



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

March 4, 2013

LICENSEE: Pacific Gas and Electric Company

FACILITY: Diablo Canyon Power Plant, Unit Nos. 1 and 2

SUBJECT: SUMMARY OF JANUARY 24, 2013, TELECONFERENCE MEETING WITH PACIFIC GAS AND ELECTRIC COMPANY ON DIGITAL REPLACEMENT OF THE PROCESS PROTECTION SYSTEM PORTION OF THE REACTOR TRIP SYSTEM AND ENGINEERED SAFETY FEATURES ACTUATION SYSTEM AT DIABLO CANYON POWER PLANT, UNIT NOS. 1 AND 2 (TAC NOS. ME7522 AND ME7523)

On January 24, 2013, a Category 1 teleconference public meeting was held between the U.S. Nuclear Regulatory Commission (NRC) and representatives of Pacific Gas and Electric Company (PG&E, the licensee) at NRC Headquarters, One White Flint North, 11555 Rockville Pike, Rockville, Maryland. The purpose of the teleconference meeting was to discuss the license amendment request (LAR) submitted by PG&E on October 26, 2011, for the Digital Replacement of the Process Protection System (PPS) Portion of the Reactor Trip System and Engineered Safety Features Actuation System at Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP) (Agencywide Documents Access and Management System (ADAMS) Accession No. ML113070457). A list of attendees is provided in Enclosure 1.

The teleconference meeting is one in a series of publicly noticed teleconference meetings to be held periodically to discuss issues associated with the NRC staff's LAR review. Preliminary issues that the NRC staff identified during the initial review, and the licensee's responses to these preliminary issues, were discussed during the teleconference meeting. The list of preliminary issues is provided in Enclosure 2.

The NRC staff and licensee confirmed that the next meeting on this topic would be held on February 21, 2013. Highlights from the meeting on January 24, 2013, include the following:

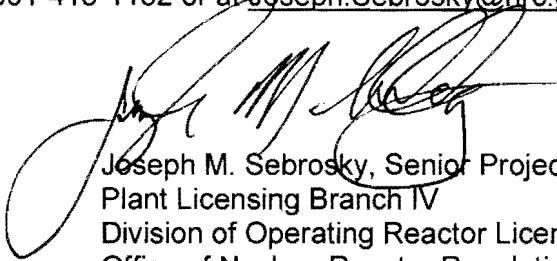
- The NRC and PG&E discussed the status of the February 11-15, 2013, audit at the Westinghouse/CS Innovations facility in Scottsdale, Arizona. The staff confirmed that members of the Nuclear Security and Incident Response (NSIR) will participate in the audit to review the cyber security aspects of this portion of the design. The staff indicated that PG&E should be receiving the audit plan shortly.
- The NRC staff discussed the status of the audit reports associated with a November 13 -16, 2012, audit at the Invensys Operations Management facility in Lake Forest, California. The audit plan dated October 10, 2012, associated with this audit is available in ADAMS at Accession No. ML12276A050. The staff noted that two following separate audit reports are being written: 1) a cyber security audit report, and 2) an audit report associated with the audit that was

performed to verify that the software products to be used at DCPD for the PPS system conform to applicable standard, guidelines, plans, and procedures by assessing the implementation of the systems developmental life cycle process (life cycle audit

Both of the audit reports will be issued to PG&E shortly. Because the cyber security audit report contains security-related sensitive unclassified non safeguards information the cyber security audit report will be withheld from the public. The staff took an action to support phone calls with PG&E and Invensys as necessary to discuss results of the audits.

- The project plan for the review of the LAR (Enclosure 3) was discussed and the major upcoming milestones were confirmed. The project plan will be updated as appropriate and discussed at the next public meeting.
- The NRC staff stated that it should be issuing a second round of requests for additional information (RAIs) shortly. Once the RAIs are issued the items identified in Enclosure 2 as needing RAIs will be closed and removed from the open item tracking list. This is because the RAIs themselves will be used to track the closure of the issue.
- PG&E took an action to provide documents associated with open item number 76 in Enclosure 2 by the end of January.

Please direct any inquiries to me at 301-415-1132 or at Joseph.Sebrosky@nrc.gov.



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

Enclosures:

1. List of Attendees
2. Staff Identified Issues That are Open
3. Project Plan

cc w/encls: Distribution via Listserv

LIST OF ATTENDEES
JANUARY 24, 2013, TELECONFERENCE MEETING WITH
PACIFIC GAS AND ELECTRIC COMPANY REGARDING
DIGITAL UPGRADE FOR DIABLO CANYON
POWER PLANT, UNIT NOS. 1 AND 2
DOCKET NOS. 50-275 AND 50-323

<u>NAME</u>	<u>ORGANIZATION</u>
Ken Schrader	Pacific Gas and Electric
Scott Patterson	Pacific Gas and Electric
G. Hough	Pacific Gas and Electric
John Hefler	Altran
R. Lint	Altran
J. Mauck	Altran
Ted Quin	Altran
J. Basso	Westinghouse
W. Odess-Gillet	Westinghouse
Stephanie Smith	Westinghouse
Roman Shaffer	Invensys/Triconex
Rich Stattel	Nuclear Regulatory Commission (NRC)
Bill Kemper	NRC
Rossnyev Alvarado	NRC
Shiattin Makor	NRC
Jennie Rankin	NRC
Alan Wang	NRC
Eric Lee	NSIR
Chris Chenoweth	NSIR
George Simonds	NSIR
Michael Shinn	NSIR
Steve Kane	AREVA
Gordon Clefton	Nuclear Energy Institute
Ken Thompson	Avila Valley Advisory Council
Ken Scarola	Nuclear Automation
Yuichi Tanaka	Mitsubishi Nuclear Energy

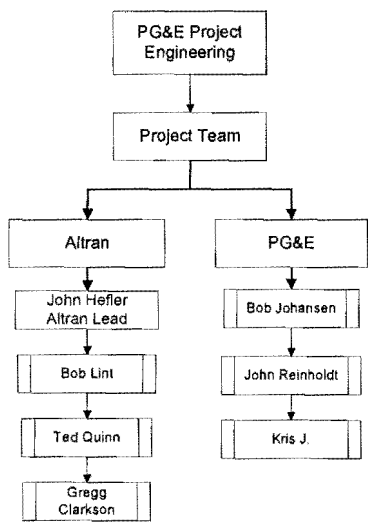
No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
21	RA	<p>Westinghouse/CSI document 6116-00005, "Diablo Canyon PPS System Test Plan," states that the ALS-102 FPGA design is changed for the DCPPS System. Further, Section 5.3.3 states: "Test as many of the ALS-102 requirements as possible."</p> <p>Please identify what document describes the design verification test for this board.</p>	<p>PG&E response: The documents that describe the design verification tests for the ALS-102 are 6116-70140, "Diablo Canyon PPS System Test Design Specification," submitted June 6, 2012, and 6116-10216, "Diablo Canyon PPS VV Simulation Environment Specification" that will be placed on the Sharepoint by January 31, 2013 and submitted by February 21, 2013.</p>	Open	RAI 10 Not used (Hold until response is received)		<p>12/19/12 update: Westinghouse/ALS will submit the documents by 12/31/2012.</p> <p>10-17-12 update (Alvarado): Westinghouse/ALS will submit the documents by 10/31/2012.</p> <p>9-19-12 update (Alvarado): Waiting for ALS document to be submitted at the end of September.</p> <p>6-13-12 update (Kemper): PG&E understands that they need to provide an update to this response. In the meantime, PG&E and ALS have provided 2 design specifications that will address this OI. These documents are placed on the PG&E sharepoint website. Doc. No</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
							<p>6116-10740 was submitted on June 6, 2012, which describes ALS system test design specification. Doc. No 6116-00005 was also submitted on June 6, 2012, which describes ALS system test plan.</p> <p>Doc. No. 6116-10216 ALS VV Simulation Environment Specification will be provided in the future.</p> <p>3/21/12 update: PG&E has created a share point website for NRC to review PPS design drawings that will address this issue. NRC staff will determine if they are needed to be submitted on the docket. PG&E will ensure the website information is only applicable to this licensing</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
							<p>action.</p> <p>NRC- the response provided does not address the question.</p> <p>7/13/12 – rjs Deleted RAI 10 pending review of revised response. Also decided to hold item open.</p>
33	RJS	<p>(ALS SQAP) Software tools are used extensively during the FPGA development process. The staff therefore considers these tools to be a key component to the assurance of quality in the ALS system development process. The ALS SQAP states that "no additional tools, techniques, or methodologies have been identified" for the ALS system. The staff considers the development tools, as well as the techniques and methodologies used during system development to be relevant to the assurance of quality for the ALS system. Please provide information on the tools, and methodologies used during system development to ensure quality of the ALS system products.</p> <p>PG&E response: Westinghouse agrees that Section 8, Tools, Techniques, And Methodologies of the ALS QA Plan (6002-00001) should be revised to reference document 6002-00030, "ALS Design Tools." This document describes the tools used and how they are used in the design process. This document is also on the ALS docket. Westinghouse submitted a revision of the ALS QA Plan, Revision 9, on the ALS docket on October 31, 2012, that provides information on the tools and methodologies used.</p>		Closed			<p>Item initiated on 6/5/12.</p> <p>6-13-12 update (Kemper): W/ALS agrees with NRC's position on tools and will revise the document (Doc. No. 6002-00001) accordingly to address this matter.</p> <p>Placed this item on hold pending review of revised QA plan.</p> <p>RJS-Verified that Rev. 9 of QA Plan refers to 6002-00030 which</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
							includes Tool identification and assessments.
35	RA	<p>Follow up of Item 21 – Software Test Plan</p> <p>In the response provided for Item 21, PG&E explained that a new revision (Rev. 1) of ALS document No. 6116-00005 was provided. The scope of Revision 1 is slightly different from the scope described in Rev. 0. For example, Section 1.2 in both revisions states that test coverage includes all ALS modules, backplane, license sense modules (LSM), and ALS service unit (ATU). However Section 2, Test Items, for these revisions are different. Revision 1 only focuses on ALS-102 and backplane assemblies. This section does not include other ALS modules, LSM and ATU. Please explain why these other ALS modules are not included in section 2 of the new revision.</p> <p>Further, Table 1-2 identifies “Diablo Canyon PPS Test Plan” as document No. 6116-00005, which is the same number than “Diablo Canyon PPS System Test Plan”. Please clarify if this is referring to a different document.</p> <p>PG&E Response: The scope of both revisions are the same. Revision 1 changes added more detail into the overall scope. The details are broken down into 2 main parts: 1- The individual components, 2 – The System components. Both parts equal the entire ALS based Diablo Canyon system which includes all ALS modules, Backplane, ASU (incorrectly stated as ATU in the open item), LSM, ALS-102A/B specific to Diablo and full ALS sub-system test which includes the testing of ALS slave cards required by the DCPD configuration.</p> <p>The entry in Table 1-2 for the Diablo Canyon PPS Test Plan, 6116-00005 is the same document as Diablo Canyon PPS System Test Plan 6116-00005.</p>	Closed	RAI 21			

