DIABLO CANYON POWER PLANT
DIGITAL PROCESS PROTECTION SYSTEM REPLACEMENT
LICENSING EXPERIENCE USING ISG-06

Kenneth J. Schrader, MSNE
Pacific Gas & Electric Co.
PO Box 56
Avila Beach, CA 93424
kjse@pge.com

Scott B. Patterson, PE, PMP
Pacific Gas & Electric Co.
PO Box 56
Avila Beach, CA 93424
sbp1@pge.com

John W. Hefler, PE
Altran Solutions Corp.
235 Montgomery Street
San Francisco, CA 94104
jhefler@altransolutions.com

Edward (Ted) L. Quinn
ANS Past President
Technology Resources
23292 Pompeii Drive
Dana Point, CA 92629
tedquinn@cox.net

ABSTRACT

This paper provides a summary of the preparation of a License Amendment Request (LAR) for replacement of the existing Diablo Canyon Power Plant (DCPP) Eagle 21 digital Process Protection System (PPS) by Pacific Gas & Electric Company (PG&E) using US Nuclear Regulatory Commission (USNRC) Digital I&C (DI&C) Interim Staff Guidance (ISG) document ISG-06, Licensing Process [1]. The USNRC has designated the LAR for the DCPP PPS replacement project as the pilot application for use of DI&C ISG-06. DI&C ISG-06, Revision 1, issued for use on January 19, 2011, describes the licensing process the NRC staff may use to review an LAR for a DI&C modification. The LAR [2] for the replacement of the Eagle 21 PPS was submitted to the NRC on October 26, 2011, was accepted for review [3] on January 13, 2012, and is currently under review.

The use of pre-application (Phase 0) public meetings with the NRC staff to ensure the PPS replacement design adequately addressed NRC criteria was instrumental to development of the proposed PPS replacement design. This paper discusses the topics discussed in the Phase 0 meetings and the approach utilized by PG&E for the Phase 0 public meetings to support efficient

development of the proposed PPS replacement design. PG&E developed a PPS Replacement diversity and defense-in-depth (D3) Assessment Topical Report [4] that was submitted to NRC in 2010 and approved [5] in 2011. This paper discusses the PG&E use of the D3 assessment to evaluate and optimize the initial PPS replacement design prior to submittal of the design to the NRC for approval. The PG&E experience with preparation of the LAR contents and supporting documents is discussed.

Key Words: Digital, Licensing, RPS, RTS, ESFAS, Defense-in-Depth

1 INTRODUCTION

Pacific Gas & Electric Company (PG&E) has submitted a License Amendment Request (LAR) [2] to obtain USNRC approval to replace the existing Diablo Canyon Power Plant (DCPP) Eagle 21 digital Process Protection System (PPS). PG&E used US Nuclear Regulatory Commission (USNRC) Digital I&C (DI&C) Interim Staff Guidance (ISG) document ISG-06, Revision 1, Licensing Process [1] to prepare the LAR. DI&C ISG-06 was developed through a joint industry working group coordinated by the Nuclear Energy Institute. PG&E was an active participant in the working group and provided input to ISG-06 during its development. The USNRC designated the LAR for the DCPP PPS replacement project as the pilot application for use of DI&C ISG-06 [6]. DI&C ISG-06, Revision 1, issued for use on January 19, 2011, describes the licensing process the USNRC staff may use to review an LAR for a DI&C modification. The LAR [2] for the replacement of the Eagle 21 PPS was submitted to the USNRC on October 26, 2011 and was accepted [3] for review on January 13, 2012. The LAR is currently under review and USNRC approval is expected in fall of 2013.

The existing digital Westinghouse Eagle 21 Process Protection System (PPS), that provides the processing portion of the protection system, is being replaced to address obsolescence and maintenance issues. Eagle 21 was installed in 1994 to replace the original analog Westinghouse 7100 PPS.

The digital process protection system (DPPS) proposed in the LAR maintains the current Westinghouse 4-channel, 2-train protection system architecture without affecting existing diverse systems (nuclear instrumentation system, ATWS mitigation system). The DPPS proposed in the LAR is based on the Invensys Operations Management Triconex Tricon processor and the CS Innovations, LLC (a Westinghouse company) Advanced Logic System (ALS). The use of both the Tricon and ALS systems as part of the DPPS architecture precludes the need for a Diverse Actuation System (DAS).

