of the system (Main FSM, described in Section 8.5 of Document No. 6116-10203). The TxB Stream FSM is described in Section 6.12 of Document No. 6116-10203. Figure 6.4-1 of Document No. 6116-10203 contains a block diagram of the CLB depicting in part this entire mechanism. Once in the registers of the communication channel interface module, the data is pushed into FIFO memory (see Section 3.6.3 of Document No. 6002-10203) by the FIFO communication module (see Section 3.6.4 of Document No. 6002-10203) as it services write requests from the communication channel transmit interface (Section 3.6.2 of Document No. 6002-10203) and popped by the transmit communication module (Section 3.8 of Document No. 6002-10203) for transmission on the external transmit output. The receive communication module is used only for a self-checking comparison of the channel transmission. The FSM described in Section 3.8.4 of Document No. 6002-10203 governs the data transmission.

In Core B, the sequencer marshals the data defined in Table 3-1 of Document No. 6116-00100 to the communication channel interface through the channel logic module (described in Section 3.3.2.4 of Document No. 6116-10204). This is performed using RAM registers as described in Section 4.4.10 of Document No. 6116-10204 to store virtual channel and slave I/O data. RAM is implemented using two dual-port RAMs. A Table in RTL (described in Section 4.4.15.1 of Document No. 6116-10204) references the data and organizes it into a table consistent with the data content, format, and order specifications for communications output as defined in Appendix A of Document No. 6116-00100. A RAM request reads virtual channel bank data and ALS slave IO registers. Then the table sends this data to the TxB port. This function is performed through an RTL state machine described in Section 4.4.15.2 of Document No. 6116-10204 which periodically traverses the table from top to bottom presenting the data contents of each row to the TxB communications channels for transmission. It is independent of the FSM that governs the safety function of the system described in Section 4.4.11.3 of Document No. 6116-10204. Data is exported for transmission by using the internal RAB bus to write to the output registers in the channel interface module. This interface is documented in Document No. 6002-10206. The communication channels, as described in Section 7.3.3.2 of Document No. 6002-10204 are identical in construction to an ALS-601 channel (described in Document No. 6002-60104) but are configured to operate as transmit-only, byte mode, with cloning disabled. Per Document No. 6002-60104, once in the registers of the communication channel interface module, the data is pushed into FIFO memory (see Section 4.4.2.10 of Document No. 6002-60104) by the write interface (Section 4.4.2.5 of Document No. 6002-60104) as it services write requests from the register interface (Section 4.4.4 of Document No. 6002-60104) and popped by the transmit interface (Section 4.4.2.8 of Document No. 6002-60104) for transmission on the external transmit output. The receiver interface is used in transmit channels for external channel error checking only. The FSM described in Section 4.4.2.8.1 of Document No. 6002-60104 governs the data transmission.

NRC RAI 61

(Open Item 101) Environmental Qualification Documentation - Per ISG 6 Section D.5.1, the NRC staff needs to determine if the PPS equipment has been demonstrated to be able to operate within the specified environment. In order to do this the staff needs to have plant specific environmental data for the plant and specifically for the cable spreading room. The ISG 6 matrix (item 2.12) states that this information has been provided in the two vendor Topical Reports, however, these reports do not contain any plant specific data.

Please provide plant specific environmental condition data for normal operating conditions and the worst conditions expected during abnormal and accident conditions where the PPS equipment is expected to perform its safety function.

PG&E Response to RAI 61

The cable spreading rooms at DCPP are considered to be a mild environment. The required environmental conditions for design of the PPS replacement equipment are contained in Section 3.1.4 of the FRS, Revision 9.

The PPS replacement instrumentation is specified to be qualified for the following conditions:
Temperature: 40 to 104°F
Relative Humidity: 0 to 95 percent (non-condensing)
Pressure: Atmospheric
Radiation: N/A (mild environment)

The seismic requirements for the design of the PPS replacement Class I equipment are contained in Section 3.1.5 of the FRS, Revision 9. The PPS replacement Class I equipment is specified to be qualified to Seismic Category I levels by test, analysis, or a combination thereof. The seismic spectra for the PPS replacement Class I equipment were provided on the Sharepoint on February 12, 2014.

