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

August 7, 2012

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

SUBJECT: DIABLO CANYON POWER PLANT, UNITS 1 AND 2 - 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)

Dear Mr. Halpin:

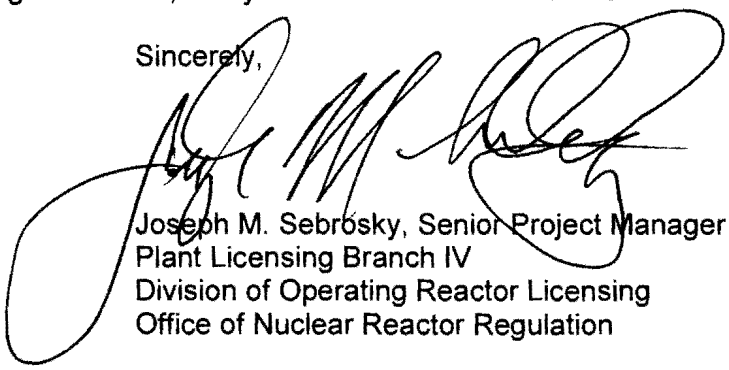
By letter dated October 26, 2011, as supplemented by letters dated December 20, 2011, and April 2, April 30, and June 6, 2012 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML113070457, ML113610541, ML12094A072, ML12131A513, and ML12170A837, respectively), Pacific Gas and Electric (PG&E, the licensee), requested the U.S. Nuclear Regulatory Commission (NRC) staff's approval of an amendment for the Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP). The proposed license amendment request would provide a digital replacement of the Process Protections System portion of the Reactor Trip System and Engineered Safety Features Actuations System at DCPP.

The NRC staff has reviewed the information provided by the licensee and determined that additional information is needed to complete its review. Enclosed is a request for additional information (RAI) for your consideration and response. Please note that review efforts on these tasks (TAC No. ME7522 and ME7523) are continuing and additional RAIs will be submitted.

These RAIs were discussed with the licensee on August 1, 2012. It was agreed that a formal response will be provided 45 days from the date of this letter. The NRC staff has determined that no security-related or proprietary information is contained in the RAIs.

If you have any questions regarding this matter, I may be reached at 301-415-1132.

Sincerely,



Joseph M. Sebrosky, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

Enclosure:
As stated

cc w/encl: Distribution via Listserv

REQUEST FOR ADDITIONAL INFORMATION

LICENSE AMENDMENT REQUEST FOR DIGITAL REPLACEMENT OF

THE PROCESS PROTECTION SYSTEM PORTION OF THE REACTOR TRIP

SYSTEM AND ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

DIABLO CANYON POWER PLANT, UNIT NOS. 1 AND 2

DOCKET NOS. 50-275 AND 50-323

By letter dated October 26, 2011, as supplemented by letters dated December 20, 2011, and April 2, April 30, and June 6, 2012 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML113070457, ML113610541, ML12094A072, ML12131A513, and ML12170A837, respectively), Pacific Gas and Electric (PG&E, the licensee), requested the U.S. Nuclear Regulatory Commission (NRC) staff's approval of an amendment for the Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP). The proposed license amendment request (LAR) would provide a digital replacement of the Process Protections System (PPS) portion of the Reactor Trip System (RTS) and Engineered Safety Features Actuations System (ESFAS) at DCPP.

The NRC staff has reviewed the information provided by the licensee and determined that the following additional information is needed to complete its review. Each request for additional information begins with a reference to an Open Item (OI). The OI number that follows corresponds to the number of the item in the open item table that the NRC staff has discussed with the licensee during various public meetings. An example of the Open Item table can be found in the meeting summary dated June 27, 2012 (ADAMS Accession No. ML12170A866).

1. (OI 6) LAR Sections 4.6, 4.10.2.4, and 4.11.1.2 provide insufficient information on the plant-specific application environmental factors. The Tricon V10 Safety Evaluation (ADAMS Accession No. ML11298A246), Section 6.2 lists 19 application-specific actions items (ASAIs) that the licensee should address for plant-specific applications. The licensee should address each of these for the Tricon portion of the PPS replacement. Similar information for the Advanced Logic System (ALS) portion of the PPS replacement will also be required.

2. (OI 10) Plant Variable PPS Scope - In the Description section of the LAR, Section 4.1.3, nine plant variables are defined as being required for RTS and Section 4.1.4 lists seven plant variables that are required for the ESFAS. Three additional plant variables were also listed in Section 4.10.3.4.