1.1 Pre-application (Phase 0) public meetings for the proposed Digital Process Protection System (DPPS)

DI&C ISG-06 [1] allows the use of the public meeting process for licensees to engage the USNRC in a pre-application discussion of how a proposed DI&C upgrade LAR will address issues such as diversity and defense-in-depth (D3), significant variances from current guidance, and other unique or complex topics associated with a proposed design. These pre-application meetings are designated as “Phase 0” meetings in DI&C ISG-06. Interdivisional digital communications, non-safety related equipment, diversity, redundancy, D3 assessment, manual operator actions, best-estimate analyses, software development, and deviations from USNRC

staff positions are examples of unique or complex topics that would be discussed. The Phase 0 meetings are intended to be two-way discussions in which the USNRC can provide feedback on critical aspects of the proposed design that are likely to affect the USNRC staff's evaluation. The staff issues meeting summaries that capture the topics discussed in the meeting and provides a preliminary USNRC staff assessment of the unique and complex topics.

The use of pre-application Phase 0 public meetings with the USNRC staff to ensure the PPS replacement design adequately addressed USNRC criteria was instrumental to development of the proposed PPS replacement design and an LAR that met the USNRC staff acceptance review requirements. The staff feedback provided on the diversity, communications, maintenance terminal, Class I/II isolation, software, and security aspects of the design permitted PG&E to proactively address areas of staff concern and to finalize design aspects where licensing uncertainty existed. PG&E found that it was important during the Phase 0 meetings to specifically identify to the staff, during the meeting, which items that staff feedback was desired to be included in the meeting summary.

PG&E held six meetings with the USNRC staff prior to the submittal of the LAR; two initial meetings beginning in 2006 to inform the staff of the planned scope and schedule for the project, and four Phase 0 meetings. The topics discussed in the DCPP Phase 0 meetings included the design redundancy and diversity, D3 assessment, communications, software development, and connections to the non-safety workstation and plant process computer.

To reduce licensing uncertainty for the project, PG&E instituted a design approach to develop a PPS replacement that was as simple as possible while eliminating the need for any manual operator actions to address software CCF in the PPS. State of the art safety-related DI&C platforms contain numerous functions and features that are not needed for all applications. These platforms are typically capable of being configured in multiple ways. Creating a simple DI&C protection system design requires considerable control and focus during the design phase to ensure that only the functions, features, and configurations that are required are utilized.

The two most significant areas of focus for the DCPP DPPP design are diversity and communications. By employing both the Tricon and ALS DI&C systems in the DPPS design, internal diversity is provided to mitigate the effects of a software CCF. This eliminates the need to perform best-estimate accident analyses, to evaluate manual operator actions to address common cause software failure, and to include a DAS in the design. Avoiding the need for a DAS is an important goal because the addition of a DAS to the plant complicates the protection system, increases the possibility of a protection system inadvertent actuation, and results in an additional system that needs to be operated, tested, and maintained. To simplify the communications, a design with four separate and independent channels was developed such that there is no communications between the redundant channels (no cross-channel communications) and no voter function between the channels. The design does not employ two-way communications in the safety-related portion of the system. The staff provided feedback in a meeting summary to PG&E that not including cross-channel communications or voting functions in the design was expected to simplify the USNRC review process. Another goal to reduce licensing uncertainty for the project was to ensure the DPPS design met all applicable requirements. While this requires diligence during the design phase to ensure each applicable

requirement will be met, it avoids the licensing risk associated with requesting USNRC approval of exceptions or deviations from requirements.

The DPPS design employs a non-safety related maintenance terminal for each of the four protection channels that is connected the DPPS during normal operations. This design feature received focused USNRC attention during the Phase 0 meetings. The use of a separate maintenance terminal for each protection channel eliminated issues related to use of a multidivisional maintenance terminal. The staff provided feedback during the Phase 0 meetings and in the meeting minutes that, although the use of a non-safety related maintenance terminal that is connected to the DPPS during normal operations had been previously approved for another licensee, this feature required significant additional staff review effort.

1.2 Diversity and Defense-in-Depth Assessment

Defense-in-depth is providing protective barriers or means that provide overlapping or compensating means of addressing faults in other defensive barriers. For nuclear plant DI&C systems, defense-in-depth is achieved through four echelons of defense; the control system, the reactor trip system (RTS), the engineered safety features actuation system (ESFAS), and the monitoring and indication system. For DI&C, diversity is a principal of using different technologies, equipment, vendors, equipment, logic, algorithms, development teams, and functions to provide a diverse means to perform a safety function. For nuclear plant DI&C systems, a CCF in software, although considered beyond design basis, needs to be considered. A D3 assessment in accordance with USNRC Branch Technical Position (BTP) 7-19 [7] needs to be performed as part of licensing a DPPS.