DCPP Final Safety Analysis Report Section 3.10.1 discusses the design requirement for the Hosgri earthquake qualification of the equipment and states guidance contained in IEEE Standard 344-1975, and NRC RG 1.100 was used where necessary. IEEE 344-1975, Section 3.5.3, states that if equipment damping is not known, a value of 5 percent is recommended. Therefore, a value of 5 percent damping is used for the PPS replacement Class I equipment.

NRC RAI 62

(Open Item 105) Interaction with other systems - In PG&E's response to IEEE 603 Clause 6.3 criteria, there is no mention of the effects of using shared sensor signals between the PPS and control systems such as the Digital Feedwater Control System

(DFWCS), or the Auxiliary Feedwater (AFW) system. The NRC staff recognizes that the general specifications for the replacement PPS are similar to the Eagle 21 system and that the PPS project would not adversely impact the compliance of the system to this criteria however, it is necessary for the NRC to confirm that the criteria is still being met.

Please provide a description of the effects of sensor failure for those systems that use common shared sensor data from the PPS.

PG&E Response to RAI 62

The effects of the sensor failure for those systems that use common shared sensor data from the PPS are contained in Table 1, "Effects of Sensor Failure," below.

Table 1 - Effects of Sensor Failure

	Inst. Loop	Description	Existing PPS Class I /Class II Isolation Measures	Current Measures to Prevent Control/Protection System Interaction from Shared Sensors [IEEE 603 Clause 6.3]	PPS Replacement Proposed Class I/Class II Isolation Measures	Proposed Measures to Prevent Control System Interaction from Shared Sensors
Set I	LM-459	PZR Level to PZR Level Control	EAO	MSS in Process Control System (PCS)	HWI on Transmitter Loop	Same as Current
	PM-455	PZR Pressure to PZR Pressure Control	EAO	SHSS in PCS	HWI on Transmitter Loop	Same as Current
	FM-512	Loop 1 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	FM-522	Loop 2 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	FM-532	Loop 3 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	FM-542	Loop 4 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-514	Loop 1 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-524	Loop 2 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-534	Loop 3 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current

Table 1 - Effects of Sensor Failure

	Inst. Loop	Description	Existing PPS Class I /Class II Isolation Measures	Current Measures to Prevent Control/Protection System Interaction from Shared Sensors [IEEE 603 Clause 6.3]	PPS Replacement Proposed Class I/Class II Isolation Measures	Proposed Measures to Prevent Control System Interaction from Shared Sensors
Set I	PM-544	Loop 4 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-505	Turbine Impulse Pressure to AMSAC (C-20)	CLI	NA [AMSAC governed by 10 CFR 50.62]	HWI on Transmitter Loop	Same as Current
	LM-529	SG 2 Level to LI-529 (VB3), DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-539	SG 3 Level to LI-539 (VB3), DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-539	SG 3 Level to AMSAC	CLI	NA [AMSAC governed by 10 CFR 50.62]	2nd HWI on Transmitter Loop	Same as Current
Set II	LM-460	PZR Level to PZR Level Control	EAO	MSS in PCS	HWI on Transmitter Loop	Same as Current
	PM-456	PZR Pressure to PZR Pressure Control	EAO	SHSS in PCS	HWI on Transmitter Loop	Same as Current
	FM-513	Loop 1 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	FM-523	Loop 2 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current

Table 1 - Effects of Sensor Failure

	Inst. Loop	Description	Existing PPS Class I /Class II Isolation Measures	Current Measures to Prevent Control/Protection System Interaction from Shared Sensors [IEEE 603 Clause 6.3]	PPS Replacement Proposed Class I/Class II Isolation Measures	Proposed Measures to Prevent Control System Interaction from Shared Sensors
Set II	FM-533	Loop 3 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	FM-543	Loop 4 Steamflow to DFWCS	EAO	SFA in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-515	Loop 1 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-525	Loop 2 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-535	Loop 3 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-545	Loop 4 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	LM-519	SG 1 Level to LI-519 (VB3), DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-549	SG 4 Level to LI-549 (VB3), DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-549	SG 4 Level to AMSAC	CLI	NA [AMSAC governed by 10 CFR 50.62]	2nd HWI on Transmitter Loop	Same as Current