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
38	RA	<p>Software Management Plan</p> <p>Section 2 of the PG&E "PPS Replacement Concept, Requirements, and Licensing Phase 1 Project Plan" does not describe the activities to be performed by the Engineering of Choice Design Change Package Team.</p> <p>It is also not clear what the roles and responsibilities of this team are. Please clarify and provide the applicable PG&E control document that describes PG&E roles and responsibilities specifically for the Engineering of Choice Design Change Package Team.</p>	<p>PG&E Response: The activity performed by the Engineering of Choice Design Change Package Team is to support PG&E in development of the design change package for the PPS Replacement. PG&E has a contract with an engineering company, currently Enercon Services, Inc., to be the "engineer of choice" to provide nuclear engineering services to PG&E. For individual scopes of work, PG&E develops a purchase request for the scope of work and a purchase order is issued to the engineering company that is the engineer of choice. When the engineer of choice is performing a design change package for Diablo Canyon Power Plant, the engineer of choice uses the PG&E Design Change Procedure, CF3.ID9, "Design Change Development" and PG&E performs an owner acceptance of the work using PG&E Procedure CF3.ID17, "Design and Analysis Documents Prepared by External Contractors."</p>	Closed	RAI 22		
39	RA	<p>Software Management Plan</p> <p>Figure 2-1 of the PG&E "PPS Replacement Concept, Requirements, and Licensing Phase 1 Project Plan" and Figure 3-1 of the SyQAP identify Altran under the PG&E Project Engineering box. However, Figure 4-1 of the SyVVP identifies PG&E project team under the PG&E Project Engineering box. Please explain the role and responsibilities for Altran during the PPS Replacement Project.</p>		Closed	RAI 23		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>PG&E Response: 09/17/2012:</p> <p>1. The PPS Organization Chart shown in SyVVP Figure 4-1 is a simplified rendering of the organization charts in Project Plan Figure 2-1 and SyQAP Figure 3-1. The latter figures show an Altran Project Team under PG&E Project Engineering and a team of three PG&E individuals directly under PG&E Project Engineering.</p> <p>The slight inconsistency between SyVVP Figure 4-1 and the other figures may be resolved thus:</p> <div><pre>graph TD A[PG&E Project Engineering] --> B[Project Team] B --> C[Altran] B --> D[PG&E] C --> E[John Heffler Altran Lead] E --> F[Bob Lint] F --> G[Ted Quinn] G --> H[Gregg Clarkson] D --> I[Bob Johansen] I --> J[John Reinholdt] J --> K[Kris J.]</pre></div> <p>2. Altran is acting as a subcontractor providing engineering support to the PG&E Project Team as shown above in the revised figure. Altran supported LAR preparation and is providing continuing support through the LAR review process. Altran's work is governed by the Altran Engineering Procedures Manual. Documents submitted to PG&E are prepared in accordance with Altran EOP 3.3 (reports) and 5.4 (specifications). All Altran documents are verified in accordance with Altran EOP 3.4. In addition, PG&E accepts Altran documents under PG&E CF3.ID17 as noted in the Altran</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		Verification Report.					
40	RA	<p>Software Tools</p> <p>In the ALS Progress Update 2012-08-01 provided to the staff, Westinghouse/CSI described that they are replacing Automated Test Environment (ATE) from IVV credited tools with a LabView based ALS Board Test System (ABTS). Also, in this presentation, Westinghouse/CSI noted that they are performing additional IV&V and equipment qualification tools.</p> <p>Since this information needs to be reflected in the software planning documents, please identify how these items will affect Westinghouse/ALS documents related to PPS replacement project. Also, identify what document will be revised to include description of these modifications.</p> <p>PG&E Response: The ALS Design Tool 6002-00030 requires revision to replace the ATE with the ABTS. The revised ALS Design Tool, Revision 9, document includes the ABST tool and was submitted by Westinghouse to the NRC on January 18, 2013 that addresses the tools used.</p>		Re- OPEN			<p>01/10/2013 update: The ALS Design Tool 6002-00030 Rev.8 indicates that Westinghouse/CSI is using ATE. Further, Rev 7 of the 6002-00003, ALS V&V Plan, states that this plan was revised to identify ABTS as the primary board integration level test tool, replacing ATE. Please clarify the discrepancy between the response provided and the information in Rev. 8.</p> <p>12/19/12 update: ALS Design Tool 6002-00030 was submitted to the NRC. NRC Staff will review this document and identify follow up</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
							questions, if necessary, creating a new open item. 10/17/12 update: Westinghouse/ALS will submit the ALS Design Tools on 10/31/2012
41	RA	<p>Software V&V and Test Plan</p> <p>Westinghouse/ALS document 6116-0005, section 8.2 identifies the software tools to be used in the PPS replacement project. However, this list is not consistent with the list of IV&V tools identified in Section 3.6 of ALS VV Plan 6002-00003. Specifically, the test tools identified in 6002-00003 are not listed in 6116-00005 and vice versa. For example, the VV Plan (6002-00003) identifies ATE tool for IV&V, but this tool is not listed in 6116-0005 Rev. 1. Furthermore, the staff reviewed 6116-0005 Rev. 0, and found that the ATE tool was listed in this version. Please clarify what software tools will be used and what document describes them.</p> <p>PG&E Response: A new revision of the ALS V&V Plan 6002-00003, Revision 7, Figure 3-2, identifies the ABTS and the ISE as the IV&V test tools. This new revision was docketed October 31, 2012 on the ALS platform docket. The ATE is removed from the set of IV&V test tools. The tools listed in document DCPD PPS Test Plan 6116-00005 section 8.2 and the tools listed in DCPD PPS VV Simulation Environment Specification, 6116-10216, (to be released by 30 September 2012) encompass the IV&V test tools in the new revision of the ALS V&V Plan, 6002-00003.</p>	Re-Open	RAI 24		01/10/2013: See comment provided in item 40. Also, DCPD PPS VV Simulation Environment Specification, 6116-10216, has not been submitted.	
42	RA	<p>Software V&V</p> <p>PG&E "PPS System Replacement System Verification and Validation Plan (SyVVP)" does not describe the V&V activities to be performed during the Operation Phase and Maintenance Phase. This document states that these activities are covered by approved DCPD procedures. Please identify these DCPD procedures.</p>	Closed	RAI 25		9/17/12 update (Alvarado): during the conference call PG&E explained that modifications to the systems will be performed by	