   Some variables are not listed in Section 4.10.3.4 as being PPS monitored plant parameters. It is therefore assumed that these parameters are provided as direct inputs to the solid state protection system (SSPS) and that the PPS is not relied upon for the completion of required reactor trip or safety functions associated with them. Provide additional information to confirm that these plant parameters and associated safety

functions will continue to operate independently from the PPS and that the replacement PPS will not adversely impact the system's ability to reliably perform these functions.

3. (OI 12) Permissive Functions - Several permissive functions are described within the LAR. It is not clear to the NRC staff whether any of these functions are to be performed by the PPS or if the PPS will only be providing input to external systems that in turn perform the permissive logic described in the LAR.

   LAR Section 4.1.9, Pressurizer Pressure Protection Features, states, in part, that "[s]ettings of the bistable comparators used to develop the permissives are not affected by the PPS Replacement Project", which implies that all of these permissive functions are performed by systems other than the PPS. However, it is still unclear if this statement applies to all permissive functions described throughout the LAR or if it applies only to those permissives relating to Pressurizer Pressure. It is also possible that the permissive functions are being performed by the existing PPS and will continue to be performed by the replacement system and therefore remain "not affected" by the PPS replacement project. Please provide additional information for the following permissive functions to clearly define what the role of the PPS system will be for each.

   P-4 Reactor Trip
   P-6 Intermediate Range Permissive
   P-7 Low Power Permissive (Bypasses low Ppzr reactor trip)[1]
   P-8 Loss of Flow Permissive
   P-9 Power Permissive
   P-10 Power Range Power Low Permissive
   P-11 Low Pressurizer Pressure SI Operational Bypass
   P-12 No-Load Low-Low Tave Temperature Permissive
   P-13 Turbine Low Power Permissive[1]
   P-14 Hi-Hi Steam Generator Level

4. (OI 15) A DI&C-ISG-04[2] compliance matrix for the DCPP PPS system was not submitted with, or referenced in, the LAR for the Westinghouse/ALS (W/ALS) platform. Instead, the DI&C-ISG-04 compliance Section 4.8 of the LAR refers the reader to the ALS licensing topical report for nearly all the points of DI&C-ISG-04. Figures 4.4 and 4.5 of the LAR indicate various 1E and non-1E communication pathways to and from ALS processor (e.g., Maintenance Work Station, plant computer, process control, port aggregator, and 4-20 ma temperature signals to Tricon processor). These are all application-specific features of the PPS and the NRC staff expects a Westinghouse/CS Innovations (W/CSI) ALS document to be submitted, similar in scope and detail to the Invensys, "Pacific Gas & Electric Company Nuclear Safety-Related Process Protection System Replacement Diablo Canyon Power Plant DI&C-ISG-04 Conformance Report," Document No. 993754-1-912 Revision 0, to be submitted on the docket, which explains

---

[1] The LAR states that "These signals are generated in the PPS."

[2] U.S. Nuclear Regulatory Commission, "Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance, Revision 1," dated March 6, 2009 (ADAMS Accession No. ML083310185).

how the ALS portion of the PPS application conforms with the guidance of DI&C-ISG-04. Please provide this document with sufficient detail to determine how the W/ALS processor complies with DI&C-ISG-04.

5. (OI 16) PPS Network Equipment Testing - Section 1.4.4, System Communication (page 12/38) of Document No. 993754-1-813(P), Revision 0, "Pacific Gas & Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Validation Test Plan (VTP)," dated October 13, 2011[3], states, in part, that

> The network equipment, including media converter, NetOptics Network Aggregator Tap, and gateway hub, and the MWS [maintenance work station] will not be within the test scope of this VTP. The Nuclear Delivery (ND) group will coordinate with Pacific Gas & Electric for system staging prior to turn over to Nuclear IV&V [independent verification and validation]. The Nuclear IV&V group will confirm proper operation of network communications system interfaces before beginning testing addressed in this VTP.

The NRC staff requests information on when, where, and what test plans and procedures will be used to test the network equipment. Test plans for testing this equipment should be submitted to the staff for review.

6. (OI 17) Section 5.1.4, Hardware Validation Test (HVT), (page 27/38) of Document No. 993754-1-813(P) states that the ALS equipment will not be included in the factory acceptance testing (FAT). This issue was discussed with PG&E and its contractors and PG&E proposed performance of separate but overlapping tests at each factory to accomplish the integration test. The NRC staff has concerns over the fact that the MWSs to be installed in the plant would only be tested during the Tricon FAT, and not tested in the fully integrated PPS configuration. In order to complete its safety evaluation, the new PPS configuration must be fully tested in an integrated manner so that all phases of the system's verification and validation (V&V) can be reviewed and credited in the safety finding. The staff requests information on where, when, and the test plans and/or procedures that will be used to fully test the Integrated PPS system (both Tricon V10 and ALS platforms together).

