As seen in the February 2015 issue of **Nuclear News**

Diablo Canyon Digital I&C ISG-06 pilot application: Lessons learned

By Kenneth J. Schrader, John W. Hefler, and Edward L. "Ted" Quinn

The review of Diablo Canyon's license amendment request for a digital I&C modification has provided valuable lessons for future applications of ISG-06.

Pacific Gas and Electric Company (PG&E) has developed the industry pilot application for the use of the Nuclear Regulatory Commission's Interim Staff Guidance document Digital Instrumentation and Controls (DI&C) ISG-06, Revision 1, *Licensing Process*. The application requests that PG&E be allowed to replace the Diablo Canyon nuclear power plant's existing Eagle 21 digital process protection system (PPS) with a state-of-the-art digital system. The ISG, issued for use on January 19, 2011, describes the licensing process the NRC staff may use to review a license amendment request (LAR) for a digital I&C modification. DI&C-ISG-06 was developed through a joint industry working group that was coordinated by the Nuclear Energy Institute and in which PG&E was a participant.

The LAR for the replacement of the Eagle 21 PPS has been under active NRC staff review since it was submitted to the NRC on October 26, 2011; final approval is expected in late 2015. Diablo Canyon's PPS replacement design and the NRC staff's review process were reviewed by the NRC Advisory Committee on Reactor Safeguards during meetings held in February and March 2014. The installation date of the PPS replacement design will be based on the plant's outage prioritization process. During the design and application process, PG&E has learned many lessons that will prove useful in future applications of safety-related digital I&C technology in plant safety systems.

Photo: PG&E

PG&E's Diablo Canyon plant, located at Avila Beach, Calif.

