



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

January 13, 2012

Mr. John T. Conway
Senior Vice President – Energy Supply
and Chief Nuclear Officer
Pacific Gas and Electric Company
Diablo Canyon Power Plant
77 Beale Street, Mail Code B32
San Francisco, CA 94105

SUBJECT: 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)

Dear Mr. Conway:

By letter dated October 26, 2011 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML113070457), Pacific Gas and Electric Company (PG&E, the licensee), submitted a license amendment request (LAR) that would allow the permanent replacement of the current Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP) Eagle 21 digital process protection system (PPS) with a new digital PPS that is based on the Invensys Operations Management Tricon Programmable Logic Controller (PLC), Version 10, and the CS Innovations, LLC (CSI, a Westinghouse Electric Company), Advanced Logic System (ALS). The purpose of this letter is to provide the results of the U.S. Nuclear Regulatory Commission (NRC) staff's acceptance review of this LAR. The acceptance review was performed to determine if there is sufficient technical information in scope and depth to allow the NRC staff to complete its detailed technical review. The acceptance review is also intended to identify any apparent information needs for the NRC staff to make a conclusion of reasonable assurance of safety and that the activities will be conducted in accordance with the Commission's regulations.

Consistent with Section 50.90 of Title 10 of the *Code of Federal Regulations* (10 CFR), an amendment to the license (including the technical specifications) must fully describe the changes requested, and following as far as applicable, the form prescribed for original applications. Section 50.34 of 10 CFR addresses the content of technical information required. This section stipulates that the submittal address the design and operating characteristics, unusual or novel design features, and principal safety considerations.

The NRC staff has performed its acceptance review of the LAR in accordance with Revision 1 of the Office Nuclear Reactor Regulation's Office Instruction, LIC-109, "Acceptance Review Procedures" (ADAMS Accession No. ML091810088), Appendix B, "Guide for Performing Acceptance Reviews." The criteria of the Digital Instrumentation and Controls Revision 1 of Interim Staff Guidance Digital I&C-ISG-06, "Licensing Process" dated January 19, 2011 (ISG-06) (ADAMS Accession No. ML110140103), was used by the NRC staff to determine the technical and regulatory acceptance of the LAR during the acceptance review. The NRC staff has reviewed your application and concluded that it does provide technical information in sufficient detail to enable the NRC staff to complete its detailed technical review and make an

independent assessment regarding the acceptability of the proposed amendment in terms of regulatory requirements and the protection of public health and safety and the environment. Given the lesser scope and depth of the acceptance review as compared to the detailed technical review, there may be instances in which issues that impact the NRC staff's ability to complete the detailed technical review are identified despite completion of an adequate acceptance review. You will be advised of any further information needed to support the NRC staff's detailed technical review by separate correspondence.

Notwithstanding the above, the NRC staff identified several items that may present challenges to the performance of a detailed technical evaluation of the proposed PPS replacement system LAR and will require further clarification as discussed below:

DCPP PPS Replacement LAR Items

1. [1.3¹] Deterministic Nature of Software: Please 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. Please ensure this matter is addressed accordingly.

2. [1.4] Software Management Plan: Regulatory Guide (RG) 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," February 2004, Revision 1, endorses Institute of Electrical and Electronics Engineers (IEEE) 1012-1998, "IEEE Standard for Software Verification and Validation," and IEEE 1028-1997, "IEEE Standard for Software Reviews and Audits," with the exceptions stated in the Regulatory Position of RG 1.168. RG 1.168 describes a method acceptable to the NRC staff for complying with parts of the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP) Table 7-1 and Appendix 7.1-A identify RG 1.168 as SRP acceptance criteria for reactor trip systems and for engineered safety features.

Westinghouse/ALS 6116-00000, "Diablo Canyon PPS Management Plan," Figure 2-2, shows the Verification and Validation (V&V) organization reporting to the Project Manager. Please explain the apparent inconsistency with the information described in the ALS Management Plan for the generic system platform, where the V&V organization

¹ ISG-06 Enclosure B information line items.

is independent from the Project Manager. Further, please explain the apparent inconsistency with the criteria of RG 1.168. This will need to be reconciled during the LAR and ALS licensing topical report (LTR) reviews.

3. [1.9] Software V&V Plan: The ALS V&V Plan states that Project Manager of the supplier is responsible for providing directions during implementation of V&V activities. Also, the organization chart in the DCPD PPS Management Plan shows the V&V manager reporting to the Project Manager.

The ALS V&V Plan described in the ISG-06 matrix for the ALS platform and the Diablo Canyon PPS Management Plan do not appear to provide sufficient information about the activities to be performed during V&V. For example, the ALS V&V Plan states that for project specific systems, V&V activities are determined on a project by project basis and are described in the Project Management Plan, in this case, 6116-00000, "Diablo Canyon PPS Management Plan." However, the 6116-00000 Diablo Canyon PPS Management Plan states: "See the ALS V&V Plan for more information and the interface between the IV&V [independent V&V] team and the PPS Replacement project team."