---

[3] Invensys Operations Management/Triconex, Document No. 993754-1-813(P), "Pacific Gas & Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Validation Test Plan (VTP), Revision 0," dated October 13, 2011 (non-proprietary version designated as 993754-1-813(NP) available at ADAMS Accession No. ML11318A028).

7. (OI 18) Document No. 993754-1-802(P), Revision 1, "Pacific Gas & Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Verification and Validation Plan (SVVP)," dated October 13, 2011[4], does not provide a clear explanation of how the Invensys SVVP complies with Institute of Electrical and Electronics Engineers (IEEE) 1012-1998, "IEEE Standard for Software Verification and Validation." Please provide a cross-reference table that explains how the Invensys SVVP implements the criteria of IEEE 1012-1998.

8. (OI 18) The Westinghouse/ALS 6116-00000 Diablo Canyon PPS Management Plan does not provide a clear explanation of how the CSI SVVP complies with IEEE 1012-1998. Please provide a cross-reference table that explains how the W/CSI SVVP implements the criteria of IEEE 1012-1998.

9. (OI 19) Section 4.1.1, SSPS, of the LAR states, in part, that

> The SSPS evaluates the signals and performs RTS and ESFAS functions to mitigate Abnormal Operational Occurrences and Design Basis Events described in FSAR [26] Chapter 15.

However, Chapter 15 of the DCPP final safety analysis report (FSAR) does not use the terms Abnormal Operational Occurrences (AOOs) or Design Basis Events (DBE). Instead, the accident analysis in Chapter 15 identifies conditions as follows:

> CONDITION I - NORMAL OPERATION AND OPERATIONAL TRANSIENTS
>
> CONDITION II - FAULTS OF MODERATE FREQUENCY
>
> CONDITION III - INFREQUENT FAULTS
>
> CONDITION IV - LIMITING FAULTS

Please explain the correlation between the conditions described in FSAR Chapter 15 and the AOOs and DBEs described in the LAR.

10. Not Used.

---

[4] Invensys Operations Management/Triconex, Document No. 993754-1-802(P), Revision 1, "Pacific Gas & Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Software Verification and Validation Plan (SVVP)," dated October 13, 2011 (nonproprietary version designated as 993754-1-802(NP) available at ADAMS Accession No. ML11318A030).

11. (OI 23) PPS Integration Testing - Refer to Section 4.2.13.1 of the LAR

LAR Section 4.2.13.1, Tricon-Based PPS Equipment Communications, states, in part, that

> Figure 4-13 only shows one TCM [Tricon Communications Module] installed in the Tricon Main Chassis (Slot 7L), the PPS replacement will utilize two TCM cards in each main chassis (Slots 7L and 7-R). This will provide two non-safety-related communication paths to the MWS and the PPC [Plant Process Computer] Gateway Computer from each Protection Set to ensure continued communications if a single TCM fails.
>
> The NetOptics Model PA-CU/PAD-CU[5] PA-CU port aggregator network tap was approved previously by NRC for a similar application in the Oconee [Reactor Protection System (RPS) Safety Evaluation Report (SER)] Section 3.1.1.4.3 [18]. The NRC staff determined that due to the electrical isolation provided by use of fiber optic cables and the data isolation provided by the Port Tap and the Maintenance and Service Interface (MSI) in the Oconee RPS, there was reasonable assurance that a fault or failure within the Oconee Gateway computer or the Operator Aid Computer will not adversely affect the ability of the Oconee RPS to accomplish its safety functions.
>
> During the SAT [site acceptance testing] PG&E will test the Protection Set communications paths illustrated in Figure 4-13 to verify that there is no inbound communications path associated with port aggregator network tap Port 1. That is, PG&E will verify that communications from Port 1 to either the TCM on Port A or the MWS on Port B of the port aggregator network tap are not permitted. Results of this test will be documented in final System Verification and Validation Report. Port aggregator dual in-line package (DIP) switch positions will be controlled by DCPP configuration management processes.