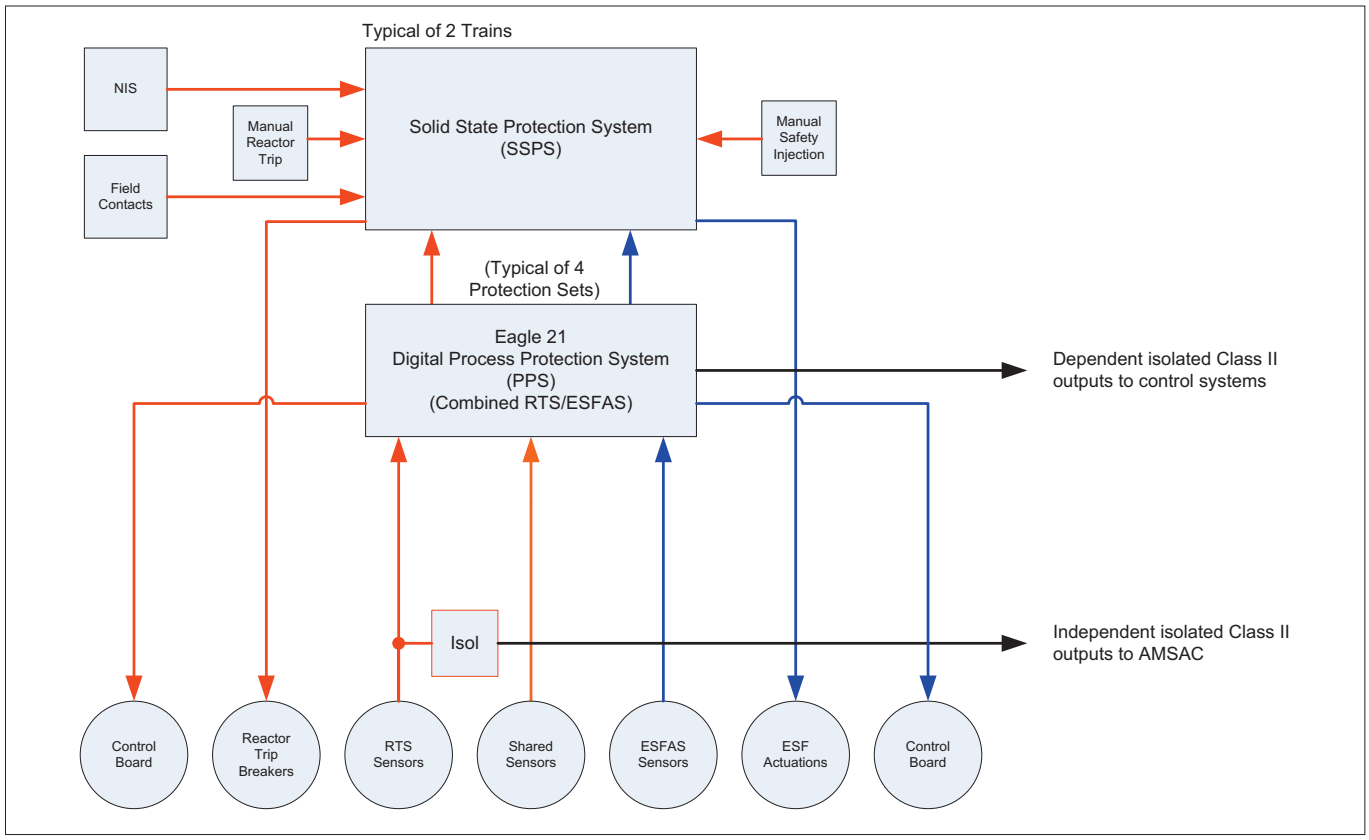
Protection system changes

The existing digital Westinghouse Eagle 21 PPS, which provides the processing portion of the protection system at Diablo Canyon, is being replaced to address obsolescence and maintenance issues. The system was installed in 1994 to replace the original analog Westinghouse 7100 PPS.

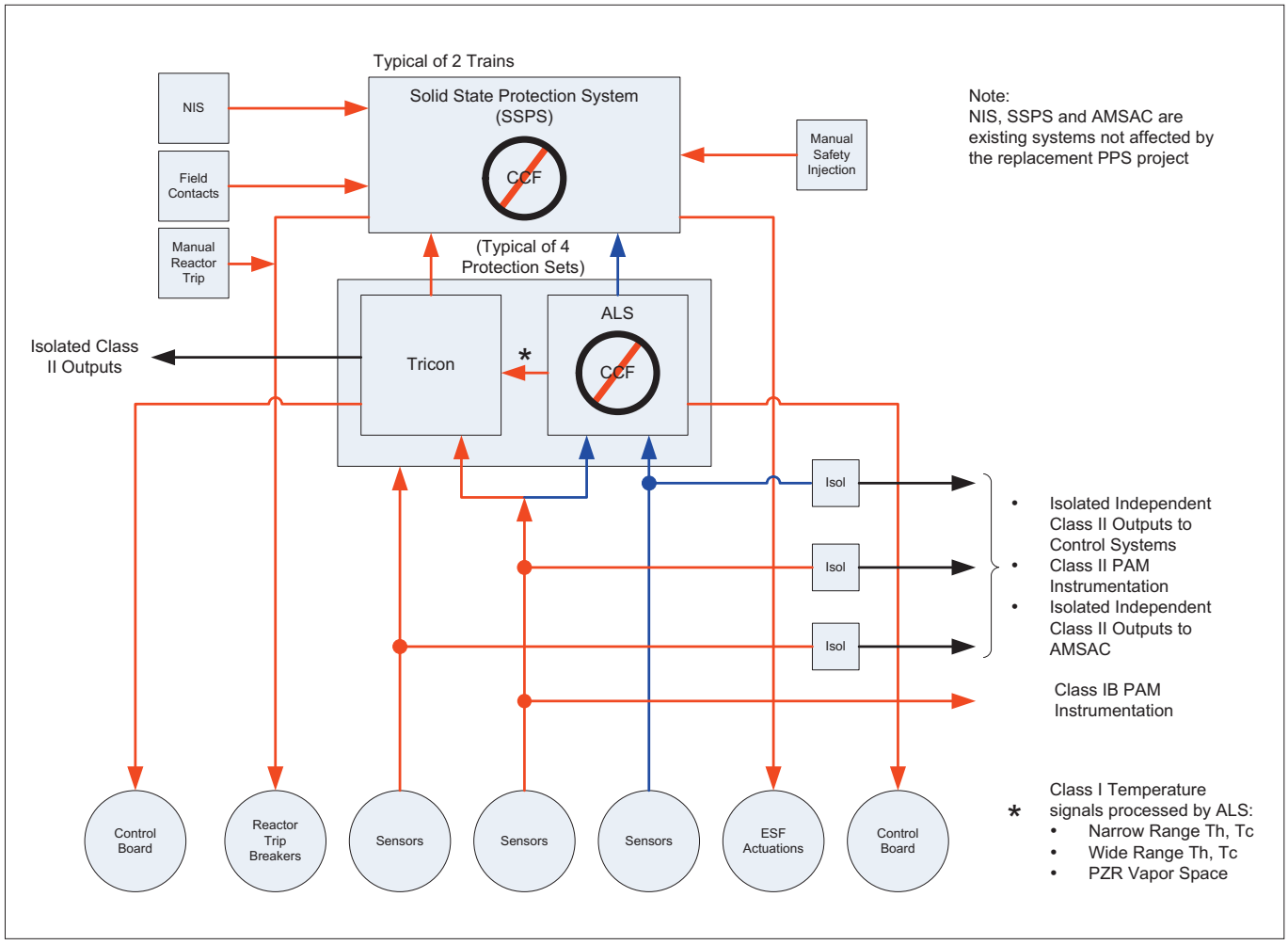
The digital PPS replacement proposed in the LAR is based on the Invensys Triconex Tricon processor and the Westinghouse Advanced Logic System (ALS). The Tricon processor is a software programmable logic controller–based processor that employs a triple-redundant architecture to facilitate high reliability. The ALS is a field-programmable gate array semiconductor device–based architecture that contains programmable logic components and programmable interconnects and that does not use software in the traditional sense when the ALS is in operation. The ALS design contains internal redundancy and diversity to eliminate the potential for a software common-cause failure (CCF) to adversely affect the PPS safety function.

