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

March 4, 2013

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

SUBJECT: DIABLO CANYON POWER PLANT, UNIT NOS. 1 AND 2 – REPORT OF REGULATORY AUDIT ON NOVEMBER 13–16, 2012, AT THE INVENSYS OPERATIONS MANAGEMENT FACILITY IN LAKE FOREST, CALIFORNIA, TO SUPPORT REVIEW OF DIGITAL INSTRUMENTATION AND CONTROL LICENSE AMENDMENT REQUEST (TAC NOS. ME7522 AND ME7523)

Dear Mr. Halpin:

By letter dated October 26, 2011, as supplemented by letters dated December 20, 2011, and April 2, April 30, June 6, August 2, September 11, November 27 and December 5, 2012 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML113070457, ML113610541, ML12094A072, ML12131A513, ML12170A837, ML12222A094, ML12256A308, ML13004A468, and ML12342A149, respectively), Pacific Gas and Electric (PG&E, the licensee), requested the U.S. Nuclear Regulatory Commission (NRC) staff's approval of an amendment for the Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP). The proposed license amendment request would provide a digital replacement of the Process Protection System (PPS) portion of the Reactor Trip System and Engineered Safety Features Actuation System at DCPP.

To support its safety evaluation, the NRC Instrumentation and Controls Branch conducted an audit at the Invensys Operations Management (IOM) facilities in Lake Forest, California, from November 13-16, 2012. The purpose of this audit was to determine if the life cycle processes used, and the outputs of those processes, will result in a PPS for use at DCPP which will meet regulatory requirements. This audit provided information necessary to complete the NRC staff's evaluation of the proposed Tricon portion of the DCPP PPS. Enclosed is the report associated with this audit.

As noted in the enclosed audit report, the audit team was unable to observe how the design phase outputs are subject to the verification and validation process for the IOM portion of the PPS design. The NRC staff anticipates performing a follow-up audit to complete these activities when the Diablo Canyon PPS application design has been fully implemented.

The audit report also notes that there were several Open Items identified during the audit. During the follow-up audit mentioned above, the NRC staff will evaluate resolution activities for each of the Open Items listed in the enclosed audit report.

The cyber security review activities performed in conjunction with this audit are being documented in a separate report that is being written by the NRC's Office of Nuclear Security and Incident Response staff.

If you have any questions, please contact me at 301-415-1132 or via e-mail at joseph.sebrosky@nrc.gov.

Sincerely,

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

Docket Nos. 50-275 and 50-323

Enclosure:
As stated

cc w/encl: Distribution via Listserv

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

REPORT OF REGULATORY AUDIT ON NOVEMBER 13-16, 2012, IN LAKE FOREST, CA

OFFICE OF NUCLEAR REACTOR REGULATION

INSTRUMENTATION AND CONTROLS BRANCH

DIGITAL PROCESS PROTECTION SYSTEM

PACIFIC GAS AND ELECTRIC COMPANY

DIABLO CANYON POWER PLANT, UNITS 1 AND 2

DOCKET NOS. 50-275 AND 50-323

BACKGROUND

The U.S. Nuclear Regulatory Commission (NRC) staff is currently engaged in a review of a digital safety system replacement for the Diablo Canyon Power Plant, Unit Nos. 1 and 2 (DCPP). By letter dated October 26, 2011, Pacific Gas and Electric (PG&E, the licensee) submitted a license amendment request (LAR) to replace the DCPP Eagle 21 Process Protection System (PPS) with a new digital PPS (Agencywide Documents Access and Management System (ADAMS) Accession No. ML11307A332). The LAR requested NRC review and approval of the proposed design.

REGULATORY AUDIT BASIS

To support its safety evaluation (SE), the NRC Office of Nuclear Reactor Regulation (NRR), Division of Engineering (DE), Instrumentation and Controls Branch (EICB), conducted an audit at the Invensys Operations Management (IOM) facilities in Lake Forest, California. The purpose of this audit was to determine if the life cycle processes used, and the outputs of those processes will result in a PPS system for use at DCPP which will meet regulatory requirements. This audit provided information necessary to complete the NRC staff's evaluation of the Tricon portion of the proposed DCPP PPS. The scope of this audit was previously defined in the associated audit plan that was sent to the licensee on September 26, 2012 (ADAMS Accession No. ML12258A382).

AUDIT ACTIVITIES

The NRC audit team, consisting of Richard Stattel, Bill Kemper, and Rossnyev Alvarado from EICB, and George Simons, Joe Deucher, and Jeff Knight from the Office of Nuclear Security and Incident Response (NSIR), and Shiattin Makor from Region IV, visited the Invensys facility

Enclosure

in Lake Forest, California, from November 13-16, 2012, to perform a thread audit. The purpose of the audit was to determine if the life cycle processes used, and the outputs of those processes, will result in a PPS system for use at DCPP which will meet regulatory requirements.

The audit was conducted for the following aspects of the DCPP PPS software life cycle:

- **Software Verification and Validation (V&V)** – Verification that the DCPP PPS application software V&V program meets the requirements of IEEE 1012, and that the V&V program is implemented in a manner which reliably verifies and validates the design outputs of each stage of the design process.

- **Configuration Management** - Verification that the configuration management system has the appropriate hardware and software under configuration management, and that the configuration management system is effectively controlling the items included under configuration management.

- **Software Quality Assurance** - Verification that the Software Quality Assurance (SQA) program is effective in controlling the software development process to assure quality of the DCPP PPS application software.

- **Software Safety** - Verification that the software safety plans and the plans and procedures used during the software safety analysis activities were adequate to determine that the software is safe to be used in a safety related application at DCPP.

- **Tricon V10 Platform Reference Design Changes** - Verification that the impact of changes between the NRC-approved Tricon version 10.5.1 and Tricon version 10.5.3. Tricon version 10.5.3 is intended to be utilized for the DCPP PPS replacement as stated in PG&E Letter DCL-12-069, dated August 2, 2012. Verify the hardware and software changes for version 10.5.3 were developed and tested in accordance with the approved regulatory requirements for the V10 Tricon platform.

- **Cyber Security** - Review of activities associated with addressing system and services acquisition controls as set forth in the licensee's NRC-approved Cyber Security Plan, and in accordance with Section 73.54 of Title 10 of the *Code of Federal Regulations* (10 CFR), will be conducted.

AUDIT SUMMARY

1.0 Entrance Meeting (Tuesday, November 13, 2012)

At the entrance meeting, the audit team provided an overview of the audit plan and objectives for the audit. Facility logistics and a detailed audit schedule were discussed. During this meeting it was decided that the NSIR audit team would perform its review independently of the NRR and Region IV audit team.

Roman Shaffer, Project Manager (PM), introduced a number of Invensys staff members, including James Austin, Director of Manufacturing Operations for Triconex, Harry Rice,

Quality Manager – Nuclear, Kenneth Harris, Project Engineer (PE), John McKay, Application Engineer (AE), and Kevin Vu, Independent Verification and Validation (IV&V) Manager, for the DCPP PPS replacement project.

2.0 Factory Facility Tour

After the entrance meeting, Invensys staff provided a factory facility tour for the audit team. The audit team was able to view safety and non-safety Triconex instrumentation and control components that will be installed in nuclear plants in China, as well as in non-safety-related projects.