Table 1 - Effects of Sensor Failure

	Inst. Loop	Description	Existing PPS Class I /Class II Isolation Measures	Current Measures to Prevent Control/Protection System Interaction from Shared Sensors [IEEE 603 Clause 6.3]	PPS Replacement Proposed Class I/Class II Isolation Measures	Proposed Measures to Prevent Control System Interaction from Shared Sensors
Set II	PM-506	Turbine Impulse Pressure to AMSAC (C-20)	CLI	NA [AMSAC governed by 10 CFR 50.62]	HWI on Transmitter Loop	Same as Current
Set III	LM-461	PZR Level to PZR Level Control	EAO	MSS in Process Control System (PCS)	HWI on Transmitter Loop	Same as Current
	PM-457	PZR Pressure to PZR Pressure Control	EAO	SHSS in PCS	HWI on Transmitter Loop	Same as Current
	PM-526	Loop 2 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-536	Loop 3 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	LM-518	SG 1 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-528	SG 2 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-528	SG 2 Level to AMSAC	CLI	NA [AMSAC governed by 10 CFR 50.62]	2nd HWI on Transmitter Loop	Same as Current

Table 1 - Effects of Sensor Failure

	Inst. Loop	Description	Existing PPS Class I /Class II Isolation Measures	Current Measures to Prevent Control/Protection System Interaction from Shared Sensors [IEEE 603 Clause 6.3]	PPS Replacement Proposed Class I/Class II Isolation Measures	Proposed Measures to Prevent Control System Interaction from Shared Sensors
Set III	LM-538	SG 3 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-548	SG 4 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
Set IV	PM-474	PZR Pressure to PZR Pressure Control	EAO	SHSS in PCS	HWI on Transmitter Loop	Same as Current
	PM-516	Loop 1 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	PM-546	Loop 4 Steamline Pressure to DFWCS	EAO	MSS in DFWCS	HWI on Transmitter Loop	Same as Current
	LM-517	SG 1 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-517	SG 1 Level to AMSAC	CLI	NA [AMSAC governed by 10 CFR 50.62]	2nd HWI on Transmitter Loop	Same as Current
	LM-527	SG 2 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current
	LM-537	SG 3 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current

Table 1 - Effects of Sensor Failure

	Inst. Loop	Description	Existing PPS Class I /Class II Isolation Measures	Current Measures to Prevent Control/Protection System Interaction from Shared Sensors [IEEE 603 Clause 6.3]	PPS Replacement Proposed Class I/Class II Isolation Measures	Proposed Measures to Prevent Control System Interaction from Shared Sensors
Set IV	LM-547	SG 4 Level to DFWCS, AFW	EAO	DFWCS: MSS AFW: MSS in PCS	HWI on Transmitter Loop	Same as Current

Table 1 Glossary:	
AFW	Auxiliary Feedwater Control System
CLI	Eagle 21 Current Loop Isolator: an analog device, independent of Eagle 21 digital processing
DFWCS	Digital Feedwater Control System
EAO	Eagle Analog Output: dependent on Eagle 21 digital processing.
HWI	Hardwired isolation device: independent of PPS replacement digital processing.
Inst. Loop	Instrument Loop
Median Signal Selector (MSS)	The MSS selects the median (middle) value of three inputs for control. The MSS eliminates the possibility that a failed sensor or channel (failed in either the high, mid-scale or low direction) will cause a transient that would require mitigation by a protection channel sharing the failed sensor or channel.
PCS	Process Control System

Second High Signal Selector (SHSS)	The SHSS selects the second highest value of four inputs for control. The SHSS prevents a failed sensor or channel from causing a control system transient that would require mitigation by a protection channel sharing the failed sensor or channel.
Steam Flow Arbitrator (SFA)	The SFA determines an appropriate control signal output based on (1) the two steam flow channels for each steam generator; and (2) an estimate of steam flow based on main turbine first stage pressure to prevent a transient caused by a failed sensor or channel that would require mitigation by a protection channel sharing the failed sensor. The SFA computes the average of its two input signals. If the two input channels differ by more than a specified amount, the value that is closest to an expected (arbitration) value of steam flow based on turbine impulse chamber pressure will be used for control. If neither of the two input channels is within a specified amount of the arbitration signal, the arbitration signal itself will be used for control.

NRC RAI 63

(Open Item 106) Describe the mechanism of the ALS-102 board's transmission logic to restrict one way communication (i.e., only configuration data added to specify the points going over the TxB communication link) and how it cannot impact the safety function logic embedded in the ALS-102.