In order for the NRC staff to approve the integrated configuration of the PPS, prior to shipment of the PPS equipment to DCPP site, all communications paths will require testing on or before FAT, and before completion of the safety evaluation report (SER). This testing is typically completed during or before the PPS FAT, otherwise, the SER will not be completed until after the Site Acceptance Test (SAT). Please provide a test scheme and test plans or procedures that satisfies all regulatory requirements prior to or during the FAT. Otherwise, if this testing will be completed during the SAT, as stated in the LAR, please provide a detailed schedule and test plans (or procedures) for this testing so the NRC can revise its PPS LAR Review Plan accordingly.

---

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

12. (OI 26) The PG&E System Quality Assurance Plan (SyQAP) defines Supplier tasks that are related to assurance of software quality for each of the following phases of development:

- Project Initiation and Planning
- Conceptual Design
- Requirements
- Design
- Implementation
- Integration
- Test

These phases do not align with the phases used in the ALS or Tricon development lifecycles. For instance, the Tricon SQAP defines the phases as Requirements, Design, Implementation, and Test (Validation). Because of this, it is not clear how assurance of task completion can be accomplished. Please clarify under which Tricon phases those tasks listed under Integration, Initiation and Planning, and Conceptual Design would be performed.

The ALS Software Quality Assurance Plan (SQAP) does not mention phases but the ALS Management plan defines the development phases as: Planning, Development, Manufacturing, System Test, and Installation.

Please provide a mapping of Phases defined in the SyQAP to the Phases of the ALS and Tricon system development processes so that the staff can correctly identify and confirm performance of these Quality Assurance tasks.

13. (OI 27 and OI 29) Software Management Plan – LAR, Attachment 3, describes the project organization, roles, and responsibilities for the PPS replacement project. Please describe the oversight activities that PG&E will perform during the PPS replacement project, as well as the interface between PG&E and Invensys and W/CSI, and the methodology to judge quality of the vendor effort.

14. Not Used.

15. (OI 31) Software Quality Assurance Plan - The PG&E SyQAP has been approved by the PG&E Diablo PPS Upgrade Project Manager and the Altran Project lead; however, there are several other organizations that have responsibilities delineated in the SQAP. The managers of these organizations have not approved the SyQAP. The following organizations are assigned roles and responsibilities within Section 3.4 of the SyQAP. Please explain the means by which these organizations have committed to comply with the requirements stated in the SyQAP.

- Vendor IVV Projects Managers
- Engineer of Choice (EOC) Design Change Package Team
- PG&E Project Engineering Team
- QA Organization

- Testing and Integration Team
- V&V Organization

16. (OI 32) LAR Section 4.2.7, Power Supply, describes how power is supplied to the PPS. From these descriptions, it is not clear to the NRC staff how these vital power sources are configured in relation to the 120V alternating current (AC) panels that feed the PPS. Please provide a simplified diagram to show the relationship between the 125V Batteries/Direct Current (DC) Buses, Battery Chargers, Inverters, and the 120V AC distribution Panels that supply power to the PPS.

17. (OI 07) DI&C ISG-06, Revision 1[6], Enclosure B, Item 1.16, Design Analysis Reports: The LAR does not appear to comply with the Standard Review Plan (SRP) (DI&C-ISG-04) regarding the connectivity of the MWS to the PPS. The TriStation V10 platform relies on software to effect the disconnection of the TriStation's capability to modify the safety system software. Based on the information provided in the Tricon V10 licensing topical report (LTR), the NRC staff determined that the Tricon V10 platform does not comply with the NRC guidance provided in DI&C-ISG-04, Staff Position 1, Point 10, hence the DCPP PPS configuration does not fully comply with this guidance.

    In order for the NRC staff to accept this Tricon V10 keyswitch function as an acceptable alternative to this staff position, please provide the DCPP PPS specific system communications control configuration—including the operation of the keyswitch, the software affected by the keyswitch, and any testing performed on failures of the hardware and software associated with the keyswitch which demonstrates that failures of the keyswitch will not affect the PPS safety protection sets from performing its safety function.

    Information pertaining to the design of the ALS platform disconnect keyswitch is unclear to the NRC staff at this time since the ALS LTR review has not been completed. Therefore, please provide a detailed description of the ALS MWS disconnect/mode change keyswitch—including the operation of the keyswitch, the software/program execution affected by the keyswitch, and any testing performed on failures of the hardware and software associated with the keyswitch which demonstrates that failures of the keyswitch will not affect the PPS safety protection sets from performing its safety function.