3.0 Thread Audit of the DCPP Application Software V&V Program

As described in Section B.3.2.2 of Branch Technical Position BTP 7-14, requirements thread audits are an accepted method for checking the verification and validation (V&V) efforts of the applicant. BTP 7-14 also notes that requirements thread audits are effective in viewing the "actual development process".

A thread audit of a number of system and software requirements was performed with the intent of tracking implementation requirements through each phase of the software development process using a requirements traceability matrix that Invensys refers to as a Project Traceability Matrix (PTM). Invensys is currently performing activities associated with the design phase of the software development lifecycle. The IV&V team is reviewing the Software Design Description (SDD), Invensys Document No. 993754-11-810, and the updated PTM. Because of this, the audit team was only able to trace requirements up to the design phase documentation and the audit team was unable to observe the design phase outputs being subject to the V&V process.

To facilitate the thread reviews, the Invensys PM explained the process for establishing the Triconex system requirements. During the acquisition phase, the PM prepared the Purchase Order Compliance Matrices (POCMs) using the PG&E's Purchase Order (PO), Functional Requirement Specification (FRS) (ADAMS Accession No. ML12222A095), Interface Requirement Specification (IRS) (ADAMS Accession No. ML12222A098), and Conceptual Design Description (CDD). The following POCMS were prepared for the DCPP PPS replacement project. These documents were available during the audit.

- POCM for Functional Requirement Specification, Invensys Document No. 993754-1-800-3
- POCM for Interface Requirement Specification, Invensys Document No. 993754-1-800-2
- POCM for Conceptual Design Description, Invensys Document No. 993754-1-800-1
- POCM for PO number 3500897372, Invensys Document No. 993754-1-800-0

The POCMs are used to define project scope and to identify high level functional requirements, which are later translated into traceable technical requirements that define the software and hardware needed to operate the system. These technical requirements are then described in the Software Requirement Specification (SRS), Invensys Document No. 993754-11-809 through 993754-14-809, and Hardware Requirement Specification (HRS), Invensys Document No. 993754-11-807 through 993754-14-807.

The PTM establishes the traceability of the SRS back to PG&E requirements. The audit team noted that several requirements within the PTM were deleted or marked as strikethrough. The PE explained that the POCM provided justifications for these deletions.

Thus during the thread reviews, the audit team referred to the POCM for explanation of why certain requirements had been deleted or otherwise dispositioned. For example, a requirement could have been removed because it was not a part of the Invensys' scope; instead it was part of the Westinghouse/ALS's scope.

Invensys uses the PTM to provide a means of tracking system requirements derived from the following documents:

- Procurement Specification
- Functional Requirements Specification
- Interface Requirements Specification

This PTM contains references to the following Requirements phase documents:

- Software Requirements Specification (SRS)
- Software Design Description (SDD)
- Hardware Requirements Specification (HRS)
- Hardware Design Description (HDD)

The HRS and SRS provide the requirements text to be used during the design phase for implementation of the functional level specifications. The SDD and HDD define how the system design will meet the hardware and software specifications defined in the SRS and HRS. The SDD also includes system specifications and Function Block Diagrams.

Note: The HDD was not available for review during this audit because it has not been completed.

The following threads were evaluated during this audit:

- FRS Requirement 3.2.1.10 – Response Time
- FRS Requirement 3.2.1.8.2a) – Verifying the Time Base
- FRS 3.2.1.5.3 – Channel in Bypass
- FRS Requirement 3.2.5.1.5 – Tcold signal development
- IRS Requirement 1.5.5.4 - ALS Signal Conditioning
- FRS Requirement 4.1.6 - AMSAC
- FRS Requirement 3.2.10.16.2 - Failure Mode Requirements
- Process Thread – Safety Analysis

Detailed notes for these requirements thread review audit activities are provided as Attachment 1. During the thread review, the NRC staff identified several Open Items, which are described in Attachment 1. The identified Open Items should be addressed by Invensys via its corrective action program during the upcoming design and implementation phases of the project. Each of these areas will be further evaluated during the next NRC audit which is to be performed when the PPS design implementation is complete.

4.0 Independent Verification and Validation (IV&V)

The IV&V portion of the audit was intended to confirm that the Invensys IV&V processes are implemented per its documentation, with a focus on record keeping, documentation, and management activities. Because the project has not completed the Design Phase, the audit team could not review all records related to the Triconex software development for DCPP PPS replacement project. The audit team was, however, able to review the currently completed examples of Triconex software development. Kevin Vu, the V&V manager for the project, was the primary Invensys participant for this portion of the audit.

IV&V Organization and Processes

The IV&V portion of the audit started with a thorough discussion of the IV&V processes, described in the IV&V Plan, for the application software development. The firmware development process was reviewed during the Triconex platform review, and thus it was not covered during this audit. The audit team had an extensive question and answer session with Invensys personnel about the software development processes, IV&V involvement and the V&V organization. The audit team made the following observations:

- The IV&V staff is knowledgeable of their roles in the DCPP PPS application development.

- Because of the status of the development process at the time of the audit, the IV&V staff could not point to any examples of serious conflict between the IV&V organization and a software development project organization; they were able to clearly articulate how disagreements would be escalated through the Invensys organization, should any arise.

- When asked about the level of resources needed to address the volume of work for the DCPP PPS replacement project, the IV&V manager indicated that they have more personnel available than the development team.

- When asked about the relative experience level of the IV&V organization, the IV&V manager showed training records for the IV&V staff.

The audit team reviewed the IV&V Requirement Phase Report, Revision 1. The IV&V Manager explained that this document was revised to reflect modifications to requirements in the PTM identified during the review and verification of the IV&V Requirement Report, Revision 0.

The Software IV&V plans were evaluated to determine if these plans were being effectively implemented in the requirements and design phases of the development process. An evaluation was also conducted to determine if the Invensys IV&V team was sufficiently independent in terms of cost, schedule, and management.

IV&V team members explained how identified problems will be documented and addressed using the corrective action processes. Invensys provided sample documentation of system changes, including documentation used for purposes of Configuration Management (CM).

Training Records Review

The NRC staff performed a review of the qualification and training records for one of the IV&V engineers assigned to the DCPP PPS project. The Invensys staffing plan being used for this project is contained in the Project Management Plan (Document

No. 993754-1-905). This plan contains a section (3.6.3) that outlines the training requirements for personnel assigned to the project.

The NRC staff noted that these individual training records are maintained on a project basis. As such, they are not comprehensive and do not contain historical records such as past certifications, or training achieved prior to assignment to the project. The individual's resume is included in this record so previous experience and qualification can be inferred. These records indicated that the individual did meet the minimum training requirements outlined in the plan. The NRC staff also confirmed that the individual had performed required reading, classroom training, and specialized training including Tristation Certification. No discrepancies were identified during this review.

IV&V Test Emulator

During the audit, the IV&V team demonstrated their IV&V TS1131 Emulator Test Driver. The IV&V organization developed the TS1131 Emulator Test Driver, which they use to evaluate the TS1131 application. During this demonstration, the audit team observed that:

- IV&V will create test cases and test data to use with the TS1131 Emulator Test Driver. These files will be created using the SDD, after it has been reviewed and verified by IV&V team.

- The TS1131 Emulator Test Driver was developed by the IV&V team in accordance with Invensys Project Procedures Manual (PPM) 7.04, "Software Tool Development."

The project has not entered the test phase, so the audit team could not observe test cases, test data, and simulations pertaining to DCPP PPS replacement project.