PG&E Response to RAI 63

The ALS-102 TxB busses are unidirectional communication links that have the same properties as described for the ALS-601 communication board, except for the location of the communication hardware. The ALS-102 communication hardware is located within the CLB FPGA, but is implemented with independent logic circuits. The communication logic circuit does not interact with the safety function logic circuit; rather it is non-intrusively monitoring the safety function logic circuit. A failure of the TxB communication circuit cannot prevent the performance of the safety function.

The two ALS-102 CLB TxB communication channels, as specified in Document No. 6002-10203 and 6002-10204, are identical in construction to an ALS-601 channel (Document No. 6002-60103 and 6002-60104), but have limited capability. The configuration settings in NVM consist of per channel control settings for channel EN, baud rate, parity enable, parity type (even, odd), and number of stop bits (1, 2). The ALS-102 TxB communication channels, unlike the ALS-601 channels, do not have control settings for direction (RX, TX), transmit type (byte, packet), clone select, and clone EN. The ALS-102 TxB communications channels operate in transmit-only, byte mode, with cloning disabled. Each channel is provided with an up-to 256x10-byte FIFO memory for buffering communication data passed between the register interface and the external communication interface. Transmit channels pass data from their channel data register to the channel's communication interface outputs buffering the data through the FIFO memory and providing channel integrity verification through the otherwise unused receive interface. The RTL 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 Document No. 6116-00100, "Diablo Canyon Units 1 and 2 Process Protection System ALS-ASU Communication Protocol," is gathered by and written from the ALS-102's CLB into the communication channel interface module's register interface. This is a one way interface. The RTL that performs the data gathering and writing is a project specific implementation (Document No. 6116-10203, "Diablo Canyon PPS ALS-102 Core A FPGA Design Specification," and Document No. 6116-10204, "Diablo Canyon PPS ALS-102 Core B FPGA Design Specification").

In Core A, the sequencer marshals the data defined in Table 3-1 of Document No. 6116-00100 to the communication channel interface from the following sources:

RAM for NVM data (including the virtual channel data: setpoint, dead-band, sensor input range minimum/maximum values, coefficients, and miscellaneous data), engineering units registers for processed input channel data in engineering units, and status registers for channel health and status. The marshalling is governed by a FSM to control a multiplexer of all the data sources. It is independent of the FSM that governs the loading of the virtual channel data from NVM (described in Section 6.2 of Document No. 6116-10201) to RAM (parameter FSM, described in Section 6.10 of Document No. 6116-10203) and the safety function of the system (main FSM, described in Section 8.5 of Document No. 6116-10203). The TxB stream FSM is described in Section 6.12 of Document No. 6116-10203. Figure 6.4-1 of Document No. 6116-10203 contains a block diagram of the CLB depicting in part this entire mechanism. Once in the registers of the communication channel interface module, the data is pushed into FIFO memory (see Section 3.6.3 of Document No. 6002-10203) by the FIFO communication module (see Section 3.6.4 of Document No. 6002-10203) as it services write requests from the communication channel transmit interface (Section 3.6.2 of Document No. 6002-10203) and popped by the transmit communication module (Section 3.8 of Document No. 6002-10203) for transmission on the external transmit output. The receive communication module is used only for a self-checking comparison of the channel transmission. The FSM described in Section 3.8.4 of Document No. 6002-10203 governs the data transmission.

In Core B, the sequencer marshals the data defined in Table 3-1 of Document No. 6116-00100 to the communication channel interface through the channel logic module (described in Section 3.3.2.4 of Document No. 6116-10204). This is performed using RAM registers as described in Section 4.4.10 of Document No. 6116-10204 to store virtual channel and slave I/O data. RAM is implemented using two dual-port RAMs. A Table in the RTL (described in Section 4.4.15.1 of Document No. 6116-10204) references the data and organizes it into a table consistent with the data content, format, and order specifications for communications output as defined in Appendix A of Document No. 6116-00100. A RAM request reads virtual channel bank data and ALS slave IO registers. Then the table sends this data to the TxB port. This function is performed through an RTL state machine described in Section 4.4.15.2 of Document No. 6116-10204, which periodically traverses the table from top to bottom presenting the data contents of each row to the TxB communications channels for transmission. It is independent of the FSM that governs the safety function of the system described in Section 4.4.11.3 of Document No. 6116-10204. Data is exported for transmission by using the internal RAB bus to write to the output registers in the channel interface module. This interface is documented in Document No. 6002-10206. The communication channels, as described in Section 7.3.3.2 of Document No. 6002-10204, are identical in construction to an ALS-601 channel (described in Document No. 6002-60104) but are configured to operate as transmit-only, byte mode, with cloning disabled. Per Document No. 6002-60104 once in the registers of the communication channel interface module, the data is pushed into FIFO memory (see Section 4.4.2.10 of Document No. 6002-60104) by