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>PG&E Response:</p> <p>Per the response to OI #28, control of the software modifications to the Tricon and ALS platforms once the PPS replacement project is completed, and the PPS is in the Operations and Maintenance phase, will be by the Process Protection System Replacement Software Configuration Management Plan, SCM 36-01, Revision 0, which was submitted as part of the Phase 2 document submittal on June 6, 2012, in Attachment 4 to the Enclosure of PG&E Letter DCL-12-050. Modification to the PPS Replacement components produced by the vendors, CS Innovations and Invensys Operations Management, will be performed by the vendors and verification and validation will be controlled by the vendor verification and validation plans created for the Diablo Canyon PPS Replacement (6116-00003 for CS Innovations and 993754-1-802 for Invensys Operations Management).</p>					the vendors. PG&E will provide additional information on their plan to perform modifications to the PPS system during operation and maintenance.
43	RA	<p>Software V&V</p> <p>PG&E "PPS System Replacement System Verification and Validation Plan (SyVVP)", Section 5.1.1, explains that during the Concept Phase, PG&E will verify system requirements in accordance with PG&E procedure CF2.ID9, "Software Quality Assurance for Software Development." However, Procedure CF2.ID9 is for in-house development of software applications. Please explain how this procedure is going to be used for the PPS replacement project.</p> <p>Further, Section 5.1.2 of the CF2.ID9 states that an independent review of the functional requirements prepared during the concept phase would be performed. The PG&E SyVVP does not identify this review, and thus there is no specific V&V product for this phase. Please identify who will perform this review and if this is considered a V&V product.</p>		Closed	RAI 26		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		PG&E Response: 09/17/2012: Altran developed the PPS Replacement FRS during the Concept phase in accordance with Altran EOP 5.4, and verified it in accordance with Altran EOP 3.4. Altran used PG&E procedure CF3.ID16 for additional guidance. PG&E accepted the FRS under CF3.ID17, which constituted verification of system requirements. This was a design activity rather than a V&V activity and there is no specific V&V product for this phase.					
45	RA	<p>Follow up of item 18 - Software V&V</p> <p>RG 1.168 identifies five of the activities in IEEE Std.1012-1998, Annex G, "Optional V&V Tasks," as being considered by the NRC staff to be necessary components of acceptable methods for meeting the requirements of Appendices A and B to 10 CFR Part 50 as applied to software. These tasks are:</p> <ol style="list-style-type: none"> 1. Audits 2. Regression Analysis and Testing 3. Security Assessment 4. Test Evaluation 5. Evaluation of User Documentation <p>Westinghouse/ ALS Document No. 6002-00003, "ALS VV Plan" describes the following techniques for V&V: reviews, testing, traceability analysis, inspection/analysis, and IV&V regression (change) analysis. This plan does not include any of the optional V&V activities identified in IEEE Std.1012-1998, Annex G. Please explain if these activities are performed.</p>		Closed			<p>12/19/12 update: NRC Staff will review the document submitted and identify follow up questions, if necessary, creating a new open item.</p> <p>10/17/12 update: Westinghouse/ALS will submit the DCPV V&V plan on 10/31/2012</p>
		PG&E Response: The DCPV VV Plan has been revised to include these optional V&V tasks required by RG 1.168 to align with the new ALS VV Plan for the Optional Tasks. The Diablo Canyon VV Plan, Revision 1, was placed on the Sharepoint on November 22 and was submitted by PG&E on December 5 in PG&E Letter DCL-12-121.					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
46	RA	<p>Software V&V</p> <p>Several sections in the Invensys Software Verification and Validation Plan (SVVP) reference "applicable Project Procedure Manual (PPM)" to perform certain activities. The reference section in this plan identifies PPM (Reference 2.4.4). It is not clear if the PPM is constituted by several procedures or if it is only one procedure. For example, Section 1.1, states the SVVP was prepared in accordance with PPM 7.0 (Ref. 2.4.4), and then Section 4 states that V&V activities will be planned and scheduled in accordance with the applicable PPM. Please describe what the PPM is, and explain how this is going to be used in the PPS replacement project.</p>	<p>PG&E Response: The Project Procedures Manual (PPM) provides appropriate controls for project activities conducted at the Invensys Operations Management (Invensys) Lake Forest facility. These controls will ensure that all nuclear Class 1E projects (or non-1E projects where the customer has specified certain 1E requirements) processes, project activities, and project documents will meet the requirements of 10 CFR 50, Appendix B, 10 CFR Part 21 and the Invensys Quality Management System. This procedures manual provides specific controls for NAD as well as other Invensys organizations that perform nuclear safety-related system integration project activities. The PPM is a collection of different procedures, including referenced Forms, and is a controlled document. Each PPM procedure is intended to implement key areas of project activities. Each procedure within the PPM is assigned a unique document number and title.</p> <p>V&V activities during the PPS Replacement Project will be governed by several procedures within the PPM as defined in the SVVP document, Invensys document 993754-1-802. The SVVP will be revised to add the title of each procedure within the PPM where referenced in the SVVP. For example, in the SVVP, Section 1.1, where it states that, "the SVVP was prepared in accordance with PPM 7.0 (Ref. 2.4.4)," will be revised to state that "the SVVP was prepared in accordance with PPM 7.0, <i>Application Program Development</i>." The revised SVVP will be submitted by TBD.</p>	Closed	RAI 27		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
47	RA	<p>Software V&V</p> <p>Invensys Document No. 993754-1-802, "Software Verification and Validation Plan" requires the use of V&V metrics to evaluate software development process and products. This section does not explain what methods and criteria will be used for software safety metrics. This information is required by section B.3.1 of BTP 7-14, RG 1.152, RG 1.173 and IEEE Std. 1061 and 1074. Also BTP 7-14 Section B.3.1.1.2. Please provide this information.</p> <p>PG&E Response: The V&V metrics are used during development of the PPS Replacement software that will reside/execute on the V10 Tricon portion. The V&V metrics measure the thoroughness of V&V reviews and testing efforts. These measurements yield data utilized to gain reasonable assurance that the design outputs are of high quality commensurate with the intended use in the PPS Replacement application. The V&V metrics methodology, utilizing a diversity of software measures, provides insight into the rigor of the PPS software development process. V&V uses three distinct metrics during PPS software development:</p> <p>Software Quality Metrics</p> <p>The purpose of these metrics is to measure software quality by tracking the number of defects found in the design outputs (e.g., design documents, software).</p> <p>The method is to count and categorize defects found during V&V review of design outputs.</p> <p>The acceptance criterion is that no technical defects remain at the end of the current phase to receive V&V recommendation to proceed to the next project phase. Any defects that cause the non-compliance with customer requirements and/or non-compliance with NRC guidance are considered technical defects.</p> <p>V&V Effectiveness Metrics</p> <p>The purpose of these metrics is to measure the effectiveness of V&V</p>		Closed	RAI 28		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>reviews by measuring the percentage of design outputs which V&V reviews or tests. The method determines the percentage of design outputs actually reviewed by V&V (which is meaningful for in-process design changes necessitating a change impact analysis, revisions to released design outputs, and a regression analysis). The Acceptance Criterion is that 100 percent of comprehensive or delta change reviews is achieved in the current phase to receive V&V recommendation of proceeding to the next project phase.</p> <p>Software Safety Metrics</p> <p>The purpose of these metrics is to assess whether software safety requirements are being met. Methods are to count software hazards found during V&V review or testing of design outputs and to confirm software hazard mitigation in each project phase, or, at a minimum, by the end of the project and approval at the completion of acceptance testing. The Acceptance Criterion is that all software hazards are mitigated by the end of the Test Phase to receive approval of the results of acceptance testing.</p>					
48	RA	<p>Software V&V</p> <p>PG&E SyVVP, Section 6, requires that anomalies detected are identified, documented, and resolved during the V&V activities. This section states that anomaly reporting and resolution requirements are defined in the respective PG&E control procedures. Section 2 "Control Procedures does not include a reference for an anomaly reporting procedure. Please identify the PG&E control procedure used for anomaly reporting.</p> <p>Further, Section 7 of the SyVVP states that the PG&E authority responsible for approving deviations from SyVVP is the PG&E Project Manager, who will document his/her approval a Change Notice or equivalent formal PG&E document. Please identify where the responsible PG&E authority will document its approval.</p>		OPEN			<p>12/19/12: item 2 still pending</p> <p>10/17/12 update: For item 2 – PG&E will revise the SyVVP and submit it on 11/30/2012</p> <p>9/17/12 update (Alvarado): NRC staff received copies of OM7.ID1 and XI1.ID2. This</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>PG&E Response:</p> <ol style="list-style-type: none"> 1. The PG&E control procedure for anomaly reporting is OM7.ID1, "Problem Identification and Resolution." This procedure governs the PPS replacement after it has been turned over to PG&E by the suppliers. The suppliers' anomaly reporting procedures are applicable prior to this turnover. 2. The responsible PG&E Project Manager will document approval in an SAP notification. This will be included in the revision of the SyVVP currently in progress. It is noted that Section 7 of the SyVVP states the deviation shall be incorporated into the SyVVP as a revision at the first practical opportunity. 					addressed item 1 of this open item.
49	RA	<p>Software V&V</p> <p>Invensys Document No. 993754-1-802, "Software Verification and Validation Plan", Section 6.3 states that the Invensys personnel prepared System Deficiency Integration Report (SDIR) to document non-conformances and corrective actions during testing; the SDIR is prepared in accordance with PPM 10.0. Please explain what PPM this is.</p> <p>Further, the Invensys "Validation Test Plan", Section 5.4.2 states that the Test Review Board and PG&E shall review SDIRs, but this is not indicated in the Invensys V&V plan. Please explain why this review activity is not identified as a V&V task in the V&V Plan.</p> <p>PG&E Response: The PPM 10.0 procedure defines the process to control nonconforming items and identify appropriate corrective action for all nuclear application projects developed at the Invensys Operations Management (Invensys) Lake Forest facility. This procedure is intended to provide controls for nonconforming items and corrective actions related to project activities. As used in this procedure, the term "nonconformance" describes deficiencies in parts and materials (items), documentation, and/or deviations from stated requirements. This procedure addresses the identification, documentation, evaluation, and disposition of nonconforming items. This procedure also describes the corrective action process to be used for project-related issues where corrective action is warranted.</p>		Closed	RAI 29		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		SVVP Section 5.2.2.2.1 4) stated that Nuclear IV&V shall generate and verify the system-level Validation Test Plan, 993754-1-813, in accordance with PPM 6.0 [Ref 2.4.4], in conjunction with IEEE 829-1983. The SVVP was developed in accordance with PPM 6.0, Test Control. In PPM 6.0, Test Control, it was stated that the Project Review Committee (PRC) shall review all test results for completeness, accuracy and acceptability. This review shall include all test documentation, e.g., the Test Procedures, the Test Logs, the System Integration Completion Checklist, the Test Report(s), and SIDRs.					
50	RA	<p>Software V&V</p> <p>The Invensys Validation test plan, Section 8.2, states that the Narrative Test Logs are used to document conduct of testing and any anomalies that occur. Please explain if this is only used during validation, and why this is not mentioned in the Invensys SVVP. Further, please explain how is this used in conjunction with Document Review Comment Sheet (DRCS) and System Deficiency Integration Report (SDIR)?</p> <p>PG&E Response: PPM 6.0, Test Control, defines the Test Logs. All test activities shall be recorded in a Test Log. The Test Log constitutes a continuous, hand-written journal of all test activities from the point of initial entry into the Test Procedure until the conclusion of all testing, including any required retesting. The Test Log shall include entries for sign-in and sign-out of all participating personnel, establishment of indicated prerequisites and initial conditions for testing, performance of testing and retesting, identification of problems, etc. The Test Log is intended to be a detailed journal of all testing activities sufficient to fully document the actual sequence of testing performed, the test results achieved and any problems that occurred, including their impact on test performance. The Test Log shall be reviewed by the PRC as part of its evaluation of the test results.</p> <p>The Test Logs are independent and separate from the Document Review Comment Sheet (DRCS) and System Deficiency Integration Report (SIDR). However, as a test narrative, the Test Log may identify the fact that a SIDR was generated as a result of test anomaly.</p>		Closed	RAI 30		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
51.1.a	RA	<p>Software Configuration Management</p> <p>1. Configuration Process</p> <p>a) In open item 4, the staff requested description of the software configuration management activities for configurable boards (e.g., ALS FPGA-102 board). Since the ALS FPGA-102 board is customer specific, its configuration management activities are not covered by "ALS Configuration Management Plan." Even though item 4 is closed, this request was not addressed in the response for item 4.</p>		Closed	RAI 31		
		<p>PG&E Response: 09/18/2012 ALS-102 Configuration</p> <p>The FPGA installed on the ALS-102 board and therefore the ALS-102 board itself is specific to the PPS Protection set and the ALS subsystem in which it is installed. PG&E will not have the capability to alter the FPGA. Any change to the FPGA must be made by CS Innovations. Therefore, ALS-102 FPGA configuration management activities are covered by the ALS Configuration Management Plan. PG&E capability to change ALS-102 configuration will be limited to board-level replacement.</p>					
51.1.b	RA	<p>Software Configuration Management</p> <p>1. Configuration Process</p> <p>b) The PG&E SCM 36-01, item 1.2.8, states that ALS board has two sets of NVRAM. Further, it explains that the configuration of the NVRAM can be changed only by removing the subject board from the ALS chassis and inserting it into a special test fixture. It is not clear who will control this process and configuration of the NVRAM. Please explain.</p>		Closed	RAI 32		
		<p>PG&E Response: 09/18/2012</p> <p>ALS I/O boards are generic; that is, each board is configured using its NVRAM for the specific function it is to perform. This activity is described in SCM 36-01 Section 1.2.8, which states that the configuration of the NVRAM is changed by removing the subject board from the ALS chassis and inserting it into a special test fixture. This would be performed as part of a</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>maintenance activity, such as replacing a failed board. If the functionality of an I/O board required modification as a result of an application change, all required NVRAM configuration alterations would be performed by CS Innovations under their ALS Configuration Management Plan.</p> <p>As with the ALS-102 FPGA discussed above, PG&E will not have the capability to alter the NVRAM configuration itself. PGE capability to change the NVRAM configuration for a specific I/O board will be limited to loading NVRAM images that are under CS Innovations configuration control and that have been previously verified and validated at the system level by CS Innovations.</p> <p>Configuring the NVRAM in order to replace an I/O board will be performed by PG&E under an approved plant maintenance procedure.</p>					
51.1.c		<p>Software Configuration Management</p> <ol style="list-style-type: none"> 1. Configuration Process c) Section 1.2 of the Invensys Document No. 993754-1-909, "Software Configuration Management Plan," states that this plan controls operating system of the computers used to run TriStation 1131 and the signal simulation software used for testing purpose. However, the description provided throughout the plan only focuses on the configuration activities for the TSAP (e.g., Section 2.3 states that the SCM procedures are for the TSAP). Further, this same section (later on) identifies the software configuration to be managed, and this list does not include operating system of the computers used to run TriStation 1131 and the signal simulation software used for testing purpose. Please clarify the scope of this plan. 	<p>PG&E Response: 09/18/2012 There was no intent for the SCMP to do more than track the revision of Commercial Off The Shelf (COTS) software. In this case "Control" is defined as tracking the revision levels such that they are recorded on the</p>	Closed	RAI 33		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		project Master Configuration List, Invensys project document 993754-1-803. On page 7 of the SCMP, under "Limitations," it states, in part, that the revision levels of this type of software will be tracked.					
51.2		<p>Software Configuration Management</p> <p>2. Organization</p> <p>The organization and responsibilities described in Section 4 of CF2.ID2 is not consistent with the information presented in Section 2 of SCMP 36-01. For example, Section 2 of SCMP 36-01 identifies system coordinator, application sponsor, and system team, who are not identified in Section 4 of Cf2.ID2. Further these descriptions are not identified in the project organization described in PG&E PPS Replacement Plan (Attachment 3 of the LAR). Please clarify the roles and responsibilities for SCM, and provide a cross reference of the PG&E organizations described in these documents.</p> <p>PG&E Response 12/16/2012:</p> <p>PG&E will revise the SCMP plan to be consistent with CF2.ID2 section 4 organization, including a description of additional roles and responsibilities not required by CF2.ID2.if needed.</p>		Open			<p>12/17/12 update: Waiting for PG&E to revise SCMP.</p> <p>10/17/12 update: PG&E will revise the SCMP to address several open items</p>
51.3.a		<p>Software Configuration Management</p> <p>3. Changes and Problems Identification</p> <p>a) PG&E SCMP36-01 states that software, hardware, and configuration problems are reported in accordance with PG&E OM7.ID1 and that software and/or configuration problems are reported via a PROG PDCM Notification. Please clarify when and how these are used. For example, for software problems does one have to report the problem using both PG&E OM7.ID1 and PROG PDCM Notification. Note that PG&E CF2.ID2 states that all problems associated with plant computer system should be reported and document per OM7.ID1 (See section 5.11 and 5.16.10 (b) of CF2.ID2)</p> <p>Further, Section 3.2.1 states that all PPS modifications should be initiated and tracked per plant procedures or CF4.ID1. Section 3.2.2 states that the implementation of the change is documented in the</p>		Open			<p>12/19/12 update: response pending</p> <p>10/17/12 update: PG&E will revise the SCMP to address several open items</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>associated Change Package and a SAP notification and order. And Section 3.2.10 states that all identified problems and corrective actions using a notification, which is not specified.</p> <p>So should software modifications require reporting and tracking using OM7.ID1, CF4.ID1, PROG PDCM Notification, Change Package, and SAP Order?</p> <p>Please explain PG&E procedures for different changes and the documenting and tracking system used for all types of modification</p> <p>PG&E Response: a) All problems are entered into the corrective action program using PG&E administrative procedure OM7.ID1 and are required to be entered into an SAP (electronic business management software) notification (electronic tracking document). Notifications can be identified as different Work Types in order to categorize the type of problem, the priority of the problem, and to facilitate routing the problem to appropriate personnel needed to review and resolve the problem. A "PROG PDCM" type notification is a program (PROG) plant digital configuration management (PDCM) type of problem and software and configuration problems are examples of problems that would be assigned a Work Type of "PROG PDCM" in the notification. Plant hardware problems are assigned a Work Type of "EQPR" to identify the problem as an equipment problem.</p> <p>Plant modifications, including software modifications, are requested using plant procedure CF4.ID1, "Plant Modification Request and Approval" and the modifications are performed using paper/electronic image based change documentation (Change Package) and are tracked in SAP using a notification and an order. An order is an electronic tracking document that allows detailed tracking of job requirements, parts, details, schedule, and approval.</p>					
51.3.b		<p>Software Configuration Management</p> <p>3. Changes and Problems Identification</p> <p>b) Please clarify the means to track changes. Section 3.2.4.7 of the SCM 36-01 states that this is done using a SAP order, but Section 3.2.4.7 states that Change Package and SAP order are entered in the Record Management System, and Section 3.3 describes a Configuration Status Account , which is used to track changes of</p>		Closed	RAI 34		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		configuration items.					
		PG&E Response: The means to track changes is the SAP order. The Record Management System is the system used at Diablo Canyon to store and allow retrieval of documents to meet 10 CFR 50 Appendix B quality assurance requirements. Completed Change Packages and SAP orders are entered into the Record Management System for storage and to allow later retrieval.					
51.4.a		<p>Software Configuration Management</p> <p>4. Document Repository</p> <p>a. SCM 36-01, Section 2.3.3 identifies the Digital Systems Engineering SourceSafe as the repository, but Section 3.2.5.5 identifies http://dcp142/idmws/home/asp, and Section 3.29 states that the files necessary for recovery of the baseline are maintained in the PPS database in SC-I-36M, Eagle 21 Tunable Constants." It is not clear if these two sections are referring to the same document repository or if it is the same. Please clarify.</p>		OPEN			12/19/12: response pending
		PG&E Response: The SourceSafe is used for executable files (exe files), source code, program code, and database files, etc. The link http://dcp142/idmws/home/asp is to FileNet, an electronic file storage system. FileNet is used to store documentation like the PPS Replacement Project documents (e.g., Software Configuration Management document, Functional Requirements Specification, Interface Requirements Specification, etc.					
51.4		<p>Software Configuration Management</p> <p>4. Document Repository</p> <p>b. PG&E has implemented restrictions to access files and documents associated with PPS replacement project. Further, PG&E requires user authentication and access to edit configuration, software, and data. It is not clear if these restrictions apply for access to the Digital Systems Engineering SourceSafe or the repository in http://dcp142/idmws/home/asp</p>		OPEN			12/19/12: response pending