Obtaining USNRC approval of the D3 assessment of the DCPP PPS replacement design was determined by PG&E to be a critical aspect in establishing an initial design that the USNRC could approve without requiring further modification. PG&E developed a PPS Replacement D3 Assessment Topical Report [4] that was submitted to USNRC in 2010 and approved in 2011 [5], prior to submittal of the LAR for PPS replacement. While a D3 assessment is normally performed after a protection system design is developed, PG&E used the D3 assessment to evaluate and optimize the initial PPS replacement design prior to submittal of the design to the USNRC for approval.

To perform the D3 assessment for the PPS replacement project, PG&E reviewed the Diablo Canyon Final Safety Analysis Report Update (FSARU) Chapter 15 licensing basis accident analyses and the USNRC Safety Evaluation Report (SER) for the current Eagle 21 protection system to determine the events that required the Process Protection System for primary or backup protection. The D3 assessment was performed in accordance with USNRC Branch Technical Position (BTP) 7-19 [7]. The assessment considered a PPS common cause failure (CCF) concurrent with each Chapter 15 event and accident for which a mitigation action by the PPS was credited in the analysis.

The assessment identified protection functions that are performed outside the PPS or do not require a backup; these functions are not affected by a CCF in the PPS. For functions where the Tricon provides automatic primary OR backup protection, the assessment determined that adequate diversity exists outside the PPS to automatically mitigate the associated FSARU Chapter 15 accidents or events given a concurrent CCF that disables the PPS. Three cases were

identified where both primary AND backup protection is provided by the PPS, and manual action was credited in the Eagle 21 safety evaluation to mitigate the associated events given a concurrent CCF that disabled the PPS. Another diverse architecture was needed to automatically perform the protections function for these cases.

The Class IE CS Innovations, LLC Advanced Logic System (ALS) [8] was chosen to perform the diverse automatic protective functions where the existing Eagle 21 safety evaluation credited manual action to mitigate events that occur with a concurrent CCF. The ALS is a logic-based platform, that utilizes a minimal set of hardware to implement a system with high reliability and integrity. The key component in the ALS design is a Field Programmable Gate Array (FPGA) that is a semiconductor device containing programmable logic components and programmable interconnects and that does not use software in the traditional sense when it is in operation. Diversity built into the ALS through a structured development process ensures that CCF considered in the D3 assessment will not affect ALS automatic protection functions. Further, a Tricon CCF cannot affect the ALS and an ALS CCF cannot affect the Tricon.

Obtaining USNRC approval [5] of the D3 assessment for the DCPP PPS replacement design provided PG&E the desired regulatory assurance needed to commit the significant resources required to develop an LAR for the DCPP PPS replacement design. Having an USNRC approved D3 assessment for the proposed PPS replacement design, supported the leadership decision to sign contracts with vendors to complete final design details and to prepare the plant specific documentation specified by ISG-06. The USNRC staff provided comments during the public LAR acceptance meeting that obtaining approval of the D3 assessment prior to the submittal of the LAR was a wise decision by PG&E.

1.3 ISG-06 Tier 2 and Tier 3 Application

ISG-06 provides different approaches that are available for licensees to prepare an LAR when using previously-approved digital platforms. ISG-06 designates three Tiers of USNRC review that have different support documentation requirements. Tier 1 is applicable to license amendments proposing to reference a previously approved topical report within the envelope of the generic approval described in the topical report. A Tier 1 USNRC review relies heavily upon the previous review efforts and documents that are already reviewed and approved by the USNRC staff do not need to be submitted. Tier 2 is applicable to license amendments proposing to reference a previously approved topical report with deviations to suit the plant-specific application. Deviations could include, a revised software development process, new hardware, or deviations from the approved topical report. Tier 3 is applicable to license amendments proposing to use a new digital I&C platform or component(s) with no generic approval. Tier 3 reviews require the largest number of documents to be submitted to support review, including documentation on the platform, software, developmental tools, and developmental methods. For example, ISG-06, Enclosure B, “Information to be Provided in Support of a Digital I&C Upgrade License Amendment Request,” specifies information be submitted in 44 areas for a Tier 3 application compared to 32 areas for a Tier 1 application.