The demonstration of the emulation test tool provided the NRC staff with a better understanding of the processes that will be used to verify that the PPS software will perform as required. The NRC staff acknowledges the benefits this tool provides however, it is important to note that this tool is not considered to be a qualified IV&V test tool. Therefore, the SE will focus on the system integration and factory hardware based test activities to provide the necessary basis for its safety conclusions.

5.0 Project Procedures Manual Review

Roman Shaffer explained that the Invensys Nuclear System Integration Program Manual (NSIPM) describes the overarching approach to be followed during the DCPP PPS replacement project, and that the Project Procedures Manual (PPM) contains the implementing procedures. Specifically, the PPM governs all project quality activities performed by project personnel. Further, Roman Shaffer explained that project-specific plans or instructions (PI) have been developed to clarify requirements and/or activities. The following PIs were established for the DCPP PPS replacement project:

- PI 1.0, "Application Project Administrative Controls"
- PI 7.0, "Application Program Development"

The audit team reviewed the PPMs and PIs, and requested that they be made available to the NRC staff in the PG&E DCPP SharePoint.

Roman Shaffer explained that for the review of the Triconex platform Licensing Topical Report, the NRC staff reviewed the Engineering Procedure (EDM) and Manufacturing Procedures (MDM) associated with the design, development, test and manufacturing of the Triconex platform. However, this evaluation did not cover the Project Procedures (PPM), that are used for a Project-specific application for nuclear delivery.

Open Item: During the audit, the PM noted that the Project organization had been restructured. This new organization is reflected in PPM 1.0, "Application Project Administrative Control." This modification should be reflected in the project plans for the DCPP PPS replacement project for consistency.

6.0 Configuration Management

The Configuration Management (CM) portion of the audit focused on Invensys' record keeping, documentation management activities, and use of CM tools. The NRC audit team reviewed plans, procedures, and guides used for CM and observed how Invensys staff used tools to control and manage software and documentation, as well as track non-conformities within its processes.

Use of CM Tools

Invensys procedure PPM 4.0, "Project Document Control and Data Control," describes the process for preparing and controlling project documents. Invensys procedure PPM 2.0, "Design Control," describes the design controls for application projects. In particular, PPM 2.0 describes how design documents should be prepared, reviewed, approved, and released.

Invensys uses several CM tools throughout various stages of the application development and product manufacturing. These tools include:

- Nuclear Integration (NI) Records
- SAP business system.

The main CM tool used by Invensys is referred to as NI Records. This tool is used to store and maintain project documents, such as technical documents, application files, executable files, test files, and SQA reports. Files within NI Records are access controlled and write protected. Access is granted to select project members and requires multiple levels of approval. Although NI Records can be used from multiple computers at the same time, team members can only read or download personal copies of these records. The PM and Project Administrator (PA) are the only people with access to remove, replace, and modify files in NI Records.

Invensys uses the SAP business system to store the application project purchase order (PO).

Invensys documents discrepancies and anomalies identified during design and verification and validation of the system following the procedure described in PPM 10.0, Nonconformance and Corrective Action." PPM 10.0 describes the process to control nonconforming items and to identify appropriate corrective actions for nuclear applications. Review documents created to track non-conformances are stored in NI Records. A log is maintained in NI Records to track all modification and non-conformances associated with an application specific nuclear project.

The audit team could not review non-conformance documents associated with the DCPP PPS replacement project because the project is currently in the Design phase, and these documents have not been created.

Management and Control of the TSAP Software Application

Ken Harris, Project Engineer, and John McKay, Application Engineer, explained the process for managing and controlling the Test Specimen Application Program (TSAP) software application for the DCPP PPS replacement project. This process is described in the Invensys Software Integration Plan. During the audit, the Application Engineer noted that this plan is currently under revision to identify specific steps to be followed when developing the TSAP programs, as well as to provide a description of the secure area where they will be stored.

Invensys follows a similar process for managing and controlling other supporting documents. Specifically, Invensys will prepare and maintain documents to track modifications and non-conformances associated with the development and testing of the TSAP programs. The TSAP programs and supporting documentation are provided to the IV&V team for their review and verification. The TSAP program is then placed under formal software configuration management, as described in the Invensys Software Configuration Management Plan. The released version of the TSAP files and their associated review documentation are stored in NI Records.

The IV&V team follows the same procedure to document non-conformances of the TSAP software application during IV&V review and verification using non-conformance forms. If a modification to a file is required, the software modification is made and a revised TSAP is released.

The audit team reviewed templates that will be used to document non-conformances associated with TSAP programs. At the time of the audit, the TSAP files for the PPS had not been created, therefore, the audit team could not review specific examples associated with the DCPP PPS replacement project. This is a follow-up item that should be reviewed during the next audit.

7.0 Tricon V10 Platform Reference Design Changes

The Triconex Topical Report 7286-545-1, Revision 4, and other Tricon platform documents prepared for the PPS Replacement LAR, describe use of the Tricon V10.5.1 platform and the TriStation 1131 V4.7.0. This is also the platform version for which the NRC provided the baseline Tricon V10 SE for generic nuclear industry approval (ADAMS Accession No. ML12146A010). Since approval of the Tricon V10 platform, the Tricon platform has undergone changes for various reasons and version V10.5.3 is the most current nuclear qualified product, subsequent to two maintenance releases (V10.5.2 and V10.5.3). The TriStation 1131 has also been changed to resolve various performance issues and version V4.9.0 is the most current nuclear qualified product. These are the versions that are intended to be implemented for the DCPP PPS replacement as referenced above.

When a licensee in its application, or the NRC staff during its review, identifies a deviation from a referenced approved Topical Report (TR), the NRC staff must address this deviation in its SE for the plant-specific license amendment application. This audit was conducted, in part, to review proposed deviations from the approved Tricon V10 TR and verify that these changes were implemented pursuant to appropriate regulatory criteria as discussed in the Audit Plan (ADAMS Accession No. ML12258A382).

PG&E notified the NRC staff of Tricon V10 platform changes associated with its PPS Replacement LAR by letter dated August 2, 2012, from James M. Welsh, Pacific Gas & Electric Corporation, to U.S. Nuclear Regulatory Commission, "DCPP Units 1 and 2, Docket Numbers 50-275, 50-323, Submittal of Quality Assurance Plan and Revised Phase 1 Documents for the License Amendment Request for the Digital Process Protection System Replacement," (ADAMS Accession No. ML12222A094). Attachment 4 to this letter, IOM Document "993754-1-916, V10 Tricon Reference Design Change Analysis, Revision 0," March 19, 2012 (ADAMS Accession No. ML12222A099), provided the scope and extent of changes to the previously approved Tricon V10 Platform TR that was referenced within the LAR.

The audit team interviewed several cognizant IOM personnel involved with implementation of the hardware, software and procedural changes associated with the Tricon V10 changes and the results of these activities and observations are documented below.

7.1 System Level Differences Between V10.5.1 and V10.5.3

Implementation of V10.5.3 changes did not require any changes to the architecture of the Tricon V10 system. Per IOM platform developmental processes and procedures, this change is considered a minor maintenance release that does not impact the platform architecture or Main Processor operating software.

7.2 Hardware Changes

Tricon V10 system hardware is unchanged between V10.5.1 and V10.5.3. No new hardware or components were added in either maintenance release V10.5.2 or V10.5.3.