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		PG&E Response: Microsoft SourceSafe requires special permissions to access the appropriate directory and then requires a login and special software to access the files. FileNet allows files to be viewed without a special login, but to modify, delete, or add, files special permissions need to be assigned.					
52	RJS NSIR	<p>Security:</p> <p>PG&E stated in its letters DCL-11-123 and DCL-11-104 that the PPS replacement will be fully compliant with the 10 CFR 73.54 cyber security requirements, including RG 5.71, Revision 0, "Cyber Security Programs for Nuclear Facilities," dated January 2010, and is being reviewed to comply with 10 CFR 50.73, the DCPD Cyber Security Plan, and NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6, dated April 2010. The cyber security program that PG&E is implementing per its NRC approved cyber security plan includes provisions applicable to all phases of a systems' life cycle, including the digital upgrade or modification of critical digital assets.</p> <p>Please explain how the provisions outlined in the PG&E's NRC-approved cyber security plan were considered, and/or implemented, as part of the PPS replacement. The provided explanations should include how all of the management, operational, and technical security controls contained within the plan, especially security controls associated with Configuration Management and System and Service Acquisition, are being addressed. The provided explanations should also include any issues associated with partial implementation of the PPS replacement and full implementation of the cyber security plan for the site, and processes to identify and resolve any such issues.</p>		OPEN			1/16/2013 – Require NSIR input prior to closing this item. Requested NSIR to either provide written response or discuss the status of this item at the 1/24/13 conference call.
		<p>PG&E Response:</p> <p>The Cyber Security program manager and other members of the CSAT (Cyber Security Assessment team) met with the Process Protection System</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>(PPS) Upgrade design engineer beginning in 2011. Many options were discussed.</p> <p>The Cyber Security program manager and project manager have met with the procurement group to discuss cyber security principles that should be written into the procurement procedures, and what steps will help to ensure a secure supply chain.</p> <p>The Cyber Security Assessment Team (CSAT) was formed in accordance with section 3.1.2 of the cyber security plan, and Milestone a, on 10/31/2011. A list of critical digital systems and assets was created in accordance with section 3.1.3 of the cyber security plan and Milestone b on 10/31/2011. The CSAT looked at scheduled digital upgrades, and added the future equipment to the list of critical digital systems. The CSAT determined the PPS equipment will be a critical system, with several CDAs.</p> <p>From July 9-12 2012, the cyber security project manager accompanied members of the Quality Verification group to examine the design and production facilities of Invensys, and examined the code production practices and the development environment, and determined that Invensys has an SDE, and ensures their employees are reliable and trustworthy.</p> <p>Activities planned for the future.</p> <p>In December of 2012, the network that the PPS will eventually reside on will be isolated from internet connected networks by a deterministic network device, per milestone c of the DCPD Cyber Security Plan. Thus many network attacks, including many that depend on a back door created by a vendor, will not be possible.</p> <p>Also by December of 2012, DCPD will have taken steps to lessen the likelihood of an attack initiated by a portable electronic device, or portable</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>media such as a thumb drive per Milestone d, and section D 1.19 of NEI 08-09. This will mitigate portable media based attacks that depend on a back door created by a vendor.</p> <p>The DCPD Cyber Security Team will interface with NUPIC (Nuclear Procurement Issues Committee) and the NEI/NITSL counterfeit parts task force to address digital equipment supply chain security.</p> <p>The Cyber Security Implementation Project Manager has developed a detailed project plan, with several tasks and schedules. Several existing plant procedures will be revised. The PPS will inherit the controls implemented by these procedures. Many of the procedures will have been changed/created before the PPS is installed.</p> <p>The CSAT is collecting design information as it becomes available. The collected design documentation is being reviewed as it is collected. The collected documentation will be reviewed in a formal desktop evaluation per the cyber security plan, section 3.1.5 prior to the PPS installation. The test set up in the offsite test lab near the plant will be visited on occasion by the CSAT, the system will be walked down repeatedly during installation, and the final walkdown will be performed when the system is ready to return to operations, per section 3.1.5 of the security plan.</p> <p>The CSAT will make recommendations to enhance the cyber security posture of the PPS upgrade throughout the project, and will make their final recommendations after the system walkdown, per section 3.1.6 of the cyber security plan.</p> <p>Disposition of all controls will be documented in the cyber security assessment tool, CyberWiz. Recommended mitigation will be documented in CyberWiz, and the Corrective Action Program.</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
55	WEK	PG&E Letter DCL-12-050, Phase 2 Documents, Attachment 2 FSAR Changes, FSAR Section 7.1.2.5, Conformance With Other Applicable Documents (page 7.1-13) does not indicate the NRC Safety Evaluation that will be produced to approve the PPS. The staff's SER should become part of the DCPD Unit 1&2 licensing basis once it is issued. How will this be documented within the FSAR??		Closed	RAI 35		Acceptable response. Send this as an RAI so that the issue does not get lost.
		PG&E Response: Reference to the staff SER will be included in FSAR Section 7.2.1.1.6 for the reactor trip portion of the process protection system and to Section 7.3.1.1.4.1 for the engineered safety features actuation system portion of the process protection system.					
56	WEK	PG&E Letter DCL-12-050, Phase 2 Documents, Attachment 2 FSAR Changes, FSAR Section x.x.x.x, (page 7.2-23) states that the evaluation for the common mode failure in the PPS is presented in References 37 [DCPP PPS D3 LTR] and approved in Reference 38 [the staff's SER approving the DCPD PPS D3 LTR]. However, it is noted that in the staff's SER it was stated in several sections that the D3 design features were approved based on "...confirmation that the proposed built-in diversity of the ALS sub-system is found to be acceptable." This confirmation will be provided in the DCPD PPS SER, therefore, the staff's SER should also be referenced in this section.		Closed	RAI 36		Acceptable response. Send this as an RAI so that the issue does not get lost.
		PG&E Response: Reference to the staff SER for LAR 11-07 will be included in FSAR Section 7.2.2.1.2 in addition to the staff SER for the DCPD D3 LTR.					
57	WEK	PG&E Letter DCL-12-050, Phase 2 Documents, Attachment 2 FSAR Changes, FSAR Section 7.2.2.9.2, IEEE 603-1991 Clause 5, Clause 5.12 (page 12) states that "...the communication path between the maintenance workstation and the ALS subsystem is normally disabled with a hardwired switch..." Also, Attachment 3, PG&E PPS Interface Requirements Specification (IRS), Rev.6 to PG&E Letter DCL-12-069 dated August 2, 2012 states in section 1.5.6 "...TAB communications between the ALS and MWS takes place via RS-485 data link. The TAB is physically disconnected from the MWS when the TAB is not in use....the TAB is open at all times unless maintenance is being performed on the ALS..." Please identify administrative controls and design features associated with the PPS that explains how the MWS is disconnected/disabled from the PPS (i.e., a		Closed	RAI 37		Acceptable response. Send this as an RAI so that the issue does not get lost.

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		means of physical cable disconnect, or a safety-qualified hardware switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes) that demonstrate how this hardwired switch disconnects the ALS maintenance workstation from the ALS safety processor.					
		PG&E Response: For the ALS subsystem, instead of using a hardware keyswitch, the ALS subsystem will be administratively controlled by physically disconnecting the communication link to the ALS MWS computer when the Test ALS Bus (TAB) is not being used for surveillance testing, maintenance, and trouble-shooting. This is a PPS replacement design change described in the response to NRC request for additional information in PG&E Letter DCL-12-083 and will be included in a supplement to LAR 11-07.					
58	RJS	ALS FMEA – There are several failure modes identified in Table 4-4 of the FMEA where the System Effects entry provides a description of functions that are not affected by the failure mode instead of stating what the effects of the failure mode are. For example, the System Effects in the ETT failure in line 5b of table 4-4 are that the Alarm Function remains operational. Though this may be the case, it does not state what the effects of the failure mode are. Examples of this can be found in lines 5b, 6a, 6b, 7a, 9h, 9i, 11b, 11c, and 11d.		Close	RAI 38		10/19/12: If I understand the PG&E response correctly, these system effects are being evaluated within the context of the local effects that are also provided in the FMEA. Application

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>PG&E Response:</p> <p>The System Effects entry does describe the functions that are affected by the failure mode. This entry must be read in the context of the entire FMEA table row. For example, the cited row for ETT failure in line 5b discusses the effects of failures of the ALS-402-1 digital output board which sends Alarm Signals to other systems. In the case of Energize to Trip outputs (ETT) a stuck open output channel will prevent the core A rack from being able to actuate the Alarm (in this case a specific instance of an ETT Alarm is cited, the "Containment Pressure in Test Alarm". However, due to the compensating features, which in this case is the redundant implementation of the function in the core B rack, the System Effect is that the Alarm function remains operational. A similar reading applies to the other examples cited.</p>					<p>specific compensating features that influence the systematic effects of these failure modes are thus accounted for within the analysis.</p> <p>Agree to close but would like the PGE response on record. Need RAI.</p>
59	RJS	<p>ALS FMEA – Some of the identified failure modes of the ALS system are detectable only by operator observations, or by means that are not necessarily performed during routine operation or during surveillance testing. See lines 10c, and 12a, What measures will be implemented to ensure that these failure modes would not occur and remain undetected for an indefinite period of time?</p> <p>It is the staffs understanding that all failure modes which are not detectable through normal means such as surveillance tests or channel checks would need to be considered present for the purpose of satisfying single failure criteria for the system.</p>	<p>PG&E Response:</p> <p>Surveillance testing includes visual inspection of the equipment in addition to the specified test cases that demonstrate functionality. Therefore, those</p>	Closed	N/A		10/19/12 – rjs: Response accepted.

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>failure modes that are detected by operator observations will be detected as part of the surveillance test. IEEE Std 379-2000 defines detectable failures as those failures that can be identified through periodic testing or that can be revealed by alarm or anomalous indication. Therefore, such failures do not need to be considered to be present for purposes of evaluating single failure criterion compliance.</p> <p>The specific cases cited are clear examples. Line 10c discusses failures of the local partial trip indicators. Failures of the indicators do not affect the actual trip function. During the test the technician uses the indicators to confirm that the trip action occurs at the appropriate threshold. Thus the act of observation of the failure during surveillance testing is assured. Line 12a discusses failure of the serial link used for continuous monitoring of the ALS health. Failure of this link does not affect the safety functions of the rack, but would be immediately obvious at the workstation used to do the monitoring. This workstation is used in surveillance testing.</p>					
60	RJS	<p>Technical Specifications:</p> <p>In order for the staff to make a determination that the existing technical specifications and surveillance intervals remain acceptable for the replacement PPS system, an evaluation to compare the ALS/Tricon PPS system reliability and performance characteristics with those of the Eagle 21 system must be performed.</p> <p>Pease provide an evaluation summary report to support the application of existing technical specification and surveillance test intervals to the upgraded ALS/Tricon based PPS system. This report is expected to include a quantitative analysis to demonstrate the new system's ability to perform its required safety functions between established surveillance intervals as well as a qualitative (i.e., deterministic) analysis which sites the self diagnosis and fault detection features of the replacement PPS. The report should address the staff's previous findings in Section 4.3, "Applicability of WCAPs to DCP,," of Amendment No. 179, dated January 31, 2005 (ML050330315).</p>		Open	RAI 39		1/16/13-Waiting for Evaluation Summary Report which is due at end of January.

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		PG&E Response: An evaluation summary report to support application of the exiting TS and TS surveillance test intervals will be provided by January 31, 2013.					
61	RA	<p>Software V&V Plan:</p> <p>ALS provided Revision 7 of its V&V plan (6002-00003). This revision provides a mapping and alignment with IEEE Std 1012-1998. This now cause a misalignment with the DCPD V&V Plan, 6116-00003, Thus, the DCPD V&V Plan will need to be revised. Please identify when this new revision will be submitted.</p> <p>PG&E Response: The DCPD V&V Plan, Revision 1 has been created to provide consistency with the ALV V&V Plan. The Diablo Canyon VV Plan, Revision 1, was placed on the Sharepoint on November 22 and was submitted on December 5 in PG&E Letter DCL-12-121.</p>		Closed			<p>12/19/12: NRC Staff will review the document submitted and identify follow up questions, if necessary, creating a new open item.</p> <p>11-28-12 update: The staff will review the V&V plan to determine if this item can be closed.</p>
62	RA	<p>Software Management Plan:</p> <p>Revision 2 of the ALS "Diablo Canyon PPS Management Plan," 6116-0000, Section 2.1 and 2.2, defines the project organization. As described in guidance documents BTP 7-14 and NUREG/CR-6101, licensees need to describe the management aspects of the software development process. Please clarify the following:</p> <p>1. The description provided in this section does not align with the organization structure provided in Figure 2-1. The description provided is not clear. For example, the bulleted list identifies "Scottsdale Operations Director", but then the 1st paragraph refers to Scottsdale Operations Director and ALS Platform & System Director. It is not clear if this is the title for one person or for two. Further, Figure 2-1 does not identify the</p>		Closed			<p>12/19/12: NRC Staff will review the document submitted and identify follow up questions, if necessary, creating a new open item.</p> <p>11-28-12 update: The staff will review the PPS Management Plan and the VV plan to</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>ALS Platform & System Director, if this role is performed by a separated individual. Please clarify this.</p> <p>2. This section states that ALS V&V Plan provide information and the interface between the IV&V team and the PPS replacement project. It is not clear why the ALS V&V plan will provide this information, since the ALS V&V plan is for the generic platform. Please clarify what document contains this information.</p> <p>3. This section states that the WEC Project Manager is responsible for the commercial process interface with PG&E. However, this role is not listed in the bulleted item list and not identified in Figure 2-1. Please clarify this role.</p> <p>4. Figure 2-1 identifies a QA Manager, but this section only describes the QA Lead. Please describe the role and responsibility for the QA Manager.</p> <p>5. Section 4.1, Planning Stage, mentions a "Project Leadership Team," which is not described in Section 2. Please explain the role and responsibilities for this team.</p>	<p>PG&E Response: To address item 1, the Diablo Canyon PPS Management Plan, Revision 3, clarifies in Section 3 the organization details. To address Item 2, the Diablo Canyon IVV Plan, Revision 1, provides information on the interface between the IV&V team and the PPS replacement project. To address items 3 to 5, the Diablo Canyon PPS Management Plan, Revision 3, clarifies in Section 3 the WEC Customer Project Manager is responsible for the commercial process interface with PG&E, the roles and responsibilities of the QA Manager, and the roles and responsibilities of the Project Leadership Team. The Diablo Canyon PPS Management Plan, Revision 3, was placed on the Sharepoint on November 15 and was submitted on December 5 in PG&E Letter DCL-12-121. The Diablo Canyon VV Plan, Revision 1, was placed on the Sharepoint on November 22 and was submitted on December 7 in PG&E Letter DCL-12-121.</p>				determine if this item can be closed
63	RA	<p>Software Management Plan:</p> <p>Revision 2 of the ALS "Diablo Canyon PPS Management Plan," 6116-0000, Section 4.1, Planning Stage, identifies that deliverables from this phase are</p>		Closed			12/19/12: NRC Staff will review the document submitted and identify follow up

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>approved by the "Managerial Review Board." However, this document does not identify the role and responsibilities for this board. Furthermore, the ALS PPS V&V Plan, 6116-00003, Rev. 0 states that IV&V will review the planning stage documents. Please clarify the person/team responsible for this review and their role and responsibilities.</p> <p>PG&E Response: The Managerial Review Board review and the IV&V reviews are two different reviews. The Managerial Review Board gives the final "exit criteria" approval for both the Planning and Development Stages; this Managerial Review Board approval is required for entrance into the next subsequent stage. Their role is clarified in the "exit criteria" details included in Section 4.1's Planning Stage and Development Stage sub-sections. The IV&V team also reviews the planning stage documents according to the criteria in the V&V Plan. Additional details have been added to the Management Plan. The Diablo Canyon PPS Management Plan, Revision 3, was placed on the Sharepoint on November 15 and was submitted on December 5 in PG&E Letter DCL-12-121.</p>					questions, if necessary, creating a new open item.
64	RA	<p>Software Management Plan</p> <p>To close Items 27 and 29, PG&E issued the DCPPS Project Quality Assurance Plan to define the oversight activities to be performed during the PPS replacement project. Section 2 of this plan describes the responsibilities of those involved in oversight activities. However, it is not clear how these roles and responsibilities correlate to the project organization described in PG&E PPS Replacement Plan (Attachment 3 of the LAR) and PG&E PPS Replacement System Quality Assurance Plan (Attachment 4 of the LAR). For example, the Project Quality Assurance Plan describes the responsibilities of the PPS replacement Project Manager, but this role is not described in other documents. Further, the responsibility described seems to align with the responsibility of the PG&E Project Manager. Please explain the relationship, if any, of the roles and responsibilities described in the DCPPS Project Quality Assurance Plan and those provided in other PG&E plans.</p>		Closed	RAI 40		