The PG&E PPS replacement LAR consisted of a Tier 2 application for use of the Invensys Operations Management Tricon PLC, Version 10 [9] and a Tier 3 application for use of the CS Innovations, LLC, Advanced Logic System [8]. Invensys Operations Management obtained approval of the Tricon PLC, Version 9 [10], in November 2000 and requested NRC approval of

Version 10 in September 2009 [9]. Since the Tricon, Version 10, was not approved, PG&E submitted the LAR requesting a Tier 2 review based on the approved Tricon, Version 9, and the differences that are included in Tricon, Version 10. This approach significantly reduced the number of ISG-06 specified documents that needed to be submitted with the LAR since the LAR referenced the approved Tricon Version 9 and the Version 10 documents that had already been submitted for review by Invensys Operations Management.

The ALS platform has not been approved by the USNRC for generic use; however CS Innovations submitted a request for USNRC approval of the ALS platform for generic use in August 2010 [8]. Since no version of the ALS platform was generically approved, PG&E submitted a Tier 3 application for use of the CS Innovations ALS platform portion of the PPS replacement. When the DCPP LAR was submitted, CS Innovations had already submitted the majority of the ISG-06 specified information to support the USNRC platform review, which allowed these documents to be referenced in the LAR. The staff provided feedback in a meeting summary to PG&E that if the Tricon, Version 10, and ALS platforms were approved, the USNRC staff could complete the LAR review as a Tier 1 review.

Preparation of the DCPP PPS replacement LAR [2] as a Tier 2 application for use of the Tricon, Version 10 [9], and as Tier 3 application for the ALS [8] required significant effort to ensure that all ISG-06 specified documentation was either submitted by the vendors or prepared to support the PPS replacement. The DCPP PPS replacement LAR [2] was approximately 250 pages and included approximately 750 pages of project specific ISG-06 specified documents. Since the majority of DI&C vendors are now obtaining USNRC generic approval of their DI&C platforms, it is expected the majority of future licensee LARs can be submitted as a Tier 1 review and the effort required to prepare the LAR documentation will be less than that required for the PG&E PPS replacement LAR.

The DCPP PPS replacement LAR itself was prepared as a nonproprietary LAR to facilitate NRC preparation of a safety evaluation that did not include proprietary information. Some information related to cyber security and the secure development and operational environment was security-related information. The security-related information was submitted separately in a letter that was requested to be withheld under 10 CFR 2.390.

1.4 ISG-06 Documentation Preparation

DI&C ISG-06 [1], Enclosures B, "Information to be Provided in Support of a Digital I&C Upgrade License Amendment Request," and Enclosure E, "Proposed Table of Contents for License Amendment Request (LAR)," describe the information and supporting documents specified to be submitted to the USNRC with an LAR for a digital I&C upgrade. To facilitate development of an LAR for the PPS replacement that would meet the significant documentation requirements of DI&C ISG-06, PG&E assembled a dedicated project team of experienced personnel in 2006 (i.e., five years before LAR submittal) with expertise in I&C design, I&C testing, software requirements, software development, cyber security, technical project management, and licensing. PG&E was fortunate to have two I&C design engineers and a technical project manager on the project team who had been involved in the previous Eagle 21 PPS upgrade and had in-depth knowledge of the PPS. Two I&C design, one technical project management, and one licensing individual on the project team spent approximately half of their time associated with the project, and full time during certain periods.

ISG-06 [1], Enclosure B, specifies information to be submitted with the LAR (Phase 0 information) and within one year of requested approval (Phase 2 information). ISG-06, Enclosure B, also specifies information be available for audit within one year of requested approval (Phase 2 information), and available for inspection after approval (Phase 3 information). Preparation of the information required to support the LAR is complicated by the fact that: (1) design aspects need to be finalized to complete documentation; (2) there are interdependencies between different documents; and (3) documents are needed at the vendor platform level, the plant specific design level, and at the plant level.

Early on in the PPS replacement project, it was determined that efficient communication and project management would be required to prepare the ISG-06 specified documents on schedule. Approximately four project team meetings were held each year with participation by vendor personnel. An Excel spreadsheet matrix was used as a tool to schedule, identify interdependencies, identify required inputs, and to track completion of each of the areas of information specified by ISG-06, Enclosure B. The matrix was provided to the staff during later USNRC Phase 0 meetings and was also included as an attachment to the LAR. The USNRC staff utilized the matrix to perform the acceptance review of the LAR.