The Triconex V&V plan states that the Engineering Project Plan (EPP) defines the scope for V&V activities. As mentioned before, the Triconex EPP is not listed in the ISG-06 matrix.

Please provide further clarification to demonstrate compliance with RG 1.168, Revision 1.

4. [1.10] Software Configuration Management Plan: The LAR includes PG&E CF2.ID2, "Software Configuration Management for Plant Operations and Operations Support," in Attachment 12. However, the document provided in Attachment 12 only provides a guideline for preparing Software Configuration Management (SCM) and Software Quality Assurance (SQA) plans. Though it is understood that the licensee will not perform development of software, PG&E personnel will become responsible for maintaining configuration control over software upon delivery from the vendor.

The NRC staff requires the actual plan to be used by the licensee for maintaining configuration control over PPS software in order to evaluate against the acceptance criteria of the SRP. For example, the ALS Configuration Management (CM) Plan (6002-00002) describes initial design activities related to ALS generic boards. This plan does describe the configuration management activities to be used for the development and application of the ALS platform for the DCPD PPS. The NRC staff requires that configuration management for this design be described in the DCPD project-specific plan. These items will need further clarification during the LAR review to demonstrate adherence with Branch Technical Position (BTP)-14.

5. [1.11] Software Test Plan: The V10 platform documents identified in ISG-06 matrix state that the interface between the Next Generation Input and Output (NGIO) Core Software and IO-specific software will not be tested. Please explain when and how this interface will be tested, and why this test is not part of the software unit testing and integration testing activities.

Further, the 993754-1-813, "Diablo Canyon Triconex PPS Validation Test Plan," states that the DCP's test system application program (TSAP) will not be loaded on the system; instead Triconex will use another TSAP for the validation test. It is not clear why the DCP's TSAP will not be used for the validation test or when the DCP's TSAP will be loaded on the system and validated for the DCP PPS. These items will need further clarification during the LAR review to demonstrate compliance with BTP-14.

6. [1.14] Equipment Qualification Testing Plans - The LAR Sections 4.6, 4.10.2.4 and 4.11.1.2 provide little information on the plant-specific application environmental factors. The Tricon V10 Safety Evaluation dated November 17, 2011 (not publicly available), Section 6.2 lists 19 application specific actions items (ASAs) that the licensee should address for plant-specific applications. Please address each of the ASAs for the Tricon portion of the PPS replacement. Accordingly, please provide similar information for the ALS portion of the PPS replacement will also be required.
7. [1.16] Design Analysis Reports: The LAR does not appear to adhere to the SRP (ISG-04²) regarding the connectivity of the Maintenance Work Station 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 LTR, the NRC staff determined that the Tricon V10 platform does not satisfy NRC guidance provided in ISG-04, Revision 1, Staff Position 1, Point 10. Consequently, the DCP PPS configuration does not adhere to this guidance.

In order for the NRC staff to accept this keyswitch function as an acceptable deviation to this NRC staff position, the NRC staff will have to evaluate the DCP 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. The status of the ALS platform on this matter is unclear at this time and will be resolved as the ALS LTR review is completed.

The Tricon V10 system Operational Mode Change (OMC) keyswitch does change operational modes of the 3008N MPs (main processors) 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 safety evaluation report (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 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 keyswitch. In order to leave the non-safety TriStation 1131 PC attached to the SR Tricon V10 system while the key switch is

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

in the RUN position, a detailed failure modes and effects analysis (FMEA) of the TriStation 1131 PC system will be needed to ascertain the potential effects this non-safety PC may have on the execution of the safety application program/operability of the channel or division. These issues must be addressed in order for the NRC staff to determine that the DCPD PPS complies with the NRC Staff Guidance provided in Staff Position 1, Point 11. Please clarify the status of the ALS platform on this point.

8. [1.21] Setpoint Methodology: The NRC staff understands that a summary of setpoint calculations will be provided in Phase 2, however, Section 4.10.3.8 of the LAR also states that PG&E plans to submit a separate LAR to adopt Technical Specification Task Force (TSTF) Change Traveler TSTF-493, Revision 4, "Clarify Application of Setpoint Methodology for LSSS [Limiting Safety System Settings] Functions." The NRC cannot accept this dependency on an unapproved future licensing action. The NRC staff therefore requests the licensee to submit a summary of setpoint calculations which includes a discussion of the methods used for determining as-found and as-left tolerances. This submittal should satisfy all of the informational requirements set forth in ISG-06 Section D.9.4.3.8 without a condition of TSTF-493 LAR approval.
9. Many important sections of the DCPD PPS LAR refer the reader to the ALS LTR to demonstrate compliance of the system with various Clauses of IEEE 603-1991, IEEE 7-4.3.2-203, and ISG-04. However, many important sections of the ALS LTR state that compliance with various Clauses of these IEEE Standards and ISG-04 are application-specific and refer the reader to an application-specific license amendment submittal (i.e., the DCPD PPS LAR in this case). The NRC staff has not yet evaluated all the LAR information in detail and compared this information with that provided in the ALS LTR to ensure there is no missing information. However, PG&E and its contractors are encouraged to review these two licensing submittals promptly to verify that compliance with these IEEE Standards and ISG-04 are adequately addressed within both licensing documents.