The digital PPS proposed by PG&E maintains the current Westinghouse four-channel, two-train protection system architecture without affecting existing diverse systems—the nuclear instrumentation sys-

Kenneth Schrader (<kjse@pge.com>) is a Principal Engineer for Pacific Gas and Electric Company and is Vice Chairman of the Pressurized Water Reactor Owners Group. John Hefler (<john.hefler@altran.com>) is a Principal Engineer for Altran. Ted Quinn (<tedquinn@cox.net>) is President of Technology Resources and is a past president of ANS (1998–1999).



The old Eagle 21 digital process protection system (PPS) architecture



The new PPS architecture, based on the Invensys Triconex Tricon processor and the Westinghouse Advanced Logic System

tem and anticipated transient without scram mitigation system. The use of both the Tricon and ALS systems as part of the PPS architecture precludes the need to incorporate a diverse actuation system (DAS)—typically required in prior NRC-approved software-based protection system designs—into the PPS design.

Factory acceptance testing of the Tricon portion of the PPS design was successfully completed in December 2014, and testing of the ALS portion is scheduled for May 2015.

Design approach

To reduce licensing uncertainty for the project, PG&E instituted a design approach to develop a PPS replacement that was as simple as possible and would eliminate the need for any required manual operator actions in the unlikely event that a software CCF in the PPS should occur. State-of-the-art digital I&C platforms contain numerous functions and features that are not needed for all applications and are typically like building blocks, capable of being combined and configured in multiple ways. Creating a simple digital protection system design requires considerable control and focus during the early development phases to ensure that only the required functions, features, and configurations are implemented.