the write interface (Section 4.4.2.5 of Document No. 6002-60104) as it services write requests from the register interface (Section 4.4.4 of Document No. 6002-60104) and popped by the transmit interface (Section 4.4.2.8 of Document No. 6002-60104) for transmission on the external transmit output. The receiver interface is used in transmit channels for external channel error checking only. The FSM described in Section 4.4.2.8.1 of Document No. 6002-60104 governs the data transmission.

Document No. 6116-00100 includes descriptions of the protocol used by the TxB1/TxB2 data stream, the contents of the data at the byte level, and the format of the data included in the data stream.

NRC RAI 64

(Open Item 110) Safe State Definition - Section 4.2.5.2 of the LAR (Page 64) states that "the redundancy checker compares outputs and critical internal states from the two cores and will drive the board to a safe state if the outputs of the cores do not agree."

The NRC staff reviewed the FRS and Interface Requirement Specification (IRS) documents to determine what the "safe state" is for any given ALS function, but was unable to identify licensee specifications that define what these safe states represent. The NRC staff determined that the fail safe states are defined in the ALS FPGA specifications (6116-10201); however, it is not clear how the system vendors determined the fail safe states, if they were not derived from licensee input (i.e. FRS and IRS). If the system safe states are not defined by the licensee, then please explain the basis used by the vendor to determine what the safe states are for each ALS function.

PG&E Response to RAI 64

Additional information regarding requirements for fail safe states has been provided to the vendors in the FRS, Revision 9, Sections 3.2.1.16.3 thru 3.2.1.16.6:

For deenergize to trip comparator outputs (which includes all except the Containment Pressure High-High Engineered Safety Feature):

> Deenergize to trip comparator outputs shall be designed such that upon loss of electrical power, the resultant output is the tripped (deenergized) condition (Section 3.2.1.16.3 of FRS, Revision 9).
>
> Detectable failures that could result in loss of ability to perform a required safety function should result in affected deenergize to trip comparators being placed in the tripped (deenergized) condition (Section 3.2.1.16.5 of FRS, Revision 9). This requirement does not apply to functions that are OOS.

For the Energize to Trip Comparator Functions (Containment Pressure High-High Engineered Safety Feature):

> Energize to trip comparator outputs shall be designed such that upon loss of electrical power, the resultant output is the non-tripped (deenergized) condition (Section 3.2.1.16.4 of FRS, Revision 9).
>
> Detectable failures that could result in loss of ability to perform a required safety function should result in affected energize to trip comparators being placed in the non-tripped (deenergized) condition (Section 3.2.1.16.6 of FRS, Revision 9). This requirement does not apply to functions that are OOS.

Note that FRS specifications 3.2.1.16.5 and 3.2.1.16.6 are "should" specifications and not "shall" specifications, since the type of failure is undefined. Some failures could result in the inability of the affected system to place the output in the desired mode.

The fail-safe status applies to both the channel and board levels, which are each described below.

Channel Level

The ALS-102 CLB application logic is designed to set the associated partial trip digital output to the deenergized state (tripped for deenergize to trip functions as specified in FRS, Revision 9 Sections 3.2.1.16.3 and 3.2.1.16.5, and non-tripped for energize to trip functions as specified in FRS, Revision 9, Sections 3.2.1.16.4 and 3.2.1.16.6 via the digital output channel health function upon a loss of power or upon detection of an ALS diagnostic fault that results in the loss of capability to actuate the partial trip output.

The ALS-102 application logic is designed to set any associated analog output to 0.0 mA as specified in IRS, Revision 9, Section 1.5.5.10, via the analog output channel health function upon a loss of power or upon detection of a diagnostic fault that results in the loss of capability to drive the analog output.