7.3 Software Changes

No new software modules were added to the Tricon system in maintenance release V10.5.2 or V10.5.3. However, three existing software modules in Tricon V10.5.1 have revised versions in V10.5.3:

1) AI firmware used in the NGAI Analog Input Module (3721N)

2) DO firmware used in the NGDO Digital Output Module (3625N)

3) TriStation 1131 Programming Software (TS 1131)

All other software remains unchanged from V10.5.1. For the PPS Replacement, the 3721 NGAI Analog Input Module is utilized for processing safety related analog inputs, the 3625 NGDO Digital Output Module is used for processing safety related digital outputs, and the TS1131 is the engineering tool for developing the safety-related application program.

7.3.1 Specific Software Changes – V10.5.1 to V10.5.3

Table 1 illustrates the progression of software changes for the two maintenance upgrades that have been made to the Tricon V10 system (i.e., V10.5.2 and V10.5.3). Differences in the Tricon V10.5.3 software are discussed in more detail below.

Table 1. V10.5.1 to V10.5.3 Software Module Revisions

	Identification	Version (for V10.5.1)	Version (for V10.5.2)	Version (for V10.5.3)	Used In
Main Processor	ETSX	6271	6271	6271	3008N
	IOCCOM	6054	6054	6054	3008N
Communication Module	TCOM	6276	6276	6276	4352AN, 4325BN
I/O Modules	AI/NITC	5661	5661	5661	3701N2
	EIAI/ITC	5916	5916	5916	3703EN (AI),

Table 1. V10.5.1 to V10.5.3 Software Module Revisions

	Identification	Version (for V10.5.1)	Version (for V10.5.2)	Version (for V10.5.3)	Used In
					3708EN (TC)
	AI	6256	**6285**	6285	**3721N**
	DO	6255	**6284**	**6293**	**3625N**
	PI	5647	5647	5647	3511N
	EDI	5909	5909	5909	3501TN2, 3502EN2, 3503EN2
	EAO	5897	5897	5897	3805HN
	EDO	5781	5781	5781	3601TN, 3607EN
	ERO	5777	5777	5777	3636TN
	TSDO/HVDO	6273	6273	6273	3603TN
	TSDO2	5940	5940	5940	3623TN
	RXM	3310	3310	3310	4200N, 4201N
Application Program Development Software	**TriStation 1131**, Developer's Workbench Suite	4.7.0	4.7.0	4.7.0, or **4.9.0**	**TriStation Workstation**

This table identifies changes implemented in numerous Tricon V10 modules and the TriStation 1131 Developer's Workbench Suite. However, the **boldface** items in Table 1 indicate changes from V10.5.1 version that impact the DCPP PPS LAR. Only those changes applicable to the DCPP PPS LAR will be addressed by this audit report.

7.3.2 I/O Module Operating Firmware

The Tricon operating software (firmware) in V10.5.3 was revised in two I/O modules, as follows:

- NGAI Analog Input Module (3721N):
  - AI firmware version 6256 was replaced by AI version 6285 as part of the V10.5.2 maintenance release.
- NGDO Digital Output Module (3625N):
  - DO firmware version 6255 was replaced by DO version 6284 as part of the V10.5.2 maintenance release.
  - The V10.5.3 maintenance release subsequently revised this module firmware, replacing version 6284 with DO version 6293.

No other operating software was changed from V10.5.1 to 10.5.3.

7.3.2.1 Maintenance Release V10.5.2

The V10.5.2 upgrade was initiated by IOM as a Maintenance-of-Line (MOL) project to resolve an internal diagnostic anomaly on selected I/O modules. This anomaly was discovered in the field (from non-nuclear sources) and caused random indication of a fault condition in the module. This condition was documented in Product Discrepancy Report (PDR) IRTX#21105 (Attachment 2, Reference 1) on August 25, 2008. As documented in Attachment 2, Reference 1, IOM made a determination that this anomaly did not affect the safety function of the modules, but was a source of nuisance alarms. Models 3721N (AI 6256) and 3625N (DO 6255) were affected by this anomaly.

- Model 3721N (AI 6256) is a TriStation configurable 0-5 VDC or -5-+5 VDC analog input module with 32 differential DC-coupled inputs. The model has a +6 percent over-range. The 3721N module uses the NG common core.

- Model 3625N (DO 6255) is a 24 VDC digital output module with 32 output points that use a common reference point. In addition to the Pass/Fault/Active indicator lights, this module also has indicator lights showing if each of the 32 output points is on or off. The 3625N module uses the NG common core.

This condition was documented by IOM on February 21, 2011 in Technical Advisory Bulletin (TAB) 183 (Attachment 2, Reference 2) and was issued to users of these modules to communicate operational restrictions and recommended actions to address the problem with installed modules, and announce that the problem has been resolved. As documented in Attachment 2, Reference 1, this anomaly was determined to be not reportable per 10 CFR Part 21 because this problem did not affect execution of the safety function within affected modules. Also, this product had not been shipped to customers for nuclear safety related services at that time.

Engineering Project Plan (EPP) 9100346-001, Revision 1.4 (Attachment 2, Reference 3) was prepared to delineate the Engineering actions, deliverables, and responsible individuals associated with the MOL Tricon V10.5.2 project. It prescribes the detailed Engineering development, verification, validation, certification, and documentation activities required to correct the problem and revise the software for 3625N (digital output module) and 3721N (analog input module). The audit team reviewed the Project Plan and it prescribes a process consistent with the NRC-approved Triconex development process procedures (i.e., carried out in accordance with the approved Triconex EDM procedures). The audit team also reviewed the NGIO Software Requirements Specification (SRS) (6200155-001) and verified that these changes had been included in the SRS for the modules affected by revision V10.5.2. The audit team observed that verification and validation of V10.5.2 software changes is documented in the Tricon V10.5.2 V&V Test Report, Revision 1.1 (Attachment 2, Reference 4), which documents the results of the execution of tests identified in the Tricon V10.5.2 V&V Test Plan (9600428-001). All prescribed V&V tests were conducted with acceptable results.

All Tricon configurations undergo an external, independent review and testing by TÜV Rheinland. As part of the independent review, TÜV Rheinland assesses process changes and performs full V&V including source code reviews in accordance with IEC 61508. The audit team's review of the Tricon V10.5.2 V&V Test Report determined that IOM utilized independent, external reviews of the design and testing activities for this change. TÜV reviewed all Tricon V10.5.2 Project documents and issued a confirmation letter, which states that Tricon 10.5.2 is certified against IEC 61508. Another external, independent review was performed by Wurldtech. Wurldtech performed a review of the Tricon V10.5.2 Project documents and issued its certification.

The audit team verified that the proper module versions of the V10.5.2 software were released in January 2011 with Software Release Definition (SRD) 6200003-226 (Attachment 2, Reference 5), which can be used as a configuration tool by Manufacturing, Customer Service, Marketing, and Sales. The audit team further verified that Tricon version 10.5.2 was added to the Nuclear Qualified Equipment List (NQEL) 9100150-001 for safety related nuclear applications.