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>PG&E Response: The "Quality Assurance Plan for Diablo Canyon Process Protection System Replacement" (referred to as the "Project Quality Plan" in response to OIs 27 and 29) was a project specific document created by the Quality Verification group (a Quality Assurance organization) to identify the Quality Assurance tasks to be performed by the Quality Verification group for the project. The "Quality Assurance Plan for Diablo Canyon Process Protection System Replacement" provides the specific plan to be used by the "Supervisor Project QA" identified in Section 3.5.1 (page 19) of the SyQAP and the "Project QA Engineer or Equivalent" identified in Section 3.5.8 of the SyQAP to provide PG&E quality oversight for the project which in part supports meeting 10 CFR 50 appendix B quality assurance requirements for the project.</p> <p>The "Supervisor Project QA" is not identified in the PPS Replacement Project Plan Figure 2-1 (PPS Replacement Project Organization) because they are not part of the Project Organization, but instead provide independent quality assurance oversight of the Project Organization. Section 6.1, "System Quality Assurance Plan (SyQAP)", of the PPS Replacement Project Plan discusses the SyQAP, which in turn references the "Supervisor Project QA" in Section 3.5.1 (page 19) and the "Project QA Engineer or Equivalent" in Section 3.5.8 to provide PG&E quality oversight for the project.</p>					
65	RJS	<p>KVM Switch Questions:</p> <p>See Attachment 3</p>		Open			
		<p>PG&E Response:</p> <p>See Attachment 3</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
66	WEK	<p>Section 4.2.13.1 of the LAR (page 85) states; "... The NetOptics Model PA-CU/PAD-CU¹ PA-CU port aggregator network tap was approved previously by NRC for a similar application in the Oconee RPS 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."</p> <p>In section 3.1.1.5.2.1 of the Oconee SER, the staff approved The NetOptics aggregator Port Tap, Model 96443, No. PA-CU, as a device intended to allow monitoring of a full duplex 10/1 00BaseT Ethernet communication link by copying the communications and sending that copied communications to a one-way simplex communications link. Due to the importance of this one-way communications path functioning properly, the NRC staff performed a detailed review of the design aspect of this one-way communications path. Circuit diagrams on the device itself indicated that the communications using Port C (Port 1 in the case of DCP PPS application) may be capable of two-way communications. Since the original review of Model 96443, part No. PAD-CU Port Tap required NRC staff examination of actual schematic drawings of the circuitry to determine that there was no inbound communications path associated with Port C (Port 1 for the PPS), a similar schematic review for any replacement or updated model of the Port Tap must be evaluated in the same manner (by the licensee) to determine the manner in which it is being used and configured are acceptable, and that do not invalidate the conclusion of this SE that use of the Port Tap provides adequate data isolation between the Gateway computer and the digital RPS/ESPS. The Port Tap</p>		Close	RAI 41		<p>12-19-2012 update: Response acceptable. OI will be closed to a new RAI.</p> <p>11-28-12 update: See 11-28-2012 update question. A new RAI will be added to clarify this inconsistency so it will be on the docket.</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>approved for Oconee was model 96443 PA-CU.</p> <p><i>11-28-2012 Update:</i> <i>The response below still needs further clarification: Section 3.7.2.1 (page 71) of the approved Tricon V10 LTR SER (ML12146A010) states: "The NetOptics Port aggregator Tap, Model 96443, No. PA-CU, or PAD-CU, is a device intended to allow monitoring of a 10/100 BaseT Ethernet communication link by communications and sending that copied information to a separate one-way communications link. Port A of the Port Tap is connected to the TCM, and Port B is connected to the Maintenance Terminal (maintenance video display unit (MVDU))." Since the LAR references the Port Tap approved within the Tricon V10 SER, this model number 96443 may still be confusing to the reader.</i> Please provide the model number of the Port Tap being that PG&C will use in the DCPP PPS and provide an explanation of its equivalency to the Port Tap approved for the Oconee RPS/ESPS LAR.</p> <p>Revised PG&E Response 12/17/2012:</p> <p>The PPS Replacement application will use the NetOptics Model PA-CU network port aggregator tap to isolate the Tricon portion of the PPS replacement from the gateway computer.</p> <p>NetOptics has confirmed via e-mail (Case# 205591) that part number "96443" is the same as PA-CU. It is the old SKU part number for the PA-CU.</p>					
67	WEK	<p>Section 4.2.13.1 of the DCPP PPS LAR (pg. 85) states, "Port aggregator dual in-line package (DIP) switch positions will be controlled by DCPP configuration management processes."</p> <p>Please provide a documented basis (e.g., a plant procedure, or engineering design package) that demonstrates how this will be controlled.</p> <p>PG&E Response: The Port aggregator DIP switch positions will be</p>		Closed	RAI 42		11-28-12 update: Response is acceptable.

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		controlled by a plant procedure or plan. The plant procedure or plan will be developed as part of the design change for installation of the PPS replacement after NRC approval of the LAR.					
68	WEK	<p>Please provide a detailed functional description of the DCPD PPS NSR Gateway Computer(s) system; including computers/processors, communications protocols, and data isolation details, Or, please indicate where this information is explained within the LAR and supporting documents. Also, please provide a detailed explanation of the Gateway Switch discussed within the LAR;including its operating principal (hardware, logic based, etc, ,data/electrical isolation design features, and any other pertinent information pertaining to its failure mechanisms.</p> <p><i>11-28-2012 follow up question:</i> <i>Figure 4-13 (Pg 87) of the LAR indicates that data communications is provided directly between the SR ALS "A" & ALS "B" Protection Sets I, II, III, and IV, and the NSR Gateway Computers via RS-422 copper media (i.e., not through the Port Tap). Section 4.8.2 b) (page 110 of the LAR) states that "...All other communication to non-safety equipment, i.e., Plant Computer, is via continuous one-way communication channels on the ALS-102." Please describe how the 1E/non-1E data communication and electrical isolation is implemented within the ALS for this configuration. Also, explain how the ALS "A" & "B" inputs to the NSR Gateway Computers are isolated from each other, and data communication protocols associated with processing this data within the Gateway Computers.</i></p> <p><i>12-19-2012 follow up question:</i> <i>As stated in the 12-17-2012 response below, the 1E/non-1E data communications electrical isolation is not part of the ALS topical reort review. Please provide a detailed explanation of how all 1E/non-1E communications data electrical isolation between the ALS processor and NSR systems will be accomplished.</i></p>	Open			12-19-2012 update: Response did not answer the question about providing a functional description of the DCPD PPS NSR Gateway computers. The staff needs to understand how the Gateway computer and the Gateway Switch communication protocols will not corrupt the the data signals coming from the ALS Protections sets 1-4 and not impact the execution of the ALS safety function. A detailed response to this question is needed	