Board Level

The ALS-102 digital output channels, ALS-402 digital output channels, and the ALS-421 analog output channels "Fail As Defined" on a per channel basis upon detection of a diagnostic fault that results in the loss of capability to drive the associated digital output or analog output. However, in one case (Halt Mode), the boards simply stop processing, and all output channels fail "As-Is". The "Fail As Defined" state is the fail-safe state specified in Sections 3.2.1.16.5 and 3.2.1.16.6 of the FRS and Section 1.5.5.10 of the IRS.

NRC RAI 65

(Open Item 111) ALS Manual Alarm Bypass Function - In the FPGA Requirements Specification (6116-10201 page 4-13) R4082 states that the Bypass alarm logic will be bypassed when the channels logic enable is not set. The rational provided is that the trip command is not being calculated so there would presumably be no need to actuate the alarm. This requirement seems to contradict requirement R4130 which requires alarm reflash as well as Clause 5.8.3 of IEEE 603.

Please provide an explanation of the benefit of providing this means of defeating the alarm bypass logic. The staff feels that operators should be aware of the bypass status of each safety channel regardless of whether the safety function is operable or not. The staff is also concerned that situations could exist when the operator could be misled into believing that a channel is not bypassed (because of the cleared alarm) when in fact the channel bypass switch is in bypass.

PG&E Response to RAI 65

The logic associated with a virtual channel may be completely inhibited based on the state of the logic enable (EN) flag stored in the associated ALS-102 board NVM. The logic EN flag is based on the configuration of the protection set which the ALS-102 board is controlling. All four protection sets require a unique logic EN flag configuration for the ALS-102 board. Table 3-5 of the Document No. 6116-00072 contains the logic EN flags utilized for each ALS-102 board.

An EN block as documented per the FPGA requirements specification, Document No. 6116-10201, Revision 2, will enable/disable the logic contained within the block. Document No. 6116-10201, Revision 2, has been updated to include that the EN block is enabled or disabled only via the logic EN flag from the associated NVM. The logic EN flag can be changed only on the bench using the applicable programming tools and cannot be changed dynamically while the ALS chassis is in service.

The use of a logic EN flag allows for one FPGA design to be used across protection sets with different logic configurations. For example there are a total of 18 virtual channels programmed on the ALS-102 FPGA, but none of the protection sets utilizes all 18 virtual channels. They all utilize a different subset of the 18 virtual channels. Those that are not utilized are disabled by setting the EN Block bit to 0 in the associated NVM.

NRC RAI 66

(Open Item 95) TAB Communication - Sections 3.2.2.5 and 4.2.13.2 of the updated LAR describe the TAB communication between the ALS and the ALS MWS.

Furthermore, Section 4.8.3 of the updated LAR, item b, states that the TAB communication is enabled through the use of the TAB access connector. The information provided in these sections implies that the TAB has to be enabled to communicate with the MWS. It is understood that the communication link has to be physically connected between the TAB and the ALS MWS for communication to occur. However, it is not clear if other means are included to enable TAB communication. Specifically, The ALS Platform Specification states: "If needed by the application a Communication Enable key switch may be located between the ASU and the ALS rack."

Westinghouse Electric Company/CS Innovations (WEC/CSI) document 6116-00011, ALS PPS System Design Specification, describes the use of the communication enable switch. Specifically, SDS-081 states that the ALS is connected to the ASU through the link when enabled through a key switch. However, PG&E's response to RAI-17 states that the ALS subsystem of the DCPPS will not use a key switch to enable and disable external TAB communications; and that TAB communication will be enabled by physically connecting the data link. This response contradicts the information provided in the updated LAR, Section 4.8., item b, which states "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."

Please clarify how TAB communication will be enabled for the ALS subsystem of the DCPP PPS, and whether an ALS key switch will be used.

PG&E Response to RAI 66

In order for the TAB to communicate with the MWS, the communication link has to be physically connected between the TAB and the ALS MWS as stated in Sections 3.2.2.5 and 4.2.13.2 of the LAR Supplement contained in PG&E Letter DCL-13-043. The Section 4.8.8 (page 129) sentence of the LAR Supplement that states, "To enable the TAB to the interface to the MWS requires the setting of a hardware key-lock switch," was inadvertently not revised during preparation of the LAR Supplement to be consistent with Sections 3.2.2.5 and 4.2.13.2 that were revised to state, "To enable the TAB to the interface to the MWS requires the communication link to be physically connected between the TAB and the ALS MWS."

