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

May 15, 2015

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 – REGULATORY AUDIT PLAN FOR JUNE 22-26, 2015, AUDIT AT WESTINGHOUSE FACILITY IN WARRENDALE, PENNSYLVANIA, IN SUPPORT OF DIGITAL PROCESS PROTECTION SYSTEM REPLACEMENT LICENSE AMENDMENT REQUEST (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, June 6, August 2, September 11, November 27 and December 5, 2012; and March 7, March 25, April 30, May 9, May 30, and September 17, 2013; and April 24 and April 30, 2014; and February 2, 2015 (Agencywide Documents Access and Management System Accession Nos. ML113070457, ML113610541, ML12094A072, ML12131A513, ML12170A837, ML12222A094, ML12256A308, ML13004A468, ML12342A149, ML13267A129, ML13093A311, ML13121A089, ML13130A059, ML13154A049, ML13261A354, ML14205A031, ML14121A002, and ML15062A386, respectively), Pacific Gas and Electric Company requested the U.S. Nuclear Regulatory Commission (NRC) staff's approval of an amendment for the Diablo Canyon Power Plant, Units 1 and 2 (Diablo Canyon). The proposed license amendment request would provide a digital replacement of the Process Protection System portion of the Reactor Trip System and Engineered Safety Features Actuation System at Diablo Canyon.

To support its safety evaluation, the NRC Instrumentation and Controls Branch will conduct an audit at the Westinghouse facility in Warrendale, Pennsylvania, during the week of June 22-26, 2015. Enclosed is the plan to support this audit.

If you have any questions, please contact me at 301-415-1564 or via e-mail at Siva.Lingam@nrc.gov.

Sincerely,

Siva P. Lingam

Siva P. Lingam, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

Enclosure:
Audit Plan

cc w/encl: Distribution via Listserv

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

REGULATORY AUDIT PLAN FOR JUNE 22-26, 2015, AUDIT AT WESTINGHOUSE FACILITY IN WARRENDALE, PENNSYLVANIA, TO SUPPORT REVIEW OF DIGITAL PROCESS PROTECTION SYSTEM REPLACEMENT LICENSE AMENDMENT REQUEST

PACIFIC GAS AND ELECTRIC COMPANY

DIABLO CANYON POWER PLANT, UNITS 1 AND 2

DOCKET NOS. 50-275 AND 50-323

Background

The U.S. Nuclear Regulatory Commission (NRC) staff is currently engaged in a review of a digital safety system replacement for the Diablo Canyon Power Plant, Units 1 and 2 (Diablo Canyon). By letter dated October 26, 2011, Pacific Gas and Electric Company (PG&E, the licensee) submitted license amendment request (LAR) 11-07 to replace the Diablo Canyon Eagle 21 Process Protection System (PPS) with a new digital PPS (Agencywide Documents Access and Management System (ADAMS) Accession No. ML11307A457). In addition, the licensee supplemented the LAR by letters dated December 20, 2011, and April 2, April 30, June 6, August 2, September 11, November 27, and December 5, 2012, and March 7, March 25, April 30, May 9, May 30, and September 17, 2013, and April 24 and April 30, 2014, and February 2, 2015 (ADAMS Accession Nos. ML113610541, ML12094A072, ML12131A513, ML12170A837, ML12222A094, ML12256A308, ML13004A468, ML12342A149, ML13267A129, ML13093A311, ML13121A089, ML13130A059, ML13154A049, ML13261A354, ML14205A031, ML14121A002, and ML15062A386, respectively). The LAR requested NRC review and approval of the proposed design. As part of this review, the NRC staff is conducting a regulatory audit of the Advanced Logic System (ALS) portion of the Diablo Canyon PPS (DCPPS) replacement system.

In February of 2013, the NRC staff conducted an initial audit of the ALS system development processes in Scottsdale, Arizona (see audit report dated October 8, 2013; ADAMS Accession No. ML13232A263). During that audit, the NRC staff was unable to observe how the design phase outputs are subject to the Verification and Validation (V&V) processes because the V&V activities had not been completed. The NRC staff also identified several open items and noted that a follow-up audit would be necessary to evaluate resolution activities for each of these open items.

Regulatory Audit Basis

To support its safety evaluation (SE), the NRC Instrumentation and Controls Branch (EICB) will conduct a second audit at the Westinghouse facility in Warrendale, Pennsylvania. The purpose of this confirmatory audit is to determine if the life cycle processes used, and the outputs of those processes have resulted in a PPS system for use at Diablo Canyon, which will meet

regulatory requirements. This audit will provide information necessary to complete the NRC staff's evaluation of the proposed ALS portion of the DCPPS.