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>PG&E Response: The DCPG Gateway computer and Gateway switch are part of an existing system that was installed by a previous project, and therefore were not included in the scope of the changes requested for approval in the LAR.</p> <p>Communications from the Gateway Switch to the Tricon are functionally isolated by the Triconex Communication Module (TCM) and NetOptics Model PA-CU Network Port Aggregator Tap discussed in Tricon V10 SER Section 3.7.2.1. A fiberoptic data link provides electrical isolation.</p> <p>The NetOptics PA-CU Network Port Aggregator Tap was approved for this use in the Oconee RPS SER. The PA-CU prevents inbound communications from external devices or systems connected to Port 1 of the Port Aggregator from being sent to interactive Ports A and B. The Oconee SER described the methods they used to verify that Aggregator Port 1 provides one way outbound communications only. As a transmit only device, it does not listen to and is not affected by the communications protocol (or lack thereof) of the external device or system to which it is connected.</p> <p>The ability of the Port Aggregator Tap to prevent inbound communications to the Tricon from its Port 1 will be verified at the Tricon V10 FAT and the SAT as previously stated in PG&E Letter DCL-12-083 dated September 11, 2012.</p> <p>Updated PG&E Response 12/12/2013: The response to OI #73, discusses Transmit Bus TxB2 data communication path from the ALS-102 Core Logic Board to the ALS MWS. Transmit Bus TxB1 transmits data from the ALS-102 CLB to the Gateway Computer. Both TxB1 and TxB2 are EIA-422 communication links in which Receive capability is physically disabled by hardware as described in the ALS-102 Design Specification, 6002-102002. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 is physically and electrically incapable of receiving information from outside the ALS-102 via the Transmit Busses TxB1 and TxB2. Therefore, messages are not disregarded or rejected by the ALS-102. This is better</p>					<p>in the LAR or supporting documents. See 12-19-2012 follow up question re: electrical isolation for the DCPG PPS ALS.</p> <p>11-28-12 update: See 11-28-2012 follow up question.</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>than a "broken wire." The wire just isn't there, and there is no place to connect a wire if someone wanted to do so.</p> <p>Updated WEC Response 12/17/2012: The 1E/non-1E data communication is described in the ALS Topical Report, Sections 2.2.1.3 and 5.3.2; and in 6116-00054, "Diablo Canyon PPS ISG04 Matrix", Position 2. The electrical isolation qualification of the 1E/non-1E data communication is not part of the ALS Platform review project, and will be qualified with an isolation fault test that will be conducted 1st quarter 2013 per IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" and Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems." A supplemental test report will be issued 2nd quarter 2013.</p>					
69	WEK	<p>Please provide a detailed explanation of the application programs contained within the Tricon and ALS MWS computers; including how they will be used to supports or enhances the performance of the PPS safety function enhance the performance of the PPS safety systems, provide required maintenance, surveillance, etc. Or, please indicate where this information is explained within the LAR and supporting documents.</p> <p>1/24/2013 Updated PG&E Response: The non-safety communications between the PPS controllers and their respective, dedicated MWS units improve PPS maintainability and thus reliability, and enabling on-line surveillance testing, calibration, and maintenance. Risk of challenging plant safety systems is reduced through the ability to test in bypass rather than requiring test in trip. The online Tricon and ALS non-safety communications capability provide real-time, online data and status information on the Plant Process Computer and in the Control Room that are required to perform maintenance,</p>		Open			<p>12-19-2012 update: The DCPP PPS ALS MWS will not be approved via the ALS topical report. Therefore, the information requested is needed to address the regulatory criteria of ISG-04, Position 1, Point 3. W/ALS document 6116-00054, Rev. 0, Diablo Canyon PPS ISG-04 Matrix, does not address this subject in its</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>calibration and testing. Without the online data links from the Tricon and ALS to the MWS and the Plant Process Computer/Plant Data Network, only the control board indicators and recorders would be available to provide a "window" on 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 determine the specific cause of an alarm.</p> <p>Lack of access to real-time, continuous, on-line PPS status data and diagnostic information introduces 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 online 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.</p> <p>The network switches between the Port Aggregator taps and the MWS ensure that Tricon multicast operation will continue if the Tricon MWS were to cease communications. The network switches are redundant to ensure continued Tricon multicast operation on failure of a single Tricon network link.</p> <p>The application programs contained in the ALS and Tricon MWS units provide the following functionality:</p> <p>A. Westinghouse/CSI ALS Maintenance Workstation</p> <p>The on-line ALS MWS is required to maintain the ALS, including surveillance testing per the Technical Specifications calibration, and other required maintenance, and is similar in effect to the existing, approved Test in Bypass capability. The diversity design of the ALS enables either (but not</p>					<p>response to Point 3. Please address this question for ALS.</p> <p>Tricon response is acceptable. Please add this to the LAR/Tricon V10 ISG-04 compliance matrix document.</p> <p>11-28-12 update: Additional clarification was provided, so the question was rephrased.</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>both) Chassis "A" or Chassis "B" in a protection set to be bypassed for maintenance or testing while the other chassis remains fully operational (Although, in the bypassed condition, certain post-accident monitoring functions may not be available; this may be controlled administratively).</p> <p>Without the flexibility provided by the ALS diversity design, Technical Specifications would require tripping all the channels associated with the chassis when removing a given protection set ALS chassis from service. In turn, this would make up one channel in the coincidence logic for all channels in the affected ALS protection set. Such action increases the risk of inadvertently challenging plant safety systems were another channel to trip with the ALS protection set out of service.</p> <ol style="list-style-type: none"> 1. Microsoft Windows™ XP Service Pack 3 operating system 2. ALS Service Unit (ASU) Application <p>The ALS MWS will utilize Microsoft Windows™ based Westinghouse/CSI ALS Service Unit (ASU) software that is described in the ALS Topical Report Section 2.6.3.</p> <p>The ALS Service Unit (ASU) is the primary tool used when accessing a particular ALS system in operation. The ASU provides plant personnel access to advanced features of the ALS system such as system diagnostics, post-trip analysis, monitoring real-time operation, and assistance in performing user-initiated test, calibration and maintenance operations.</p> <p>The DCPP PPS Replacement MWS will be mounted permanently in the PPS rack containing the PPS in a manner similar to that shown in ALS Topical Report Figure 2-25; however, ASU functions that use interactive Test ALS Bus (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 at a time.</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>The TAB from ALS-102 Chassis "A" and Chassis "B" is provided with individual EIA-485 ports on the ALS Maintenance Workstation computer. The ASU ensures that the correct TAB is connected to the respective EIA-485 port when the TAB is enabled.</p> <p>The main features of the ASU are:</p> <ul style="list-style-type: none"> • State Information – Provides monitoring of real-time operation, including all I/O signals as well as detailed status information from debugging registers. The advanced monitoring capabilities enable fast system diagnostics and troubleshooting. • System and Board Information – Provides detailed information about the configuration of an ALS system, including board FPGA programming, board build information, and board configuration. • Blackbox – The ASU includes a so-called "blackbox" functionality where all events of an ALS system are transmitted by the ALS-102 CLB Transmit Bus TxB2 to the ASU for storage and subsequent retrieval. This allows plant personnel to inspect the ALS system's reaction to a past event. The blackbox function enhances ALS reliability and therefore safety by helping to reduce the time required to pinpoint the cause of a series of events. The ASU must be connected to the ALS via the Transmit Bus TxB2 during an event in order to capture and store the event via the blackbox function. Given the difficulty in predicting when an event will occur, the ASU should be connected to the ALS chassis via Transmit Bus TxB2 and receiving data during online operation in order to benefit from this capability. • Test – Application specific periodic surveillance tests can be implemented to be performed through the ASU. Based on the needs of the application features may be implemented in the CLB that allows surveillance testing to be performed and/or monitored through the ASU. • Calibration – The ASU is used to readout and change application Setpoints and channel calibration coefficients. The CLB holds the 					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>application Setpoints and according to the application, it will allow the ASU to modify these Setpoints. The ASU is also used during input/output channel calibration where it is used for selecting the board and board channel to be calibrated and to changes calibration coefficients based on the readings received on an external calibrator.</p> <p>Operation of the ASU is passive and non-intrusive, i.e., it can only modify the safety system tunable parameters stored in NVM for which it is designed (i.e., input/output calibration coefficients, setpoints and tuning constants). It is not possible to modify the safety algorithm or logic using the ASU. All communications initiated by the ASU take place on the TAB, and only when the TAB is physically connected between a protection set ALS and its dedicated MWS. No RAB interruption is possible, effectively isolating the ASU from ALS safety functions.</p> <p>3. ALS Parameter Display</p> <p>The ASU also provides a 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 online by the one-way TxB2 transmit bus described in ALS Topical Report Section 2.2.1.3. The parameter display function does not require the TAB to be connected.</p> <p>The ASU parameter display function is a Visual C++ based application developed for the Microsoft Windows API using Microsoft Foundation Class (MFC) libraries to provide graphical user interfaces for displaying ALS system status on the MWS and for providing user controlled access to the ALS controllers for performing maintenance operations such as calibration.</p> <p>Upon start-up, the application establishes a dedicated serial port connection to the MWS RS-422 serial communication card port that is connected to the ALS-102 unidirectional one-way TxB2 output in each ALS chassis "A" and "B." These dedicated MWS serial ports receive ALS system status at a rate of 10 Hz (i.e., once every 100 ms).</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>Upon establishing the dedicated serial port connection on the MWS, the ASU parameter display function spawns a software thread to receive, validate, and store the data received from the respective ALS-102 TxB2. Validation of the received data consists of checking the packet header contents, checking packet length, performing a CRC check on the packet contents, and then comparing the calculated CRC with the CRC inside the TxB2 packet. If the data received by the parameter display application is invalid (i.e. invalid CRC), the application indicates the issue on its graphical user interface (GUI) and an entry is made in the application status log. If the data received by the parameter display application is valid, the application records the ALS system status in a data class which contains methods that are called by different GUI to extract and display the specific ALS system status.</p> <p>Malfunctions of the ASU parameter display function cannot adversely affect ALS safety system operation because EIA-422 communications between the ALS and the ALS MWS via TxB2 are strictly one-way from the ALS-102 to the ALS MWS and the EIA-485 TAB is physically disconnected except for brief periods when the TAB for either ALS "A" OR "B" is connected to the MWS for maintenance under administrative control by trained technicians.</p> <p>4. One way TxB1/TxB2 Communications</p> <p>Transmit Bus TxB1 transmits data from each ALS chassis "A" and "B" ALS-102 CLB to the Gateway Computer. Transmit Bus TxB2 transmits data from each ALS chassis "A" and "B" ALS-102 CLB to dedicated EIA-422 ports on the ALS MWS. Both TxB1 and TxB2 are EIA-422 communication links in which Receive capability is physically disabled by hardware as described in the ALS-102 Design Specification, 6002-102002. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 does not disregard or reject external messages; rather, the ALS-102 is physically and electrically incapable of receiving external messages via the Transmit Busses TxB1 and TxB2. In effect, this is the same as the</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>data isolation achieved by a "broken wire." Interdivisional communications between the MWS and the ALS are also described in ALS Topical Report section 5.3.</p> <p>5. TAB Disconnect</p> <p>TAB communications are enabled by physically connecting the TAB to the respective MWS EIA-485 port under administrative control by trained technicians. TAB communications are disabled when not needed by physically disconnecting the TAB from the MWS. The ASU is connected to and communicates with the ALS via the TAB only when required to calibrate the ALS, normalize RCS flow coefficients, perform surveillances required by Technical Specifications, as well as to troubleshoot and otherwise maintain the ALS. The diverse ALS subsystem whose TAB has not been enabled will continue to perform its safety function without impact. An ALS trouble alarm is initiated on the Main Annunciator when the TAB is enabled. The non-safety communications provided by the Transmit busses will allow the operator to ascertain quickly the cause of the alarm, if the operator is not already aware of the maintenance activity being performed under procedural control.</p> <p>TAB communications are described in ALS Topical Report Section 5.2.</p> <p>6. Electrical Isolation</p> <p>The Transmit Bus TxB1 and TxB2 1E/non-1E data communication is described in the ALS Topical Report, Sections 2.2.1.3 and 5.3.2; and in 6116-00054, "Diablo Canyon PPS ISG04 Matrix", Position 2. The electrical isolation of the Transmit Busses is performed by magnetic couplers located on the ALS-102 CLB. The TxB isolators are described in 6002-10202, "ALS-102 Hardware Design Specification," Section 3.9.1.</p> <p>Fault isolation occurs by way of board mounted transient voltage suppressors, board mounted fuses, and external fuses.</p> <p>Qualification of the 1E/non-1E data communication is not part of the ALS</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>Platform review project, and will be qualified with an isolation fault test that will be conducted 1st quarter 2013 per IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" and Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems." A supplemental test report will be issued 2nd quarter 2013.</p> <p>B. Triconex Maintenance Workstation</p> <p>The Tricon MWS will implement four Microsoft Windows™ -based application programs: (1) Invensys WonderWare™ InTouch™ PPS application; (2) TriLogger; (3) Tricon Diagnostic Monitor; and (4) TriStation 1131 (TS1131) Developers Workbench Version 4.9.0.</p> <p>1. Microsoft Windows™ XP Service Pack 3 operating system</p> <p>2. WonderWare™ InTouch™PPS Application</p> <p>The WonderWare InTouch application provides online display of selected PPS internal parameters and trouble alarm details. The WonderWare InTouch application also is used for maintenance of individual PPS instrument channels in conjunction with the hardwired OOS switches that have been discussed in the response to other Open Items. The MWS WonderWare InTouch application will be the tool normally used to determine the specific cause of an alarm. The Main Annunciator System only displays system level alarms. The MWS InTouch application contains an alarm monitor, which is a troubleshooting aid that provides a detailed, specific display of the alarms generated by the Tricon PPS application.</p> <p>3. Non-Safety Tricon Communications</p> <p>Communications from the Tricon to external non-safety systems are functionally isolated by the Triconex Communication Module (TCM) and NetOptics Model PA-CU Network Port Aggregator Tap discussed in Tricon V10 SER Section 3.7.2.1. A fiberoptic data link provides electrical isolation. The PA-CU prevents inbound communications from external devices or systems connected to Port Aggregator Port 1 from being sent to interactive</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>Ports A and B. Port 1 is a transmit-only port that does not listen to and is not affected by the communications activity generated by the external device or system to which it is connected.</p> <p>Port Aggregator port 1 will provide one-way data to the Gateway Computer via the Gateway Switch. The Gateway Computer transmits the data to the Plant Process Computer for use in the Control Room by the operators. The Gateway Computer and Gateway Switch were installed by another project. The Plant Process Computer is an existing system.</p> <p>4. Triconex TriLogger</p> <p>The TriLogger software provides the ability to record, display, play back and analyze data from the Tricon system. Data can be viewed in real-time on the MWS. The TriLogger provides data trending and analysis capabilities and can be configured to trigger on specific events to log detailed data to aid technicians in isolating, diagnosing, and troubleshooting problems. However, the TriLogger must be connected and running at all times to perform these functions.</p> <p>5. Tricon Diagnostic Monitor Utility</p> <p>The Tricon Diagnostic Monitor utility displays Tricon system and module status by mimicking the actual Tricon chassis and slots, so that the user can find the exact location (chassis number and slot number) of a module that may be experiencing a fault or other problem. The Tricon Diagnostic Monitor Utility improves reliability by aiding rapid troubleshooting and fault location at the Tricon system level.</p> <p>6. Startup Delayer</p> <p>Startup Delayer delays WonderWare startup until DDE Server has initialized. Otherwise, WindowViewer may startup first and never connect to DDE Server.</p> <p>7. TriStation 1131 (TS1131) Developers Workbench</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>TriStation 1131 is a PC-based application development workstation that provides a comprehensive set of development, test, monitor, validation and diagnostic tools for Triconex Programmable Logic Controllers (PLC). The TS1131 program is utilized to maintain the PPS application program and may also be used for monitoring and troubleshooting purposes. The TS1131 program is described in the Tricon V10 SER Section 3.1.3.2.</p> <p>The TS1131 tool will be installed on the MWS. However, the TS1131 tool will not normally be running while the Tricon is performing its safety function [Tricon V10 SER Section 3.10.2.9]. If the TS1131 workstation is connected during online safety operation for maintenance or troubleshooting purposes, its use will be controlled via administrative controls and qualified maintenance personnel.</p> <p>Write access to the operating Tricon is governed by the controller keyswitch. With the keyswitch in the RUN position, use of the TS1131 program is limited to read only access to the Tricon. Parameters may be examined, and application program logic operation may be observed in real time, but changes are not possible. The TS1131 program can only write to the Tricon when the controller keyswitch is in the PROGRAM position. With the keyswitch not in RUN, the PPS application will initiate an alarm on the Main Annunciator system and the affected PPS set will be declared inoperable with respect to its safety function.</p> <p>Regardless of whether the keyswitch has been deliberately manipulated or whether the condition is the result of Tricon hardware or software failure, the internal Tricon diagnostics will detect a "keyswitch not in RUN" condition and the PPS application program will initiate a PPS Trouble alarm on the Main Annunciator System. When the "keyswitch not in RUN" condition exists, the affected Tricon is considered to be INOPERABLE with respect to its safety function. The operator would enter the appropriate Technical Specification LCO upon determination that the PPS trouble alarm was caused by the "keyswitch not in RUN" condition.</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>The condition could be active in multiple Tricon protection sets because it could occur as a result of common cause Tricon failure. Even with the "keyswitch not in RUN" condition existing in multiple protection sets, negative impact is limited because on-line maintenance will normally be performed in one protection set at a time, and each Tricon protection set has its own dedicated, independent MWS. Therefore, only one Tricon protection set at a time would be configured physically to make software changes. If the TS1131 is not connected and running changes cannot occur even if the "keyswitch not in RUN" condition exists. That is, the mere existence of the "keyswitch not in RUN condition" does not initiate changes. Intentional action by a trained, knowledgeable individual is also required. Given the PPS trouble alarms that would be active in all affected protection sets, it is highly unlikely that unintended changes could occur.</p> <p>If a PPS Trouble alarm were to occur on the Main Annunciator System due to the "keyswitch not in RUN" condition, regardless of the cause, the operator would notify DCP Maintenance. In the absence of the detailed alarm monitoring provided by an on-line MWS (via the TCM NET2 interface), the maintenance technicians would be required to obtain work orders, gain access to the affected protection set, connect and boot the MWS, and only then could begin to determine the cause of the alarm. The alarm information would not be available if the alarm were due to a transient condition that cleared between the time the condition initiated and when the MWS was operational. Diagnosis of the condition could be delayed for several hours. With the on-line MWS and the alarm monitor function, the condition – whether caused by intentional manipulation of the Tricon controller keyswitch or by a hardware or software failure involving the keyswitch– would be identified immediately.</p> <p>As with the ALS, the on-line Tricon MWS is essential to maintain the Tricon safety function, including surveillance testing per the Technical Specifications and other required maintenance and is equivalent to the existing, approved Eagle 21 Test in Bypass capability. The MWS is</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		required to bypass channels for testing. Removing a Tricon from service during such routine maintenance would require tripping all the channels in that protection set, which would make up one channel in the coincidence logic for all channels in the protection set. This condition increases the risk of challenging plant safety systems should another channel trip inadvertently with the protection set out of service.					
70	WEK	<p>KVM Switch Question 1:</p> <p>If the Enumerated USB switching function is used, will you be able to use the Keyboard hotkeys and mouse buttons to perform switching? The brochure seems to indicate on page 3 that the Enumeration switching process will not enable control switching using the USB keyboard or mouse. However, it further says that Emulation USB switching was developed to support these enhanced monitor switching functions/devices (keyboard hotkeys or mouse buttons).... Albeit, other USB devices (e.g., printer) do not need to use the Emulated USB switching function. Could you please clarify this point.</p>		Open			11-28-12 update: Response Okay. Leave open until the KVM Switch information is provided within the LAR revision.
		<p>PG&E Response:</p> <p>The USB1 and USB2 ports, which use enumerated switching, pass data straight through the KVM switch without interpretation. Therefore, you cannot connect a keyboard to USB1 or USB2 and use the hotkeys to perform switching, and USB1 and USB2 traffic cannot cause an inadvertent switch. The block diagram shows the output of the emulated portion of the switch and the enumerated portion going to a USB hub before being sent to the computer. The keyboard and mouse will use the emulated switching function, not the enumerated switching function; only the keyboard and mouse can control the switch.</p>					
71	WEK	<p>KVM Switch Question 2:</p> <p>Will the KVM switch will be on-line 24-7 monitoring data from either</p>		Open Hold			12-19-2012 update: The staff