The ALS System Design Specification, design statement item 81 (SDS-081), referenced in this question is from ALS Document No. 6116-00011, Revision 0. ALS Document No. 6116-00011 has been revised to Revision 1. Item SDS-081 in Document No. 6116-00011, Revision 1, states in part, "through a keyswitch or similar connection method." The PPS replacement design, that requires the MWS communication link to be physically connected between the TAB and the ALS MWS to enable the TAB, is considered a similar connection method and therefore meets the item SDS-081 in Document No. 6116-00011, Revision 1.

NRC RAI 67

(Open Item 96) ALS Parameter Display - Section 4.2.13.5 of the updated LAR describes the ALS Parameter Display function. This section states that this function will acquire data from the ALS via the TxB2 bus. However, the 2nd paragraph in this section states that this function will "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." It is not clear how the ALS Parameter Display function will provide access to the ALS controllers for performing maintenance operations. If this function is gathering data through TxB2, it can't access the ALS-102 controller. Furthermore, access from the MWS to the ALS is only through the TAB communication, when the communication link is connected. Please clarify if the ALS Parameter Display function can access the ALS controller.

PG&E Response to RAI 67

The phrase, "...and for providing user controlled access to the ALS controllers for performing maintenance operations such as calibration..." is not applicable. The ALS MWS parameter display function access to the ALS controller is read-only.

The MWS provides a strictly passive parameter display function using one-way ALS-102 EIA-422 Transmit Bus TxB2. The ALS parameter display function allows the MWS to display parameters transmitted to it on-line by the one-way TxB2 transmit bus described in ALS Topical Report Section 2.2.1.3. The MWS RS-422 serial communication port is a dedicated serial port that is connected to the ALS-102 unidirectional one-way TxB2 output in each ALS Core A and Core B chassis. Communications between the ALS and the ALS MWS via TxB2 are strictly one-way from the ALS-102 CLB to the ALS MWS. The TxB1 and TxB2 are EIA-422 communication links in which receive capability is physically disabled by hardware as described in the ALS-102 CLB Document No. 6002-10202, design specification. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 CLB is physically and electrically incapable of receiving external messages via the Transmit Busses TxB1 and TxB2. Two-way communications between the ALS MWS and the ALS-102 CLB are possible only when the TAB has been physically connected and enabled. The roles of the transmit busses and TAB are clarified on page 97 in the same section of the LAR Supplement, PG&E Letter DCL-13-043, beginning with the heading, "ALS to ALS MWS Communications."

NRC RAI 68

(Open Item 112) The licensee discussed having the option of connecting a thumb drive to the MWS, in addition to connecting a printer, in order to allow technicians to print-to-file. Please clarify if a thumb drive will be connected to the MWS, and if so,

what procedures will be implemented to maintain and secure the thumb drive. Please clarify how unused ports in the MWSs will be controlled.

PG&E Response to RAI 68

As described in PG&E Letter DCL-13-043, Section 4.2.14, the two keyboard video mouse (KVM) switched Universal Serial Bus (USB) ports will be used for the touchscreen interface device and a printer. One printer per protection set will utilize the KVM switch USB-2 port. The touchscreen peripheral will utilize the USB-1 port. Therefore, all KVM switch USB ports will be occupied, precluding connecting a USB drive to the KVM switch to transfer data.

Also, as described in PG&E Letter DCL-13-043, Section 4.2.14, "...unused MWS and KVM switch ports will be addressed in accordance with the DCPP CSP... The local printer for each protection set will ... be controlled by the PG&E SCMP..."

Diagnostic data files generated by the Tricon MWS computer may be transferred out of the MWS computer for processing on an external system, when necessary, using available MWS USB port(s). The transfer of data files using the MWS USB port(s) will be controlled by the DCPP Code of Safe Practices (CSP).

NRC RAI 69

(Open item 113) In the response provided to RAI 48, the licensee only addressed control of the USB ports of the Keyboard Video Mouse (KVM) switch. The KVM switch user guide states control of the switch can be performed using external switching control RC4 remote, RS-232 or input lines through the options port. The IRS Rev. 9, item 2.3.7.1 item (1) does not identify that the KVM switch can be controlled remotely. The LAR states that a custom serial cable is required to use the options port. Please confirm if PG&E expects to use the options port to control the KVM switch.

The KVM user guide states the KVM switch can be locked with a password to restrict access to the MWS connected. Please clarify if PG&E will use this feature. The KVM switch includes an autoscan mode switch, which allows the KVM to cycle through the MWS during a defined period. Please clarify if PG&E will use this feature.