1.5 Summary

PG&E submitted the pilot application LAR [2] for use of DI&C ISG-06 [1] for a DI&C PPS replacement design based on the Invensys Operations Management Tricon PLC, Version 10 [9] and the CS Innovations ALS [8] FPGA-based platforms in October 2011 and the LAR was accepted [3] by the USNRC staff for review in January 2012. The diversity, communications, maintenance terminal, Class I/II isolation, software, and security aspects of the design were important topics discussed during the pre-application meetings. The PG&E approach to obtain licensing certainty was to design the PPS replacement as simple as possible, to not utilize cross-channel communications, voting, or two-way communications in the safety-related portions of the design, and to avoid any deviations or exceptions to applicable requirements.

The D3 assessment was utilized as an optimization tool early in the design and was submitted [4] and approved [5] by the USNRC staff prior to submittal of the PPS replacement LAR. A dedicated project team with expertise in the each of the areas involved in the design was created early in the development phase. Tools were used to plan and manage the development of the information specified by ISG-06.

2 CONCLUSIONS

PG&E found USNRC DI&C ISG-06 to be an excellent document to prepare the LAR for DCPP PPS replacement. USNRC staff feedback provided on the diversity, communications, maintenance terminal, Class I/II isolation, software, and security aspects of the design permitted PG&E to proactively address areas of staff concern and to finalize design aspects where licensing uncertainty existed. PG&E found that it was important during the Phase 0 meetings to identify to the staff, during the meeting, the items expected for staff feedback.

The performance of the D3 assessment early on in the design for the DCPP PPS replacement design allowed optimization and verification of the preliminary design early in the design process. Obtaining early NRC approval of the D3 assessment was critical to obtain the desired

regulatory assurance needed to commit the significant resources required to develop an LAR for the DCPP PPS replacement design. PG&E received positive USNRC staff feedback for the D3 approach.

The DCPP PPS replacement LAR, prepared as a Tier 2 application for use of the Tricon, Version 10, and as a Tier 3 application for the ALS, required significant effort. A tool was used to ensure that all ISG-06 specified documentation was either submitted by the vendors or prepared to support the PPS replacement. The DCPP PPS replacement LAR was approximately 250 pages and included approximately 750 pages of project specific ISG-06 specified documents. It is expected the majority of future licensee LARs can be submitted as a Tier 1 review and that the effort required to prepare the LAR documentation will be less than for the PG&E PPS replacement LAR.

3 REFERENCES

1. USNRC DI&C-ISG-06, Task Working Group #6: Licensing Process, Revision 1, January 19, 2011.
2. PG&E Letter DCL-11-104, James R. Becker (PG&E) to USNRC, "License Amendment Request 11-07, Process Protection System Replacement," October 26, 2011 (ADAMS Accession No. ML113070457).
3. USNRC, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 – Acceptance Review for License Amendment Request for Digital Process Protection System Replacement," January 13, 2012 (ADAMS Accession No. ML120120005).
4. PG&E Letter DCL-10-030, James R. Becker (PG&E) to USNRC, "Review of Diablo Canyon Power Plant Topical Report, Process Protection System Replacement Diversity and Defense-in-Depth Assessment," April 9, 2010 (ADAMS Accession Number ML101100646).
5. U.S. Nuclear Regulatory Commission, Letter "Diablo Canyon Power Plant, Unit Nos. 1 and 2 - Safety Evaluation for Topical Report, "Process Protection System Replacement Diversity & Defense-In-Depth Assessment" (TAC Nos. ME4094 and ME4095)," April 19, 2011 (ADAMS Accession No. ML110480845).
6. USNRC Letter, J. E. Dyer (NRC) to James R. Becker (PG&E) (October 14, 2009).
7. USNRC Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Rev. 5 (March, 2007).
8. CS Innovations Document No. 6002-00301-NP, Revision 1, "ALS Topical Report and Supporting Documents Submittal," August 11, 2010 (ADAMS Accession No. ML102570797).
9. Invensys Letter No. NRC-V10-09-01, J. Polcyn (Invensys) to NRC, "Nuclear Safety-Related Qualification of the Tricon TMR Programmable Logic Controller (PLC) – Update to Qualification Summary Report Submittal" (September 9, 2009).
10. EPRI TR-1003114, Letter from Stuart A. Richards (NRC) to Troy Martel (Triconex Corporation), "Review of Triconex Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 to Qualification Summary Report," Revision 1" (December, 2001).