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>the Tricon or the ALS platform? If so, what can we say about the failure modes of the KVA switch? Can it fail in such a manner so as to inject faults into the MWS computers, and hence into the Tricon or ALS safety system processors? If not, why? If so, what can be done to circumvent this problem, and show conformance with ISG-04, Points 10 & 11? We will need to cover this matter in the SER.</p> <p><i>10-17-12 Update: Response below did not answer the question regarding failure modes of the KVM switch...agree that it is Okay to lose the Tricon but I do not see how the ALS is protected due to its "inherent 1-way communications" design. Please explain this further.</i></p> <p>12-19-2012 Update question: In order for the staff to verify the response below regarding the ALS-102 Core Logic Board's one-way communications design attributes the staff will need to review the ALS-102 Design Specification document 6002-10202, and any other documents that explain this key design feature for the ALS Platform portion of the PPS (e.g., 6116-00100, PPS ALS to ASU Communications Protocol??). ALS document 6002-10102 has not been submitted on the docket for staff review of the ALS Platform Topical Report. Therefore, please submit this document (and any others that explain this communications protocol) on the docket as part of the PPS LAR review.</p>					<p>will review 6002-10202 and determine if this document provides the information requested. Nonetheless, PG&E needs to address the inherent 1-Way communications design and communications protocol of the 102 board in detail within this OI—as it relates to the DCP PPS.</p>
		<p>PG&E Response:</p> <p>The KVM switch will be on-line 24-7 for monitoring data from either the Tricon or ALS platform via the respective MWS computers. There is additional isolation because the ALS communicates strictly one way to its MWS except when TAB communications are enabled by connecting the TAB cable. Connection of the TAB is performed as directed by trained technician using an approved procedure. Therefore, if the KVM switch failed in some way to connect the two MWS together, the ALS would not be affected. The Tricon might be affected, but the D3 analysis allows the Tricon to fail due to CCF.</p> <p>The following paragraphs have been added to the IRS Section 2.3.7:</p>					<p>Also, need to update the LAR to cover the portions not being addressed in the ALS TR SER, i.e., 1E/non-1E data communications electrical isolation for ALS. See follow up question for OI 68.</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>b, The KVM switch shall permit only connections between a single computer and the selected video display and HMI interface devices. Connection between the computers shall not be permitted.</p> <p>g. The AV4PRO-VGA KVM switch shall utilize the default switching mode, in which the video display, keyboard and mouse and the enumerated USB ports are all switched simultaneously.</p> <p>Paragraph g was necessary to prevent the enumerated ports from being switched separately from the KVM.</p> <p>Added PG&E Response 12/16/2012: During normal, non-maintenance operation, the ALS communicates one-way to its dedicated MWS computer via Transmit Bus TxB2 as discussed in the response to OI #73. Inter-divisional safety to non-safety communications are addressed in ALS Topical Report Section 5.2.3. The TxB2 data communication paths from the ALS-102 Core Logic Board to the ALS MWS computer is a EIA-422 communication link in which Receive capability is physically disabled by hardware as described in 6002-102002, the ALS-102 Design Specification. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 is physically and electrically incapable of receiving information from outside the ALS-102. Therefore, the ALS cannot be affected by a malfunction in the dedicated, MWS computer associated with an ALS protection set regardless of whether the malfunction is caused by KVM switch malfunction or by malfunction of the MWS computer itself.</p> <p>WEC Response 12/17/2012: The 1E/non-1E data communication is described in the ALS Topical Report, Sections 2.2.1.3 and 5.3.2; and in 6116-00054, "Diablo Canyon PPS ISG04 Matrix", Position 2. The electrical isolation qualification of the 1E/non-1E</p>					<p>11-28-12 update: ALS ISG-04 compliance was submitted, and Westinghouse thinks that this will answer this question. PG&E needs to respond to 10-17-12 update in the description section. Leave open until the KVM Switch information is provided within the LAR revision.</p> <p>10-17-12 Update: Note: "IRS" is the Interface Requirements Specification (Attachment 8 of the LAR).</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		data communication is not part of the ALS Platform review project, and will be qualified with an isolation fault test that will be conducted 1st quarter 2013 per IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits" and Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems." A supplemental test report will be issued 2nd quarter 2013.					
72	WEK	<p>KVM Switch Question 3:</p> <p>Also, you will likely need to address how you will disable the features you are not using such as the audio interface, unused USB ports, remote control/channel switching by external control from and SDOE perspective—and probably a cyber security perspective later on (after SER).</p> <p><i>10-17-12 Update: The methods used to block Ports in the KVM Switch must be addressed in the LAR revision. Block all unused Ports and keep any that may need to be reopened under design or configuration control.</i></p> <p><i>Again, we need a detailed explanation of how this 1-way design feature will prevent the KVM switch failures from affecting the ALS system.</i></p>		Open	RAI 43		<p>12-19-2012 update: response acceptable, however, this information needs to be provided in the LAR. Also, address how this will be maintained by the DCP Configuration Management Process.</p> <p>11-28-12 update: PG&E needs to respond to 10-17-12 update in the description section. Leave open until the KVM Switch information is provided within the LAR revision.</p>
		<p>PG&E Response:</p> <p>Specific answers to these questions depend on the detailed design. Ports can be physically blocked, which might be appropriate for unused computer ports and the audio ports. It might not be appropriate for the unused USB port (which may be needed for a future printer) and the options port (which may be needed for firmware updates). Remote control switching or firmware update requires a custom serial cable. The firmware update requires specialized software on the computer being used to perform the update. Firmware update will be done by procedure. The MWS will be inside a locked cabinet inside a vital area inside the protected area. Inadvertent actions, while not impossible, will not be easy. If the switch is</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>somehow manipulated, the ALS will not be affected even if the KVM switch fails because the ALS communicates only one-way with the MWS except for short periods when the TAB is enabled.</p> <p>Revised PG&E Response 12/16/2012: PG&E will physically block the audio port, USB Port 2 and unused computer ports. Physical blocks will be verified at SAT and controlled thereafter by the SCMP. PG&E considers that opening any of the unused ports for use after the SAT is a modification of the physical plant configuration that will require an engineering design change.</p>					
73	WEK	<p>KVM Switch Question 4:</p> <p>If the KVM switch does fail in some manner allowing data flows between the two platforms, then the ALS system would not be affected because the ALS platform will only transmit data in one direction to its MWS (with the TAB cable disconnected of course). This is good, however, the LAR (or attachments) need to explain how the engineering design principals of the ALS platform physically prevent bad/erroneous data from corrupting the ALS platform. In other words, explain how these messages emanating from the MWS (regardless of origin) will be disregarded/rejected by the ALS platform thus allowing only one direction of data flow.</p> <p><i>10-17-12 Update:</i> <i>The ALS-102 Design Specification document 6002-10202 has not yet been submitted to the NRC. When will it be submitted?? Will this EIA-422 (or is it RS-422 per Fig. 4-13 in the LAR) communication link (twisted pair copper wire) also serve as the 1E/non 1E isolation devices as required by IEEE 603, Clause 5.6.3 and IEEE 7-4.3.2, Clause 5.6?? Please clarify.</i></p> <p><i>11-28-2012 Update:</i> <i>Still need more information re:1E/non-1E isolation of the ALS-102</i></p>		Open Hold	RAI 44		<p>12-19-2012 update: As discussed in the 10-17-2012 update for this OI, and the 12-19-2012 Follow up Question for OI 71, the staff needs ALS Design Specification document 6002-10202 submitted for its review in order to resolve this OI. This OI will be placed on Hold until the documents are received on the docket.</p> <p>11-28-2012 update: PG&E needs to respond to <u>11-28-</u></p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		board.					12 update in the description section. PG&E needs to respond to 10-17-12 update in the description section.
		<p>PG&E Response:</p> <p>Revised PG&E Response 12/16/2012: The design of the TxB1 and TxB2 data communication paths from the ALS-102 Core Logic Board and the Gateway Computer and MWS, respectively, are EIA-422 communication links in which Receive capability is physically disabled by hardware as described in 6002-102002, the ALS-102 Design Specification. The receiver is configured such that the transmit data is looped back for channel integrity testing. The ALS-102 is physically and electrically incapable of receiving information from outside the ALS-102. Therefore, messages are not disregarded or rejected by the ALS-102. This is better than a "broken wire." The wire just isn't there, and there is no place to connect a wire if someone wanted to do so.</p> <p>Updated PG&E Response 12/16/2012: Per the 10/17/2012 update, NRC is correct regarding the typographical error in Section 2.4.13.5 on page 90 of the LAR. The correct ALS-102 Design Specification document number per LAR Reference 94 is 6002-10202.</p> <p>Per the 11/28/2012 update, RS-422 is the common short form title of American National Standards Institute (ANSI) standard ANSI/TIA/EIA-422-B Electrical Characteristics of Balanced Voltage Differential Interface Circuits. This technical standard specifies the electrical characteristics of the balanced voltage digital interface circuit. For the purposes of the LAR, the two designations are equivalent and may be used interchangeably.</p>				10-17-12 Update: there is a typo in section 2.4.13.5 on page 90 of the LAR. The first paragraph references ALS doc. 6002-61202 (typo) as the document that explains how the EIA-422 communication channels on the ALS-102 are electrically isolated and inherently 1-way communications capability only. The document 6002-10202, in reference 94 is the correct document.	
74	WEK	KVM Switch Question 5: Please explain in detail how "Connection between the computers		Open			11-28-12 update: Leave open until the KVM Switch

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		shall not be permitted." Will this be handled via a configuration control process, administrative controls, or a physical means of preventing connection between computers?					information is provided within the LAR revision.
		<p>PG&E Response:</p> <p>This section was intended to be a functional requirement for the KVM switch. Administrative and configuration controls will prevent inadvertent loading of an EPROM image that could corrupt operation of the KVM switch. If the KVM switch fails and connects the ALS and Tricon MWS together, the above-described physical and electrical restrictions of the KVM switch will prevent the ALS from being corrupted by its MWS computer.</p>					<p>10-17-12 Update: Response is Okay, but the LAR revision will need to expand further on this matter to explain how these controls will provide this protection.</p>
75	RJS/ NSIR	<p>ALS Security Plan Document 6002-00006 references the CS Innovations Cyber security plan document (Reference 7) which is not docketed. Without having access to this referenced document, the staff is unable to confirm implementation of the system security requirements. We need to discuss if this document can be made available on the share point or if it can be made available during the audit.</p> <p>In addition CS-00013-GEN, Development Environment Evaluation Report – CS Innovations Isolated Development Infrastructure might be another document of interest to the staff. It seems that this document would provide evidence that the actual development environment was in fact secure. This document was not docketed.</p>		Open			Note: RJS – We need to resolve if document needs to be docketed now that we have reviewed it during audit.
		PG&E Response: Westinghouse can make available during the audit both CSI document 9000-00360, "CS Innovations Cyber Security Plan" and					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		WNA-CS-00013-GEN, "Development Environment Evaluation Report – CS Innovations Isolated Development Infrastructure."					
76	WEK	<p>The documents listed below are necessary for the staff to complete its assessment of the Tricon V10 platform changes/software revisions that have occurred since the platform was approved generically, and will be applied to the DCPD PPS.</p> <p>1. Reference Design Change Analysis (RDCA), 993754-1-916</p> <p>2. Nuclear Qualified Equipment List (NQEL), 9100150-001, Rev 16</p> <p>Rev 11: Tricon V10.5.2</p> <p>Rev 13: TriStation V4.9.0</p> <p>Rev 14: Tricon V10.5.3</p> <p>Tricon NGIO Software SRS, 6200155-001</p> <p>Tricon V10.5 Verification and Validation Report (19 Sept, 2012)</p> <p>3. V10.5.2 Documents</p> <p>a) PDR (IRTX) 21105</p> <p>b) Technical Advisory Bulletin (TAB) 183</p> <p>c) Engineering Project Plan (EPP) Tricon V10.5.2, 9100346-001</p> <p>d) V10.5.2 V&V Test Report</p> <p>e) Software Release Definition (SRD), V10.5.2, 6200003-226</p> <p>4. V10.5.3 Documents</p> <p>a) PDR (IRTX) 22481</p> <p>b) Product Alert Notice (PAN) 25</p> <p>c) Engineering Project Plan (EPP) Tricon V10.5.3, 9100428-001</p>		Closed	RAI 45		<p>12-19-2012 Update: the staff has reviewed all of these documents and some of them will require submittal on the docket for approval of these changes within the SER—see 12-19-2012 follow up item for this OI.</p> <p>Invensys Audit Item</p> <p>11-28-112 update: Response Acceptable. We will also need this information submitted on the docket.</p> <p>Invensys Audit Item</p>

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		<p>d) Tricon PAN 25 Master Test Report e) Software Release Definition (SRD), V10.5.3, 6200003-230 f) NGDO SRS 6200170-001</p> <p>(ii) Tristation V4.9.0 documents</p> <p>a) Product Alert Notice (PAN) 22 b) Product Alert Notice (PAN) 24 c) Technical Advisory Bulletin (TAB) 147 d) Engineering Project Plan (EPP) Tristation V4.9, 9100359-001 e) Tristation V4.9.0 Master Test Report f) Software Release Def. (SRD), Tristation V4.9.0, 6200097-038 g) Spec. Software Design – Tristation 1131 SDS, 6002168-002 (Section Applicable to V4.9.0 Change) h) TriStation 1131 V4.9 V&V Plan, 9600442-002 i) TriStation 1131 V&V Summary Report (26 Oct. 2012)</p> <p>12-19-2012 Follow up Item: The staff has reviewed all of these documents, which have been placed on the Invensys Sharepoint website and concluded its assessment of the Tricon Platform changes from V10.5.1 to V10.5.3. The results of this assessment will be published in the Invensys Audit Report. In order to provide a safety finding to approve these changes in the DCPD PPS SER It is necessary for the following documents to be formally submitted to the staff to facilitate completion of its safety assessment of the Tricon V10 platform changes/software revisions that have occurred since the platform was approved generically, and will be applied to the DCPD PPS.</p> <p><u>Please submit the following Documents on the Docket:</u></p> <p>1. Product Discrepancy Report (PDR) IRTX#21105</p>					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		2. Technical Advisory Bulletin (TAB) 183 3. Engineering Project Plan (EPP) V10.5.2, 9100346-001, Rev. 1.4 4. Tricon V10.5.2 V&V Test Report, Rev. 1.1, January 14, 2011 5. Software Release Definition (SRD) V10.5.2, 6200003-226, Rev.1.0 6. PDR IRTX#22481 7. Product Alert Notice (PAN) 25 8. Document "ARR 932 NSC Evaluation .pdf" 9. Tricon PAN 25 Fix Engineering Project Plan (EPP) 9100428-001, Rev.1.2 10. Tricon PAN 25 Master Test Report, Rev.1.0 11. Software Release Definition (SRD) V10.5.3, 6200003-230, Rev.1.0 12. Product Alert Notice (PAN) 22 13. Product Alert Notice (PAN) 24 14. Technical Advisory Notice (TAB) 147 15. Engineering Project Plan (EPP) TriStation V4.9 & Safety Suite Apps, 9100359-001, Rev.1.3 16. TriStation V4.9.0 Test Report, Rev. 0.4 17. Software Release Definition (SRD) 6200097-038, Rev.1.2					
		PG&E Response: Invensys will place the requested documents on the Invensys SharePoint by December 3, 2012, for access by the NRC. The documents will be marked in accordance with 10 CFR 2.390 prior to placing them on the SharePoint.					
77	RJS	The staff requests that the Purchase Order Compliance Matrices (Multiple Documents) be placed on the SharePoint site to support verification of requirements traceability determinations.					Invensys Audit Item
		PG&E Response: Invensys will place the requested documents on the Invensys SharePoint by December 7, 2012, for access by the NRC. The documents will be marked in accordance with 10 CFR 2.390 prior to placing					RJS – I do not believe that the POCM's will need to be docketed.