7.3.2.2 Maintenance Release V10.5.3

The V10.5.3 upgrade was initiated by IOM to resolve a potential safety issue that was discovered in Tricon digital output modules. On June 21, 2011, a condition of spurious output transitions in the 3625 series digital output modules was reported under certain circumstances. The nuclear qualified digital output module 3625N was one of the affected modules. The condition was documented in PDR IRTX#22481 (Attachment 2, Reference 6) and assigned a Criticality 1, which means this condition can "Impact System Safety." As required by the Triconex Quality Assurance program, on October 12, 2011, Product Alert Notice (PAN) 25 (Attachment 2, Reference 7) was issued to alert customers of this condition and proposed appropriate compensatory actions pending a final resolution. A revision to the digital output module firmware was required to eliminate the cause of the potential spurious transitions. As documented in Attachment 2, Reference 6, this anomaly was determined to be not reportable per 10 CFR Part 21 because this condition could not cause substantial safety hazard.

Open Item: During the audit, it was not clear how this determination meets the criteria for not being reportable pursuant 10 CFR Part 21. Additional information will be required during the follow-up audit, or a submittal to the NRC staff to provide the documented basis for the determination that this condition could not create a substantial safety hazard (PDR IRTX#22481 references document "ARR 932 NSC Evaluation .pdf" (Attachment 2, Reference 8) as the apparent assessment for this determination).

Tricon PAN 25 Fix Engineering Project Plan (EPP) 9100428-001, Revision 1.2 (Attachment 2, Reference 9) was prepared to delineate the Engineering actions, deliverables, and responsible individuals associated with the MOL Tricon V10.5.3 project. It prescribes the detailed Engineering development, verification, validation, certification, and documentation activities required to correct the problem and revise the software for the 3625 series digital output module, including the 3625N. The audit team

reviewed the Project Plan and it prescribes a process consistent with the NRC-approved Triconex development process procedures (i.e., carried out in accordance with the approved Triconex EDM procedures).

The audit team also reviewed the NGDO Software Requirements Specification (SRS), (6200170-001) and verified that these changes had been included in the SRS for the modules affected by revision V10.5.3. The audit team observed that verification and validation of V10.5.3 software changes is appropriately documented in the Tricon PAN 25 Master Test Report, Revision 1.0 (Attachment 2, Reference 10). This test report documents the test results of all tests performed during the Verification and Validation of the PAN 25 resolution (i.e., defects as described in IRTX#22481 pertaining to the NGDO module), as delineated in the Tricon PAN 25 Fix Master Test Plan (9600472-001), and provides a recommendation to release the software module. All specified V&V tests were conducted with acceptable results.

The audit team's review of the Tricon PAN 25 Master Test Report also determined that IOM utilized an independent, external review resource for the design and testing activities associated with this change. TÜV Rheinland reviewed all Tricon PAN 25 project documents and issued a confirmation letter, which states that Tricon 10.5.3 is certified against IEC 61508.

The audit team verified that the proper module versions of the V10.5.3 software were released in September 2011 with Software Release Definition (SRD) V10.5.3, 6200003-230 (Attachment 2, Reference 11) The audit team further verified that Tricon version 10.5.3 was added to the Nuclear Qualified Equipment List (NQEL) 9100150-001 for safety related nuclear applications.

7.3.3 TriStation 1131 Application Programming Software Change V4.9.0

The TriStation 1131 Developers Workbench is a software tool designed to generate the plant-specific application programs. The software runs on a standard commercial personal computer using the Windows operating system. The TriStation 1131 Developers Workbench does not perform safety-related functions, but allows the user to generate safety-related software for the Tricon controller. Tricon version V10.5.3 includes an updated version of the TriStation 1131 programming software. The Tricon V10.5.1 system was originally released with TriStation 1131, version 4.7.0. This programming software suite has since been upgraded to correct performance issues and has been made available as TriStation 1131 V4.9.0 for use in Tricon V10.5.3 systems.

The TriStation version 4.9.0 upgrade was initiated as a MOL project to resolve accumulated PDRs and to add minor functional improvements to the TriStation and Safety Suite Applications product. The project included resolution of several high priority safety-significant PDRs for conditions noted in Product Alert Notices (PANs) 22 and 24 (Attachment 2, References 12 and 13), and Technical Advisory Bulletin (TAB) 147 (Attachment 2, Reference 14).

The TriStation 1131 V4.9.0 change did not add any new features, but provided enhancements to existing features. Therefore, the TriStation 1131 V4.9.0 maintains the features described in the V10 SE (ADAMS Accession No. ML12146A010). The TriStation V4.9.0 and Safety Suite Apps Engineering Project Plan, document 9100359-001 (Attachment 2, Reference 15), was prepared to identify the Engineering actions, deliverables, and responsible individuals associated with the MOL TriStation 1131 V4.9.0 project. It prescribes the detailed Engineering development, verification, validation, certification, and documentation activities required to correct the problems documented in Attachment 2, References 12, 13, and 14, and to revise the TriStation 1131 software. The audit team reviewed the Project Plan and it prescribes a process consistent with the NRC-approved Triconex development process procedures, and contains a complete list of deliverables for the project with regard to the software changes and enhancements. The audit team reviewed some of the deliverables associated with this change. The TriStation 1131 Software Design Specification, Document 6200168-002, Revision 1.48, incorporates the software changes required to resolve the problems noted above with the pre-V4.9.0 versions of the TriStation 1131. The audit team observed that verification and validation of TriStation V4.9.0 software changes are appropriately documented in the TriStation V4.9.0 Test Report, Revision 0.4 (Attachment 2, Reference 16). This test report documents the successful test results of all tests performed during verification and validation of the problems documented in Attachment 2, References 12, 13, and 14, as delineated in the TriStation 1131 V4.9.0 V&V Test Plan, Revision 1 (9600442-002), and provides a recommendation to release the software module. All specified V&V tests were conducted with acceptable results.

The audit team verified that the proper versions of the TriStation V4.9.0 software were released in August 2011 with Software Release Definition (SRD) 6200097-038, Revision 1.2 (Attachment 2, Reference 17). The audit team further verified that TriStation V4.9.0 was subsequently added to the Nuclear Qualified Equipment List (NQEL) 9100150-001 for safety related nuclear applications.

7.4 Regulatory Evaluation

7.4.1 Development Process

The regulations in 10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. SRP Chapter 7, Appendix 7.0-A, Section 3.H, "Review Process for Digital Instrumentation and Control Systems," states that

> All software, including operating systems, that is resident on safety system computers at runtime must be qualified for the intended applications. Qualification may be established either by producing the PDS [pre-developed software] items under a 10 CFR 50, Appendix B quality assurance program or by dedicating the item for use in the safety system as defined in 10 CFR 21.

On April 12, 2012, the NRC staff approved the Tricon V10 system developmental processes in its SE (ADAMS Accession No. ML12146A010), which included process changes from that which was approved in the V9 Tricon SE dated December 11, 2001 (ADAMS Accession No. ML013470433). The IOM development process is contained in three IOM documents that govern IOM internal development; the Quality Assurance Manual (QAM), Quality Procedure Manual (QPM), and the Engineering Department Manual (EDM).