Regulatory Audit Scope

The objective of this audit is to verify, via an independent evaluation, the ALS subsystem of the DCPPS conforms to applicable regulations, standards, guidelines, plans, and procedures by assessing the implementation of the systems developmental life cycle process.

Audit Requirements

1. Threads reviewed during first audit -

   Several requirement threads were reviewed through the requirements phase during the first ALS audit. The team will select from this list to perform follow-up reviews through the design and implementation phases of PPS system development. The team intends to trace system requirements to specific test cases to be performed during the Factory Acceptance Test.

2. Additional topic areas to be covered during second audit:

   a. **Time Response** – The NRC will review the relation between the specified time response requirements for PPS and the safety analysis response time assumptions listed in the Updated Final Safety Analysis Report Table 15.1-2. The objective of this audit activity is to understand and confirm how the PPS component of the overall safety system response time assumptions is derived.

   b. **Project Risk Mitigation** (SE Section 3.4.1.1) - Westinghouse uses Risk Assessment Worksheet (RAW) to identify risk, problem and mitigation strategies. This worksheet is maintained and reviewed periodically by the Project Leadership Team. The NRC staff plans to review RAWs associated with the PPS project to confirm performance of risk mitigation activities.

   c. **Configuration Verification** (SE Section 3.10.1.7) - Conduct Audit activity to observe how the Maintenance Workstation/ALS Service Unit (ASU) is used to verify that correct logic implementation is installed into the DCPPS ALS-102 Core Logic boards. Determine if this verification activity can be done with the system operable and if surveillance tests will be performed to periodically verify correct logic implementation. Determine if accessing the board's Non-Volatile Memory will require connecting the Test ALS Bus (TAB) or if this configuration information can be accessed through the communication channels TxB1, and TxB2 communication links. Review the Configuration Status Accounting document 6116-00050 and verify that the revision number and other identification information is available for each of the configuration items. This audit item is associated with Open Item 109 of the DCPPS Open Item List.

d. **Redundancy Checker** (LAR 4.2.5.2 page 64) - The LAR states that the redundancy checker compares outputs and critical initial states from the two cores and will drive the board to a safe state when the outputs do not agree. The NRC staff plans to audit the requirements associated with defining these states and confirm implementation within the system design. This audit item is associated with Open Item 110 of the DCPPS Open Item List.

e. **TAB Connection Verification** (LAR 4.2.13.5 page 95) – The LAR states that the ASU software ensures that the correct TAB is connected to the respective Electronics Industries Alliance (EIA)-485 port when the TAB is enabled. The NRC staff plans to review requirements associated with this function and confirm implementation within the ALS system design.

f. **TAB and TXB Configuration and Communication** (LAR 4.2.9 page 74) – Transmit Bus TxB2 transmits data from each ALS chassis "A" and "B" ALS-102 Core Logic Board to the Maintenance Workstation. Two-way communications are permitted only when the TAB communication link is physically connected between the TAB and the ALS Maintenance Workstation. The NRC staff plans to review requirements associated with these functions and confirm implementation within the ALS system design. This audit item is associated with Open Items 69, 81, and 106 of the DCPPS Open Item List.

g. **V&V Activities Associated with "Verification of Diversity"** – The NRC staff will audit V&V activities used to ensure that the completed Core A and Core B logic implementations are sufficiently diverse so that logic implementation errors common to both cores will not need to be considered. The audit team plans to evaluate the ALS Platform Field Programmable Gate Array (FPGA) V&V Test Plan, 6002-00018 and the V&V activities prescribed therein to confirm the necessary degree of diversity is achieved.

h. **Indication of Channel Bypass Status** – This audit item is associated with Open Item 111 of the DCPPS Open Item List. The NRC staff will perform a thread review of requirement R4082 of the FPGA Requirements Specification 6116-10201. This requirement has been superseded; however, the NRC plans to evaluate how the initiating functional requirement is being satisfied in the completed system design.

   Additional V&V activity documents will be reviewed as necessary to accomplish the objectives of this audit item.

i. **Secure Development Environment** – Verify that the development environment established for the DCPPS development effort conforms to the requirements of Regulatory Guide 1.152, Revision 3. The NRC staff will review the secure development activities by Westinghouse since moving the development environment from Scottsdale, Arizona, to the Warrendale, Pennsylvania, facility.