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
		them on the SharePoint.					
78	RA	The staff requests that the Invensys Project Procedures Manual and Project Instructions (Multiple Documents) be placed on the SharePoint site to support review of Invensys process to design, develop and test the Tricon system.		Closed			12/19/12: Document was posted in Invensys' Sharepoint
		PG&E Response: Invensys will place the requested documents on the Invensys SharePoint by December 14, 2012, for access by the NRC. The documents will be marked in accordance with 10 CFR 2.390 prior to placing them on the SharePoint.					
79	RA	Invensys to confirm that the following terms are not used, and that they will be removed from their plans and replaced with the correct terms. <ul style="list-style-type: none"> • Test Review Board • Test Case Incident Report • Master Configuration Checklist • Configuration Database 		Open			12/19/12: item open until new document revisions are submitted
		PG&E Response: The following Invensys documents will be revised to reflect correct terminology and placed on the Invensys SharePoint by December 21, 2012: <ol style="list-style-type: none"> 1) 993754-1-905, Project Management Plan 2) 993754-1-906, Software Development Plan 3) 993754-1-909, Software Configuration Management Plan 4) 993754-1-813, Validation Test Plan The revised documents will be marked in accordance with 10 CFR 2.390 prior to placing them on the SharePoint.					
80	RA	PG&E Response: Invensys to revise its plans to reflect the current project organization.		Open			12/19/12: item open until new document revision is submitted
		PG&E Response: The Invensys Project Management Plan (PMP), 993754-1-905, will be revised to reflect the current project organization and placed on the Invensys SharePoint by December 21, 2012. The revised PMP will be marked in accordance with 10 CFR 2.390.					

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
81	RJS	<p>Channel level Bypass Functionality</p> <p>The criteria in ISG-04 position 10 only allows for software configuration activities when the entire safety division, (i.e. all channels and functions) is inoperable.</p> <p>The Diablo Canyon PPS design however, allows channel or specific function level configurability while the remaining safety division functions remain operable. This design does not meet the criteria of ISG-04 positions 10. The licensee will need to provide a justification for this as an alternative means of meeting the regulatory requirements of IEEE 603-1991 clauses 5.7, 6.5, and 6.7</p>		New			
		PG&E Response: IN PROGRESS					
82	RA	<p>V&V Plan</p> <p>Westinghouse/CSI document 6116-00001 Rev. 1 includes Table 2 in Appendix A. This table identifies several notes, which provide additional information. However, the descriptions for these notes are not included in the Appendix. Please provide this information.</p> <p>PG&E Response: Does this question refer to CSI document 6116-00003 Rev. 1 (Diablo Canyon PPS VV Plan) submitted December 5, 2012?</p>		New			

No	Src/RI	Issue Description	P&GE response:	Status	RAI No. (Date Sent)	RAI Response (Due Date)	Comments
83	RA	V&V and Hazard Analysis Westinghouse/CSI documents 6116-00001 Rev. 1 and 6116-00000 Rev. 3 state that software hazard analysis of the ALS system is the responsibility of PG&E. However, the PG&E SyVVP, which was submitted as Attachment 5 of the LAR, does not describe how PG&E will perform the software hazard analysis of the ALS system. The SyVVP, Section 5.1.2.3 states that PG&E will verify that new hazards were not introduced during installation. Please clarify who will perform the hazard analysis activities for each phase of the development process that are required by IEEE 1012, for the ALS system.		New			
		PG&E Response: IN PROGRESS					

Project Plan for Diablo Canyon Replacement of Digital RPS and ESFAS (PPS) - LAR Review (Rev. 7)

Step	Planned Date	Task	Actual Date
1	Oct. 26, 2011	PG&E LAR Submittal for NRC approval. Submittal includes all Phase 1 documents needed to be docketed prior to acceptance for review per ISG-06, "Digital Licensing."	Oct. 26, 2011
2	Jan. 12, 2012	Acceptance Review complete. LAR accepted for detailed technical review. Several issues identified that could present challenges for the staff to complete its review. Scheduled public meeting with PG&E to discuss the results of the acceptance review.	Jan. 12, 2012
3	Jan. 13, 2012	Acceptance letter sent to licensee.	Jan. 13, 2012
4	Jan. 18, 2012	Conduct Public Meeting to discuss staff's findings during the LAR acceptance review. Staff proceeds with LAR technical review.	Jan. 18, 2012
5	March 18, 2012	PG&E provides information requested in acceptance letter. Initiate bi-weekly telecoms with PG&E and its contractors to discuss potential RAI issues. Open Items spreadsheet will be maintained by NRC to document staff issues and planned licensee responses.	April 2, 2012
6	May 30, 2012	PG&E provides partial set of Phase 2 documentation per commitments made in LAR. <i>*PG&E provided a subset of the Phase 2 documents on June 6th and committed to send the rest by July 31, 2012.</i>	June 6, 2012*
7	July 2012	First RAI sent to PG&E on Phase 1 documentation (e.g., specifications, plans, and equipment qualification). Continue review of the application. Request 45 day response. (ML12208A364)	August 07, 2012
8	June 2012	SER for Tricon V10 Platform issued final. This platform becomes a Tier 1 review of the LAR. (ML12146A010)	May 15, 2012
8.1	March 2013	SER for Westinghouse ALS Platform issued final. This platform becomes a Tier 1 review of the LAR.	
9	September 2012	Receive answers to first RAI. (ML12256A308)	Sept. 11, 2012
10	November 2012	Audit trip to Invensys facility for thread audit; audit the life cycle planning documents and outputs, with particular emphases on verification and validation, configuration management, quality Assurance, software safety, the Invensys application software development procedures, and application software program design.	Nov. 13-16, 2012
11	December 2012	Audit report provided to PG&E and its contractor.	
11.1	TBD	LAR revision and all supporting documentation associated with the change in ALS and Tricon V10 workstation designs for the PPS are submitted.	
11.2	TBD	Follow-up audit trip to Invensys facility for thread audit; audit the life cycle planning documents and outputs, with particular emphases on verification and validation, configuration management, quality assurance, software safety, the Invensys application software development procedures, and application software program design.	

Project Plan for Diablo Canyon Replacement of Digital RPS and ESFAS (PPS) - LAR Review (Rev. 7)

11.3	February 2012	Audit trip to Westinghouse/CSI facility for thread audit; audit the life cycle planning documents and outputs, with particular emphases on verification and validation, configuration management, quality Assurance, software safety, the W/ALS application software development procedures, and PPS ALS application software program design.	
12	March 2013	PG&E provides remaining set of Phase 2 documentation per commitments made in LAR.	
12.1	March 2013	All Documentation for DCPD W/CSI ALS and IOM/Triconex V10 processors applicable to the DCPD PPS LAR are submitted.	
13	April 2013	Second RAI to PG&E on Phase 2 documentation (e.g., FEMA, safety analysis, RTM, EQ Tests results, setpoint calcs, SW Tool analysis reports, and any incomplete or un-satisfactory response to first RAI. Continue review - hardware and program design and V&V activities	
14	May 2013	Receive answers to second RAI. Continue review - V&V program, security requirements (RG 1.152, Rev.2)	
15	March 2013	Audit trip to W/ALS facilities for additional thread audit items; audit hardware and software installation plans, configuration management reports, detailed system and hardware design, completed test procedures, V&V activities, summary test results (including FAT) and incident reports, and application code listings.	
15.1	April 2013	Audit trip to Invensys facilities for additional thread audit items; audit hardware and software installation plans, configuration management reports, detailed system and hardware design, completed test procedures, V&V activities, summary test results (including FAT) and incident reports, and application code listings.	
15.2	TBD	Audit trip to DCPD test facilities for additional thread audit items; audit hardware and software installation plans, configuration management reports, detailed system and hardware design, completed test procedures, V&V activities, summary test results (including FAT) and incident reports, and application code listings.	
16	May 2013	Audit reports provided to PG&E and its contractors.	
17	November 2013	Presentation to ACRS Subcommittee/Full ACRS Committee on DCPD PPS LAR Safety Evaluation.	
18	November 2013	Complete draft technical SER for management review and approval.	
19	December 2013	Issue completed draft technical SER to DORL	
20	December 2013	Draft SER sent it to PG&E, Invensys, and W/CSI to perform technical review and ensure no proprietary information was included.	
21	January 2014	Receive comments from PG&E and its contractors on draft SER proprietary review.	
22	~March 2014	Approved License Amendment issued to PG&E	

**Project Plan for Diablo Canyon Replacement of Digital RPS and
ESFAS (PPS) - LAR Review (Rev. 7)**

23	~September 2014 (tentative)	Inspection trip to DCPD for PPS Site Acceptance Testing (SAT), training and other preparation for installing the new system. To be coordinated with regional visit. Date based on receipt of new PPS system at the site in preparation for September 2015 Unit 1 Refueling Outage (1R19).	
24	~September 2015	Inspection trip to DCPD for PPS installation tests, training and other system installation activities for the new system. To be coordinated with regional visit. Date based on September 2015 Unit 1 Refueling Outage (1R19).	

performed to verify that the software products to be used at DCPD for the PPS system conform to applicable standard, guidelines, plans, and procedures by assessing the implementation of the systems developmental life cycle process (life cycle audit

Both of the audit reports will be issued to PG&E shortly. Because the cyber security audit report contains security-related sensitive unclassified non safeguards information the cyber security audit report will be withheld from the public. The staff took an action to support phone calls with PG&E and Invensys as necessary to discuss results of the audits.

- The project plan for the review of the LAR (Enclosure 3) was discussed and the major upcoming milestones were confirmed. The project plan will be updated as appropriate and discussed at the next public meeting.
- The NRC staff stated that it should be issuing a second round of requests for additional information (RAIs) shortly. Once the RAIs are issued the items identified in Enclosure 2 as needing RAIs will be closed and removed from the open item tracking list. This is because the RAIs themselves will be used to track the closure of the issue.
- PG&E took an action to provide documents associated with open item number 76 in Enclosure 2 by the end of January.

Please direct any inquiries to me at 301-415-1132 or at Joseph.Sebrosky@nrc.gov.

/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

Enclosures:

1. List of Attendees
2. Staff Identified Issues That are Open
3. Project Plan

cc w/encls: Distribution via Listserv

DISTRIBUTION:

PUBLIC	RidsNsirDsp Resource	Sachen, RIV/DRS/EB2
LPLIV Reading	RidsOgcRp Resource	ELee, NSIR/DSP/CSIRB
RidsAcrsAcnw_MailCTR Resource	RidsRgn4MailCenter Resource	DParsons, NSIR/DSP/CSIRB
RidsNrrDeEicb Resource	JCassidy, EDO RIV	GSimonds, NSIR/DSP/CSIRB
RidsNrrDorl Resource	TWertz, NRR	THarris, NSIR/DSP/FCTSB
RidsNrrDorlLpl4 Resource	WKemper, NRR/DE/EICB	MShinn, NRC/CSO
RidsNrrDraApla Resource	RStattel, NRR/DE/EICB	CNickell, NRR/DLR/RAPB
RidsNrrDssStsb Resource	RAIvarado, NRR/DE/EICB	MSnodderly, NRR/DRA/APLA
RidsNrrLAJBurkhardt Resource	WMaier, RIV	KBucholtz, NRR/DSS/STSB
RidsNrrPMDiabloCanyon Resource	SMakor, RIV/DRS/EB2	

ADAMS Accession Nos. Meeting Notice ML12355A138; Meeting Summary ML13035A167

OFFICE	NRR/DORL/LPL4/PM	NRR/DORL/LPL4/LA	NRR/DE/EICB	NRR/DORL/LPL4/BC	NRR/DORL/LPL4/PM
NAME	JSebrosky	JBurkhardt	RStattel	MMarkley	JSebrosky
DATE	2/19/13	2/19/13	2/22/13	3/1/13	3/4/13

OFFICIAL RECORD COPY