PG&E Response to RAI 69

Per PG&E Letter DCL-13-043, Section 4.2.14, "The IRS ... includes specifications to control the type of connection and operation modes of the KVM switch ... Section 2.3.7 of the IRS ... states the AV4PRO-VGA KVM switch shall utilize the default switching mode..." Therefore, PG&E is not using the options port to control the KVM switch. Further, PG&E is not using the KVM switch password protection feature to

restrict access to the MWS and is not using the KVM switch autoscan mode switch to allow the KVM to cycle through the MWS during a defined period.

NRC RAI 70

(Open Item 114) The LAR, Section 4.8.10, notes; when the Tricon keyswitch is in the STOP mode, the application program will not halt. It is not clear why this setting was selected, when the safety evaluation for the Tricon V10 requires the keyswitch to be in the STOP position to remove a module and perform maintenance or firmware upgrade, as well as imposing administrative controls to perform such functions. Please explain the reasoning for not halting the application program when in STOP mode. Please describe how PG&E will halt operation of the main chassis to support maintenance or firmware upgrade activities.

PG&E Response to RAI 70

Disabling program halt on STOP in the application is an Invensys requirement contained in the Triconex Application Guide, Appendix B of the V10 Tricon Topical Report, which the NRC reviewed, but did not approve as part of the V10 Tricon Topical Report Safety Evaluation Report. The Triconex Application Guide, Section 3.11, Operational Constraints item B states: "The STOP position on the keylock switch shall be disabled in the system software configuration to preclude inadvertently stopping the program while performing software maintenance functions."

The Tricon V10 Safety Evaluation Report, Sections 3.7.3.1.2 (page 78) and 3.7.3.1.0 (page 87) states that it is necessary to remove a Tricon module from the chassis and take the controller OOS (keyswitch to STOP) to upgrade firmware. However, placing the keyswitch in STOP will have no effect because the STOP switch is disabled in the application software in accordance with the Tricon V10 Application Guide. Should it be necessary to halt operation of the main Tricon chassis, the controller keyswitch is placed in PROGRAM and the main processors (MP) are halted from the Tricon MWS via the TS1131 program.

Firmware upgrade is expected to be an infrequent evolution that is unlikely to be performed on-line. Should MP firmware upgrade be necessary, then PG&E will halt the processors in the affected Tricon chassis and replace them with MP that have been upgraded by Triconex.

The Tricon V10 Safety Evaluation Report does not require the Tricon chassis to be removed from service for replacement of a module in kind; i.e., if the module firmware is not being updated. PG&E normally will not take a Tricon chassis OOS to perform maintenance such as in-kind MPU or I/O module replacement. The Tricon is designed with hot swap capability to maintain its safety function upon removal and

replacement of an inactive I/O module or one or two redundant MP modules as described in Triconex Application Guide, Section 3.11.C.

Regulatory Commitments

Commitment # 1

If the routine maintenance activity that is being performed is associated with NR RTD signal processing within the affected ALS Core Chassis, TS 3.3.1 and TS 3.3.2 actions will be entered as appropriate.

Commitment # 2

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 OOS, as previously discussed in PG&E Letter DCL-13-043 Section 4.12, and the routine maintenance activity resulting in the Core Chassis OOS condition is not associated with NR RTD signal processing. If an ALS Core Chassis is OOS in Protection Sets I and II, TS 3.3.3 Condition A will be entered as a minimum per PG&E Letter DCL-13-043 Section 4.12.

Commitment #3

PG&E will verify that the maximum test voltages applied to the ALS-102 during ALS qualification testing envelope the maximum credible voltages for the Non-Class 1E interfaces with the DCPP PPS.

Commitment #4

The response to the ALS PSAIs 4, 5, 6, 8, 10, 20, and 22 requires additional input from Westinghouse on the detailed ALS design to fully address the PSAI. The documentation to identify how ALS PSAIs 4, 5, 6, 8, 10, 20, and 22 to address RAI 59 will be submitted by August 30, 2014.

Commitment #5

Diagnostic data files generated by the Tricon MWS computer may be transferred out of the MWS computer for processing on an external system, when necessary, using available MWS USB port(s). The transfer of data files using the MWS USB port(s) will be controlled by the DCPP CSP.