In developing the Tricon V10.5.3 system, several changes, additions, and deletions were made to the development process. Changes to these IOM developmental process documents that govern IOM internal development processes were reviewed during this audit and are described below:

Since the V10.5.1 version was submitted for NRC staff approval in 2010, Table 2 provides a summary of changes to EDM procedures that have occurred and are applicable to the V10.5.2 and V10.5.3 software revisions:

Table 2: Developmental Process and Procedure Changes

EDM Procedure Title	Procedure Number	Revision (used for V10.5.1)	Revision Date	Revision (used for V10.5.2 and 10.5.3)	Revision Date
Product Development Process	12.00	4.9	12/3/2010	5.0 5.1 5.2	4/27/2011 5/20/2011 6/5/2012
Project Planning	12.10	7.1	6/29/2009	7.2 7.3	4/7/2011 11/4/2011
Design Review	12.30	3.1	9/15/2009	3.2 3.3 3.4	10/7/2011 1/6/2012 6/5/2012
Requirements Management	12.50	0.0	9/18/2006	1.0	10/26/2011
Engineering Change Order Control	21.00	4.5	11/19/2010	4.6	1/6/2012
Change Impact Analysis	21.30	3.4	10/15/2010	3.5 3.6 4.0 4.1	5/20/2011 1/6/2012 4/20/2012 5/31/2012
Software Development Guidelines	40.50	1.4	10/15/2007	1.5	6/5/2012
Product Verification	90.00	4.3	3/19/2010	4.4	3/22/2011
Product Validation	90.10	1.3	7/26/2010	1.4	3/22/2011
Control of Tools	90.30	1.0	3/25/2008	1.1	9/1/2011

Table 2: Developmental Process and Procedure Changes

EDM Procedure Title	Procedure Number	Revision (used for V10.5.1)	Revision Date	Revision (used for V10.5.2 and 10.5.3)	Revision Date
and Test Software					

The NRC staff reviewed each of these IOM Development Process procedure changes and determined that these changes were either editorial, clarified/strengthened existing development processes, or reflect stronger conformance to industry and IEC standards.

The NRC staff identified no reduction in previous commitments in these changes. No other IOM Development Process procedures applicable to the V10.5.2 and 10.5.3 software upgrades were changed or discussed.

7.4.2 V10.5.1 to V10.5.3 Software Changes

The results of this audit indicates that the Tricon V10.5.2 and V10.5.3 platform software changes were developed using the same high quality design and development process used to develop the original Tricon V10.5.1 software components. The details of this assessment are addressed above. The development process was approved in the NRC staff SE on the original Tricon V9 TR and updated as appropriate in the Tricon V10.5.1 TR SE. Based on the information reviewed by the audit team, the Tricon V10.5.2 and V10.5.3 platform software changes appear to meet the operational and safety requirements for the DCPP PPS application and are acceptable for use in safety-related applications at nuclear power plants. However, in order to substantiate this conclusion in the DCPP PPS SE, the documents referenced in Attachment 2 are required to be submitted on the docket. This is consistent with information referenced in Enclosure B of Interim Staff Guidance ISG-06, Revision 1, Digital I&C Licensing Process that is required to be submitted on the docket for an LAR referencing a Tier 2 platform.

8.0 Cyber Security

The Cyber Security review activities performed in conjunction with this audit are being documented in a separate report that is being written by NSIR personnel.

9.0 Exit Meeting (Friday – November 16, 2012)

During the exit meeting, Invensys was provided with a summary of the Open Items identified during the audit. In addition, a list of documents was provided with a request to provide the NRC staff access in order to complete its review activities. This list is provided in this report as Attachment 2.

CONCLUSION

The NRC staff addressed each of the planned audit activities outlined in the audit plan. Eight requirements threads were selected and evaluated for compliance with the DCPP specific

planning documents. Interviews were conducted with Invensys personnel from the IV&V, Design Engineering, Quality Control, and Configuration Management groups. The following Open Items were identified during this audit.

- During the audit, the PM noted that the Project organization had been restructured. This new organization is reflected in PPM 1.0, "Application Project Administrative Control." This modification should be reflected in the project plans for consistency.

- When a requirement is not implemented in the system design or if it is being implemented via another requirement, the justification is provided in the POCM. Because the POCMs were not available to the NRC staff prior to the audit, there was an appearance that the requirements implementation was not complete. The NRC staff therefore requested that the POCM documents are made available to the NRC on SharePoint. The NRC staff will refer to these documents for follow-up requirements tracing activities.

- In several cases where FRS requirements are being fulfilled via other identified requirements, the POCM does not provide a means of tracing these requirements to the part of the design that is credited for meeting the requirement. As an example, many of the FRS requirements were applicable only to the ALS portion of the PPS system. The POCM did not always state that these requirements were outside of the Tricon scope though this was apparent in many cases. In the case of the thread, FRS-3.2.1.10, no reference to the alternate IRS specification IRS-1.5.8 was provided in either the PTM or the POCM. Invensys should evaluate the extent of this issue and initiate corrective actions to ensure the completeness of requirements implementation in the PPS design.

- At the time of the audit, the software development had only progressed to design phase of the software development lifecycle. Because of this, the audit team was only able to trace requirements up to the design phase documentation some of which was still in development or had not been verified and validated.

- While reviewing the SDD, the audit team discovered that Requirement R-3001 is identified in Section 3. 7.1.9.1, "Process the Input Signals." However, this requirement was not identified in the functional diagrams included in the Appendices of the SDD. Invensys should evaluate the extent of this issue and initiate corrective actions to ensure the completeness of requirements implementation in the PPS design.

The audit team was unable to observe how the design phase outputs are subject to the V&V process. The NRC staff anticipates performing a follow-up audit to complete these activities when the DCPP PPS application design has been fully implemented. During this follow-up audit, the NRC staff will evaluate resolution activities for each of the Open Items listed above. The NRC staff will also review SDC examples associated with the DCPP PPS replacement project during this audit.

Principal Contributors: Richard Stattel, NRR/DE/EICB
Bill Kemper, NRR/DE/EICB
Rossnyev Alvarado, NRR/DE/EICB

Date: March 4, 2013

Attachments
1. Detailed Requirement Thread Notes
2. List of Requested Records

REGULATORY AUDIT REPORT FOR NOVEMBER 13–16, 2012, AUDIT

DIABLO CANYON POWER PLANT, UNITS 1 AND 2

DIGITAL PROCESS PROTECTION SYSTEM

DETAILED REQUIREMENT THREAD NOTES

FRS Requirement 3.2.1.10 – Response Time

This requirement states that the maximum response time for the PPS shall be 409 milliseconds. This requirement was found on page 27 of the PTM and is identified as requirement number 967. The PTM adds clarification to this requirement by stating that the delay time is defined as the elapsed time following a step change at the signal conditioner from 5 percent below to 5 percent above a setpoint with all externally adjustable transfer functions set to one and all externally adjustable time delays set to zero.

The PTM does not provide traceability for this requirement to the SRS, HRS or the SDD. To determine the reason for this apparent omission, the NRC staff was referred to the POCM. Here the requirement was labeled as "Information Only" and an explanation was provided that the Tricon throughput time will be dependent on several factors. It also states that Invensys does not anticipate any issues with meeting throughput time for Tricon and states that the requirement will be verified during the project test phase.

The NRC staff was then directed to Section 1.5.8 of the Interface Requirements Specification which does provide a traceable path for meeting this requirement. Because PPS time response is shared between the ALS and Tricon portions of the PPS system for functions requiring RCS temperature inputs, an allocation breakdown of times available was performed and the Tricon portion of the time response allocation is 200 milliseconds. This requirement traces to Section 3.3.2.5 of the SRS as a single requirement which states that:

> The Tricon Protection Set total throughput time shall not exceed 200 mS.

This requirement is repeated for all four protection sets (same Section 3.3.2.5 of four documents).