Information Necessary for the Regulatory Audit

The following documentation and supporting materials will need to be available for review in the performance of this audit. The NRC requests that these documents be available to the audit team upon arrival at the Westinghouse facility.

- Configuration Diagrams for the ALS portion of the DCPPS
- PPS Architecture drawings as required to demonstrate required functionality
- Diablo Canyon FPGA Requirements Specification 6116-10201
- Diablo Canyon Core A and Core B FPGA Design Specifications (6116-10203 and 6116-10204)
- Current DCPPS Requirements Traceability Matrix 6116-00059
- Configuration Status Accounting, 6116-00050, Rev. X (most current)
- DCPPS Configuration Management Report, 6116-00400, Rev. X (most current)
- DCPPS Secure Development Environment Vulnerability Assessment, Rev. X (most current)
- Cyber Security Plan, NA 5.10 (current revision)
- IDI Requirements, WNA-PS-02884-GEN
- IDI Assessment, WNA-CS-00117-GEN

The audit staff also requests access to the current Project Traceability Matrix information in order to observe that applicable functional requirements are correctly implemented in the PPS.

Team Assignments / Resource Estimates

The resource estimate for this audit visit is approximately 200 hours of direct review activity. The NRC staff performing this audit will be:

NRC/NRR [Office of Nuclear Reactor Regulation]/DE [Division of Engineering]/EICB

- Richard Stattel (301) 415-8472
- Rossnyev Alvarado (301) 415-6808
- Samir Darbali (301) 415-1360
- John Thorp (301) 415-8508

NRC/Region IV/DRS [Division of Reactor Safety]/EB2 {Engineering Branch 2]

- Shiattin Makor (817) 200-1507

Logistics

The audit will start at 1:00 p.m. on Monday, June 22, 2015, and conclude on Friday, June 26, 2015, at the Westinghouse offices in Warrendale, Pennsylvania.

Our tentative schedule for the audit is as follows:

Date	***Time***	***Audit Activity***	***Lead***
Monday	1:00 p.m.	Entrance meeting • Introductions • Discuss purpose & objectives of audit • Westinghouse staff to provide overview of Warrendale PPS Project & facility.	Stattel
	2:00 p.m.	Review Results of first audit in Scottsdale and Open Items identified during that audit with PG&E and Westinghouse. Discuss CS Innovations, LLC (CSI), a Westinghouse Electric Company, procedures superseded by Westinghouse.	Alvarado
	3:00 p.m.	Perform follow-up actions associated with the requirement threads evaluated during previous audit. Review Secure Development Environment documentation.	NRC Darbali
	5:00 p.m.	Adjourn	
Tuesday	9:00 a.m.	Morning meeting between NRC staff and Westinghouse to discuss activities and logistics for the day.	
	9:30 a.m.	Review of PPS documentation / Conduct interviews with key Westinghouse personnel. Observe Secure Development Environment and Configuration Management features of the facility.	NRC Darbali
	2:00 p.m.	Discuss Preliminary Inspection Items List with Licensee	Stattel
	4:00 p.m.	Discuss software planning documents.	Alvarado
	5:00 p.m.	Adjourn	
Wednesday	9:00 a.m.	Morning meeting between NRC staff and Westinghouse to discuss activities and logistics for the day.	
	9:30 a.m.	Discuss ALS system communication and Interim Staff Guidance (ISG)-04 compliance. Observe Configuration Verification features of the ALS Maintenance Work Station (MWS)/ASU.	NRC
	2:00 p.m.	Review status of Equipment Qualification (EQ) evaluations.	Stattel
	5:00 p.m.	Adjourn	
Thursday	9:00 a.m.	Morning meeting between NRC staff and Westinghouse to discuss activities and logistics for the day.	
	9:30 a.m.	Perform audit review activities.	NRC
	3:00 p.m.	NRC staff internal meeting - identification / resolution of any open items.	NRC

Date	Time	Audit Activity	Lead
Friday	9:00 a.m.	NRC Staff Internal Meeting – Preparation for Exit	NRC
	10:00 a.m.	Exit meeting - NRC staff – provide general overview of observations & identification of any open items.	All
	11:00 a.m.	Adjourn	

Deliverables

At the conclusion of the audit, the NRC staff will conduct an exit briefing and will provide a summary of audit results in each subject area defined in the audit scope.