18. The Tricon V10 system Operational Mode Change (OMC) keyswitch changes operational modes of the 3008N Main Processors (MPs) and enables the TriStation 1131 personal computer (PC) to change parameters, software algorithms, etc., related to the application program of the safety channel without the channel or division being in bypass or in trip. As stated in Section 3.1.3.2 of the Tricon V10 SER, the TriStation 1131 PC should not normally be connected while the Tricon V10 is operational and performing safety critical functions. However, it is physically possible for

---

[6] U.S. Nuclear Regulatory Commission, "Digital Instrumentation and Controls, DI&C-ISG-06, Revision 1, Task Working Group #6: Licensing Process, Interim Staff Guidance," dated January 19, 2011 (ADAMS Accession No. ML110140103).

the TriStation PC to be connected at all times, and this should be strictly controlled via administrative controls (e.g., place the respective channel out of service while changing the software, parameters, etc). The LAR does not mention any administrative controls such as this to control the operation of the OMC (operational mode change) keyswitch. However, in PG&E letter DCL-12-030 dated April 2, 2012 (ADAMS Accession No. ML12094A072), the licensee stated that connection of the TriStation will be controlled under administrative controls (password protection, key control, etc) and that the affected PPS channel will procedurally be placed out of service any time the Tricon keyswitch is not in the RUN position. PG&E further committed to provide a detailed failure mode and effects analysis (FMEA) of the TriStation 1131 PC system to ascertain the potential effects this non-safety PC may have on the execution of the safety application program/operability of the PPS channel while the non-safety TriStation 1131 PC is permanently attached to the safety-related Tricon V10 system (with the OMC keyswitch in RUN position). Please ensure the TriStation and ALS FMEA addresses this matter so that the NRC staff can determine that the DCPP PPS complies with the NRC Staff Guidance provided in Staff Position 1, Point 11.

19. (OI 01) [ISG-06 Enclosure B, Item 1.3] Deterministic Nature of Software. The DCPP-specific application should identify the board access sequence and provide corresponding analysis associated with digital response time performance. This analysis should be of sufficient detail to enable the NRC staff to determine that the logic-cycle:

    a. has been implemented in conformance with the ALS Topical Report design basis,
    b. is deterministic, and
    c. the response time is derived from plant safety analysis performance requirements and in full consideration of communication errors that have been observed during equipment qualification.

    As stated in the LAR, information pertaining to response time performance will be submitted as a Phase 2 document. The NRC staff has received the digital response time calculation for the Tricon V10 portion of the PPS (Document No. 993754-1-817(P), Revision 1, "Pacific Gas & Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Maximum TSAP Scan Time," dated April 9, 2012[7]).

    However, the NRC staff has not yet received a similar calculation to predict the digital response time for the ALS platform. Please provide this calculation addressing the above subject matter accordingly.

---

[7] Invensys Operations Management/Triconex Document No. 993754-1-817(P), Revision 1, "Pacific Gas & Electric Company, Nuclear Safety-Related Process Protection System Replacement, Diablo Canyon Power Plant, Maximum TSAP Scan Time," dated April 9, 2012 (no public version available in ADAMS).

20. (OI 34) (Software Integration Plans) The integration planning documentation referenced in LAR Section 4.5.4, Software Integration Plan (Section D.4.4.1.4 of DI&C-ISG-06), does not include integration of the two subsystems (ALS integrated with Tricon). Please provide additional documentation to describe how system integration is to be accomplished for the Tricon/ALS PPS combined system.

If you have any questions regarding this matter, I may be reached at 301-415-1132.

Sincerely,

/RA/

Joseph M. Sebrosky, Senior Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

Enclosure:
As stated

cc w/encl: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL4 R/F
RidsAcrsAcnw_MailCTR Resource
RidsNrrDeEicb Resource
RidsNrrDorlLpl4 Resource
RidsNrrLAJBurkhardt Resource
RidsNrrPMDiabloCanyon Resource
RidsOgcRp Resource
RidsRgn4MailCenter Resource
WKemper, NRR/DE/EICB
RStattel, NRR/DE/EICB
RAlvarado, NRR/DE/EICB
SMakor, RIV/DRS/EB2

ADAMS Accession No. ML12208A364

OFFICE	NRR/LPL4/PM	NRR/LPL4/LA	NRR/DE/EICB/BC	NRR/LPL4/BC	NRR/LPL4/PM
NAME	JSebrosky	JBurkhardt	JThorp	MMarkley	JSebrosky
DATE	8/6/12	8/1/12	8/6/12	8/7/12	8/7/12

OFFICIAL RECORD COPY