Open Item: When a requirement is not implemented in the system design or if it is being implemented via another requirement, the justification is provided in the POCM. Because the POCMs were not available to the NRC staff prior to the audit, there was an appearance that the requirements implementation was not complete. The NRC staff therefore requested that the POCM documents be submitted to the NRC. The NRC staff will refer to these documents for follow-up requirements tracing activities.

The hardware implementations for IRS1.5.8 are traceable to the HRS. Section 4.8 of the HRS identifies this as requirement R3004 and it restates the requirement as follows:

> The V10 Tricon shall meet a 200 mS throughput for the DTTA OTDT, and OPDT Reactor Trip protection functions.

This requirement was traceable to the SDD as well. The PTM points to Section 2.8.2.2 of the SDD. This also refers to requirement R3004 for establishing time response requirements as follows:

> Scan Time will be set in accordance with Max TSAP scan time document 993754-1-817.

This document contains the calculation that determines the expected execution times for the DCPP application and it is being evaluated separately. The results of this calculation determined that the maximum TSAP scan time setting to be used for the DCPP PPS application is 63.4 mS in order to meet the 200mS throughput requirement stated in the FRS.

Open Item: In several cases where FRS requirements are being fulfilled via other identified requirements, the POCM does not provide a means of tracing these requirements to the part of the design that fulfills the requirement. As an example, many of the FRS requirements were applicable only to the ALS portion of the PPS system. The POCM did not always state that these requirements were outside of the Tricon scope though this was apparent in many cases. In the case of this thread, FRS-3.2.1.10, no reference to the alternate IRS specification IRS-1.5.8 was provided in either the PTM or the POCM. Invensys should evaluate the extent of this issue and initiate corrective actions to ensure the completeness of requirements implementation in the PPS design.

FRS Requirement 3.2.1.8.2a) – Verifying the Time Base

This requires that IO signal processing shall have the means of verifying measurable time base with an accuracy of 0.1 percent.

> The measurable time base shall have an accuracy of +- 0.1% of the utilized time base (e.g., for a 100 msec time base this would be +-0.1 msec).

This requirement is listed in the PTM as ID No. 963 with a requirement number of R-801. This requirement then traces to Section 4.5.1.2 of the HRS. This section of the HRS repeats the requirement but does not provide any clarification or implementation details. Since the Hardware Design Description was not completed at the time of this review, the details of implementation are not available for audit. This audit item should be followed through to ensure implementation of this requirement when design implementation of the PPS is completed.

FRS 3.2.1.5.3 – Channel in Bypass

This requirement defines functional characteristics of the Channel in Bypass switches in the PPS system. This requirement maps to several requirements in the PTM:

- R-785 – Bypass of channel causes Alarm (MAS)
- R-786 – One contact of the switch is used to satisfy the indication requirements
- DR-786-01 – Exception of Trip over Bypass priority for Turbine Impulse Chamber High pressure function

Requirement R-785 traces to the SRS Section 3.3.1.2.3 which requires that the TSAP provide a signal upon actuation of any comparator Bypass Function or channel OOS function.

This requirement also maps to various SDD sections for each of the signals that have channel bypass functions associated. This audit item should be followed through to ensure implementation of this requirement when design implementation of the PPS is completed.

FRS Requirement 3.2.5.1.5 – Tcold signal development

This requirement states that the Tricon TSAP shall calculate a filtered average cold leg temperature, Tfcavg, signal using the two (2) TCold RTD inputs. This requirement includes four constraints. For this thread, the following constraints were reviewed:

a) All Tcold inputs shall be processed through a Lag Filter per Section 3.2.5.13.1.

b) Only Tcold signals that have been validated by the Sensor Quality Algorithm (SQA2) [Reference Section 3.2.5.13.8] shall be used in the Tfcavg calculation.

Using the PTM, the NRC staff identified requirements R-872 and R-873 for these requirement constraints, respectively. Also, the PTM identifies the sections in the SRS and SDS in which these requirements are described. Requirement R-872 is described in Section 3.3.5.12.1 of the SRS, which states "The Tricon TSAP shall process all TCold inputs through a Lag Filter. See SRS Section 3.3.5.12.1." This requirement is being met using the analog signal from the ALS portion of the PPS and a standardized lag filter, defined in Section 3.2.5.13.1 of the FRS. Requirement R-873 is described in Section 3.3.5.1.1 of the SRS, which states "The Tricon TSAP shall only use TCold signals that have been validated by the Sensor Quality Algorithm (SQA2) in the Tfcavg calculation. See SRS Section 3.3.5.12.7." This requirement is being met for the analog signal from the ALS portion of the PPS and the SQA2 function, which is described in Section 3.3.5.12.7 of the SRS.

The Software Design Specification was then consulted to determine how these requirements were being implemented for the DCPP PPS replacement project.

For requirement R-872, Section 3.7.1.9.1, "Process the Input Signals," provides a description of how the input signal for the cold leg temperature (aTE410B) uses the lag function, and its

associated tuning constant (eL1_410B_tau7). The SDD also provides a diagram which represents this algorithm. Appendix 4, DTTA_PSI.vsd: Cold Temp, sheet 15 of 27, includes a block labeled "LAG FILTER PGE" inputs represents how the analog inputs from the AI SCALE block goes into the Lag function.

For requirement R-873, Section 3.1.1.9.4.7 "Sensor Quality Algorithm 2 (SQA2)" provides a description of specific settings for the Sensor Quality Algorithm 2 (SQA2). Specifically, for this requirement "The SQA2 CFB validates the THot signals and uses only the validated signals to calculate the TfCAvg." This seems to be inconsistent with the description provided in the SRS, since R-873 is associated with Tcold and not Thot. Since the SDD was under review and verification at the time of the audit, the design team could not modify the SDD to address this inconsistency. The SDD also provides the logic diagram that represents this algorithm. This logic diagram is provided in Appendix 4, DTTA_PSI.vsd: SQA2 Voting, sheet 13 of 27, which includes a block labeled "SQA2" showing the temperature signal, fT410B (from sheet 5, AI Scale block), inputting the SQA2 block. The Software Design Description provides additional details on how these algorithms function.

At the time of the audit, the test cases for providing functional verification of the R-872 and R-873 were not available for review. This audit item should be followed through to ensure implementation of this requirement when design implementation of the PPS is completed.

IRS Requirement 1.5.5.4 ALS Signal Conditioning

This requirement states that the temperatures shall be transmitted from the ALS to the Tricon via 4-20 mA analog signals scaled per Appendix 3.1, "I/O List." Note that for this audit, the audit team used Revision 4, which did not include Appendix 3.1. However, the PE had a copy of Revision 6 which included the I/O list. The audit team used Revision 6 to perform this thread.

Using the PTM, the NRC staff identified requirements R-3001 for this IRS section. Also, the PTM identifies the sections in the SRS, HRS, and SDS in which this requirement is described. Requirement R-3001 could not be found in the SRS. However, Section 3.3.5.8.1 of the SRS, identifies requirements associated with scaling temperature signals from the ALS. This section identifies requirements originating in the FRS related to scaling temperature signals. Specifically Section 3.2.5.9.1 describes how the temperature signals from ALS should be scaled. Based on this, the audit team used the section identified in the SRS to continue the thread.
Section 3.3.5.8.1 of the SRS identifies Requirements R-913 and R-914, and their respective derived requirements (DR-913 and DR-914, respectively) to scale temperature signals from ALS. For example, Requirement R-913 states that the Tricon TSAP shall scale the Class I 4-20 mA THot input signal to a calibrated range of 530 to 650°F.