The NRC Regulatory Audit Report will be issued by August 10, 2015.

References

Licensee Documentation:

- Westinghouse Electric Company LLC, 6002-00301-NP-A, Revision 4, "Advanced Logic System Topical Report and Safety Evaluation," September 2013 (ADAMS Accession No. ML13298A094).

- Pacific Gas & Electric, "Diablo Canyon Units 1 and 2, License Amendment Request 11-07 Process Protection System Replacement," dated October 26, 2011 (ADAMS package Accession No. ML113070457).

- Pacific Gas & Electric Company, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment Topical Report, Revision 1," August 2010 (ADAMS package Accession No. ML102580728).

- Pacific Gas & Electric Company, "Process Protection System (PPS(Replacement System Quality Assurance Plan (SyQAP), Revision 1," March 2013 (ADAMS Accession No. ML13130A059).

- Pacific Gas & Electric Company, "Process Protection System (PPS) Replacement System Verification and Validation Plan (SyVVP), Revision 1," February 2013 (ADAMS Accession No. ML13093A312).

- Pacific Gas & Electric Company, "Process Protection System Replacement, SCM 36-01 Software Configuration Management Plan (SCMP), Revision 1," May 2013 (ADAMS Accession No. ML13154A047).

- Pacific Gas & Electric Company, "Security Related Information to Support Process Protection System Replacement License Amendment Request 11-07" (security-related Enclosure to PG&E Letter DCL-11-123 dated December 20, 2011; ADAMS Accession No. ML113610541).

NRC Guidance:

- U.S. Nuclear Regulatory Commission, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP), Chapter 7, "Instrumentation and Controls."

- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," July 2011 (ADAMS Accession No. ML102870022).

- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.153, Revision 1, "Criteria for Safety Systems," June 1996 (ADAMS Accession No. ML003740022).

- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," February 2004 (ADAMS Accession No. ML040410189).

- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (ADAMS Accession No. ML003740102).

- U.S. Nuclear Regulatory Commission, Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," September 1997 (ADAMS Accession No. ML003740101).

- U.S. Nuclear Regulatory Commission, Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," January 2010 (ADAMS Accession No. ML090340159).

- Nuclear Energy Institute, NEI 08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," April 2010 (security-related).

Industry Standards:

- Institute of Electrical and Electronics Engineers Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

- Institute of Electrical and Electronics Engineers Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

- Institute of Electrical and Electronics Engineers Standard 828-1990, "IEEE Standard for Software Configuration Management Plans."

- Institute of Electrical and Electronics Engineers Standard 829-1998, "IEEE Standard for Software Test Documentation."

- American National Standards Institute/Institute of Electrical and Electronics Engineers Standard 1008-1987, "IEEE Standard for Software Unit Testing."
- Institute of Electrical and Electronics Engineers Standard 1012-1998, "IEEE Standard for Software Verification and Validation."
- Institute of Electrical and Electronics Engineers Standard 1028-1997, "IEEE Standard for Software Reviews and Audits."
- American National Standards Institute/Institute of Electrical and Electronics Engineers Standard 1042-1987, "IEEE Guide to Software Configuration Management."
- Institute of Electrical and Electronics Engineers Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."

If you have any questions, please contact me at 301-415-1564 or via e-mail at Siva.Lingam@nrc.gov.

Sincerely,

/RA/

Siva P. Lingam, Project Manager
Plant Licensing Branch IV-1
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket Nos. 50-275 and 50-323

Enclosure:
Audit Plan

cc w/encl: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPL4-1 R/F
RidsAcrsAcnw_MailCTR Resource
RidsNrrDeEicb Resource
RidsNrrDorlLpl4-1 Resource
RidsNrrLAJBurkhardt Resource
RidsNrrPMDiabloCanyon Resource
RidsRgn4MailCenter Resource
RStattel, NRR/DE/EICB
RAlvarado, NRR/DE/EICB
SMakor, RIV/DRS/EB2
SDarbali, NRR/DE/EICB

ADAMS Accession No.: ML15121A310 *by memorandum

OFFICE	NRR/DORL/LPL4-1/PM	NRR/DORL/LPL4-1/LA	NRR/DE/EICB/BC*	NRR/DORL/LPL4-1/BC	NRR/DORL/LPL4-1/PM
NAME	SLingam	JBurkhardt	JThorp	MMarkley	SLingam
DATE	5/4/15	5/4/15	4/2/15	5/15/15	5/15/15

OFFICIAL RECORD COPY