Licensee's Dates of Submittals Required for Safety Evaluation Completion

Per LAR Commitment #1, PG&E has stated that Phase 2 documents as defined in ISG-06 that have not been submitted previously to the NRC staff will be submitted within 12 months of the requested approval date, by May 30, 2012, with the exception of specific Phase 2 documents which require manufacture and factory acceptance testing (FAT) to complete.

With completion of this acceptance review, the NRC staff has identified the following documents as being necessary for completion of the Phase 2 submittal requirements. These documents should be submitted to the NRC prior to May 30, 2012.

- 2.1 Safety Analysis
- 2.2 V&V Reports with exception of summary test reports and test results.
- 2.4 Test Design Specifications
- 2.7 Requirements Traceability Matrix
- 2.8 Failure Modes and Effects Analysis
- 2.9 System Build Documentation
- 2.11 Qualification Test Methodologies

- 2.13 As-Manufactured Logic Diagrams
- 2.14 System Response Time Confirmation Report
- 2.15 Reliability Analysis
- 2.16 Setpoint Calculations
- 2.17 Software Tool Analysis Report
- 2.18 Commercial Grade Dedication Reports

Final Safety Analysis Report Update Changes and Technical Specification Basis Changes
(Commitment 3)

The NRC staff agrees that all remaining Phase 2 documents that have been identified under licensee commitment #2 should be submitted before December 31, 2012. In addition, the NRC staff expects that the following documents will be available for NRC staff review on or before May 30, 2012:

- 3.1 Software Integration Report
- 3.2 Individual V&V Problem Reports up to FAT
- 3.3 Configuration Management Reports
- 3.4 Test Procedure Specification
- 3.5 Completed Test Procedures and Reports
- 3.6 Test Incident Reports
- 3.7 Code Listings
- 3.8 Software Project Risk Management Report
- 3.9 Circuit Schematics
- 3.10 Detailed System and Hardware Drawings

Conclusion

The issues identified above may challenge the NRC staff's ability to complete its technical review of the PPS replacement LAR. PG&E is requested to submit to the NRC within 60 days of this letter, responses to the above issues, which should include discussions of how the items identified above will be addressed via supplemental information if required.

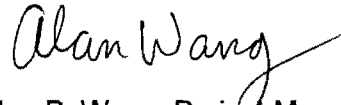
Based on PG&E providing: 1) a high quality license application and supporting documentation as described in ISG-06, "Licensing Process," 2) acceptable responses to items as noted above, and 3) a timely response to licensee actions requested by the NRC staff during the LAR review, the NRC staff would expect that the amendments could be issued by October 31, 2013.

J. Conway

- 7 -

If you have any questions, please contact me at 301-415-1445 or alan.wang@nrc.gov.

Sincerely,

A handwritten signature in black ink that reads "Alan Wang". The signature is fluid and cursive, with a long horizontal stroke extending from the end of the name.

Alan B. Wang, Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

cc: Distribution via Listserv

J. Conway

- 7 -

If you have any questions, please contact me at 301-415-1445 or alan.wang@nrc.gov.

Sincerely,

/RA/

Alan B. Wang, Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

cc: Distribution via Listserv

DISTRIBUTION:

PUBLIC

LPLIV Reading

RidsAcrsAcnw_MailCTR Resource

RidsNrrDeEicb Resource

RidsNrrDirsltsb Resource

RidsNrrDorlDpr Resource

RidsNrrDorlLpl4 Resource

RidsNrrLAJBurkhardt Resource

RidsNrrPMDiabloCanyon Resource

RidsOgcRp Resource

RidsRgn4MailCenter Resource

ADAMS Accession No. ML120120005

***via email**

OFFICE	NRR/LPL4/PM	NRR/LPL4/LA	NRR/DE/EICB	NRR/DE/EICB
NAME	AWang*	JBurkhardt*	RStattel	WKemper
DATE	1/12/12	1/12/12	1/12/12	1/12/12
OFFICE	NRR/DE/EICB/BC	NRR/LPL4/BC	NRR/LPL4/PM	
NAME	GWilson	MMarkley	AWang	
DATE	1/12/12	1/13/12	1/13/12	

OFFICIAL RECORD COPY