The PTM identified Section 5.4 in the HRS for this requirement. However, this information was strikethrough, meaning that this requirement was no longer covered in the HRS. The audit team reviewed the POCM for IRS to observe the explanation, which stated that signal scaling is made via software.

The Software Design Specification was then consulted to determine how these requirements were being implemented for the DCPP PPS replacement project. Section 3.7.1.9.1, "Process

the Input Signals," describes how input signals are processed. For requirement R-913, this section states that "the Hot Leg Temperature 1A, (wTE410A), has an engineering unit span of 530-650 degrees F." The SDD also provides a diagram which represents the algorithm for scaling Analog Inputs. Appendix 4, DTTA_PSI.vsd: Hot Temp 1A, sheet 7 of 27, includes a block labeled "AI Scale" inputs representing how the analog inputs are used in the AI Scale block. For requirement R-914, this section states that "the Cold Leg Temperature 1B, (wTE410B), has an engineering unit span of 510-630 degrees F." The SDD also provides a diagram which represents the algorithm for R-914. Appendix 4, DTTA_PSI.vsd: Cold Temp 1, sheet 15 of 27, includes a block labeled "AI Scale" inputs representing how the analog inputs are used in the AI Scale block. The Software Design Description provides additional details on how these algorithms function.

Open Item: While reviewing the SDD, the audit team discovered that Requirement R-3001 is identified in Section 3. 7.1.9.1, "Process the Input Signals." However, this requirement was not identified in the functional diagrams included in the Appendices of the SDD.

Since the SDD was under review and verification at the time of the audit, the design team could not modify the SDD to address this inconsistency.

At the time of the audit, the test cases for providing functional verification of the R-913 and R-914 were not available for review. This audit item should be followed through to ensure implementation of this requirement when design implementation of the PPS is completed.

FRS Requirement 4.1.6 AMSAC

This requirement states that the PPS shall provide shared signals from the S/G Narrow Range Level and Turbine Impulse Chamber Pressure channel sensor inputs to interface with the AMSAC.

The PTM does not identify a requirement for this FRS item. The audit team reviewed the POCM for FRS and found that the remark section for this item states that this is for information only, since wiring to AMSAC is not part of Invensys scope. No further information was reviewed.

FRS Requirement 3.2.10.16.2 Failure Mode Requirements

This requirement states that the Steamline Break Protection channels shall be designed so that upon detection of a fatal PPS processing instrumentation error or failure, the output of each trip or interlock channel is an actuation signal.

Using the PTM, the NRC staff identified requirement R-1065 for this item. Also, the PTM identifies the sections in the SRS, HRS, and SDS in which this requirement is described. Requirement R-1065 is described in Section 3.3.9.15 of the SRS, which repeats the description provided in the FRS. This requirement is described in Section 4.6.2 of the HRS.

The Software Design Specification was then consulted to determine how these requirements were being implemented for the DCPP PPS replacement project. Sections 3.9.1.9.3, 3.9.2.9.3,

3.9.3.9.3, and 3.9.4.9.3, "Generate Discrete Output Signals" (all with the same title) provide the following description for this requirement: "The Tricon TSAP will cause the output of each Steamline Break Protection trip or interlock channel to actuate upon detection of fatal faults (fL1_FATAL). See Section 3.2.1.9." Section 3.2.1.9 of the SDD describes system diagnostic, module diagnostic, and annunciation of alarms. In the case of R-1065, this signal will be sent to the Fatal Diagnostics signal, (fL1_FATAL), which will drive all discrete outputs in the event of a Fatal Diagnostic. The SDD also provides a diagram which represents the algorithm for Steamline break protection. Appendix 6, Steamline Break Protection PS I.vsd: Loop 1 Low SI, sheet 2 of 9, shows the logic to create a signal to trip in case of steamline break. The Software Design Description provides additional details on how these algorithms function.

At the time of the audit, the test case for providing functional verification of the R-1065 was not available for review. This audit item should be followed through to ensure implementation of this requirement when design implementation of the PPS is completed.

Process Thread – Safety Analysis

The Software IV&V Plan refers to IEEE Std. 1012 for direction on performing the Safety Analysis task. The safety analysis is broken into the following four parts:

a. Criticality

b. Hazard

c. Risk

d. Interface

The IV&V summary report for the requirements phase 993754-1-860 identifies a report, (Document No. 993754-1-915 Revision 0) as supporting documentation for performance of this task. Within this Safety Analysis report are the four task reports that describe the results of each subtask.

This report identifies any hazards introduced to the system during the phase. For the requirements phase, the following hazards were identified:

- Interface – 2 Hazards, H-1, & H-3(a)
- Criticality – 0 Hazards
- Hazard Analysis – 3 Hazards, H-2, H-3 a & b and H-4
- Risk – H-1, H-2, H-3 a & b, and H-4

The NRC staff reviewed these hazards and confirmed that each was properly identified, documented and had been entered into the corrective action program to be addressed during subsequent phases of the software development. The Safety Analysis and IV&V summary report will describe hazards identified during all phases of software development and should describe how these hazards are resolved. These documents are expected to be submitted to the NRC during the next Phase 2 supplement.

REGULATORY AUDIT REPORT FOR NOVEMBER 13–16, 2012, AUDIT

DIABLO CANYON POWER PLANT, UNITS 1 AND 2

DIGITAL PROCESS PROTECTION SYSTEM

LIST OF REQUESTED RECORDS

It is necessary for the following documents to be made available to the NRC staff to facilitate completion of 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 DCPP PPS.

References (Documents Required to be Submitted on the Docket):

1. Product Discrepancy Report (PDR) IRTX#21105
2. Technical Advisory Bulletin (TAB) 183
3. Engineering Project Plan (EPP) V10.5.2, 9100346-001, Revision 1.4
4. Tricon V10.5.2 V&V Test Report, Revision 1.1, January 14, 2011
5. Software Release Definition (SRD) V10.5.2, 6200003-226, Revision 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, Revision 1.2
10. Tricon PAN 25 Master Test Report, Revision 1.0
11. Software Release Definition (SRD) V10.5.3, 6200003-230, Revision 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, Revision 1.3
16. TriStation V4.9.0 Test Report, Revision 0.4
17. Software Release Definition (SRD) 6200097-038, Revision 1.2

The cyber security review activities performed in conjunction with this audit are being documented in a separate report that is being written by the NRC's Office of Nuclear Security and Incident Response staff.

If you have any questions, please contact me at 301-415-1132 or via e-mail at joseph.sebrosky@nrc.gov.

Sincerely,

/RA/

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

Docket Nos. 50-275 and 50-323

Enclosure:
As stated

cc w/encl: Distribution via Listserv

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

ADAMS Accession No.: ML13018A149

OFFICE	NRR/DORL/LPL4/PM	NRR/DORL/LPL4/LA	NRR/DE/EICB/BC	NRR/DORL/LPL4/BC	NRR/DORL/LPL4/PM
NAME	JSebrosky	JBurkhardt	JThorp (RStattel acting)	MMarkley	JSebrosky
DATE	1/29/13	1/25/13	2/22/13	3/1/13	3/4/13

OFFICIAL RECORD COPY