The two most significant areas of focus for the Diablo Canyon PPS design were diversity and communications. By employing both the Tricon and ALS digital I&C platforms in the PPS replacement design, internal diversity is provided to mitigate the effects of a postulated software CCF. The design of a protection system that can still automatically perform the safety function in the event of a software CCF provides the significant benefit of scope reduction in other areas of the design. Benefits include the elimination of the need to perform best-estimate accident analyses, to justify and implement manual operator actions to address software CCF, and to include a DAS in the design, as well as the simplification of the diversity and defense-in-depth (D3) assessment. Avoiding the need for a DAS is an important goal, since its addition complicates the protection system, increases the possibility of an inadvertent actuation of the protection system, and is one more system to be operated, tested, and maintained.

To simplify communications, the PPS replacement design was developed with four separate and independent channels so that there is no communication between the redundant channels (that is, no cross-channel communication). Cross-channel communication is not required for coincidence logic—or "voting"—because the voting function is performed in the existing nonsoftware-based solid-state protection system. The design does not employ two-way communications to perform any safety-related function. This design was based on the NRC staff's providing feedback to PG&E that it would simplify the review process.

Another goal was to reduce licensing uncertainty by ensuring that the PPS replacement design met all applicable NRC requirements and current guidance. While this requires diligence during the design process, it reduces the risk that the licensing process might be extended by staff requests for additional information regarding exceptions or deviations from current requirements and guidance.

Pre-application NRC meetings

DI&C-ISG-06 allows the use of the public meeting process for licensees to engage the NRC in a pre-application discussion of how a proposed digital I&C safety system upgrade LAR will address issues such as significant variances from current guidance and other unique or complex topics associated with a proposed design, such as interdivisional digital communications, nonsafety-related equipment, diversity, redundancy, D3 assessment, manual operator actions, best-estimate analyses, software development, and deviations from NRC staff positions. These pre-application meetings, designated as "Phase 0" in DI&C-ISG-06, are intended to be two-way discussions in which the NRC can provide feedback on critical aspects of the proposed design that are likely to affect the staff's evaluation. The NRC staff issues meeting summaries that capture the topics discussed in the meeting and provide a preliminary staff assessment of the unique and complex topics.

PG&E found the Phase 0 public meetings to be instrumental in obtaining initial feedback as to whether the proposed PPS replacement design met NRC guidance and whether the draft LAR contents met NRC staff acceptance review requirements. The topics discussed during the four meetings included design redundancy, design diversity, D3 assessment, communications, software development, and system connections to the nonsafety maintenance computer and plant process computer.

Feedback provided by the NRC staff on the diversity, communications, maintenance computer, isolation between Class 1 and Class 2 circuits, software, and security aspects of the design permitted PG&E to proactively address areas of staff concern and to finalize design issues where licensing uncertainty existed. PG&E found that it was important to specifically identify for the NRC staff, during the Phase 0 meetings, the items on which staff feedback was to be included in the staff-written meeting summaries.

D3 assessment

Defense-in-depth involves providing overlapping protective barriers or means to compensate for weaknesses in the defensive barriers. For nuclear plant digital I&C systems, defense-in-depth is achieved through four echelons of defense—the control system, the reactor trip system, the engineered safety features actuation system, and the monitoring and indication system—such that a failure in one of the echelons does not adversely affect the ability of the other echelons to perform their safety functions. For digital I&C, diversity is the principle of using different technologies, equipment, vendors, logic, algorithms, and development teams to perform safety functions. For nuclear plant digital I&C systems, a CCF in software, although beyond design basis, needs to be considered, and a D3 assessment in accordance with NRC Branch Technical Position (BTP) 7-19 needs to be performed as part of the licensing of a digital-based safety-related system.

Because the Diablo Canyon PPS replacement design contained two platforms not previously approved by the NRC for a large-scale protection system, PG&E concluded that obtaining the NRC's approval of the D3 assessment prior to submittal of the LAR provided the most certainty that the initial design would ultimately be approved without the need for significant modifications in the future to secure licensing approval. PG&E developed a PPS Replacement D3 Assessment Topical Report that was submitted to the NRC in 2010 and was approved in 2011, prior to the submittal of the LAR. While a D3 assessment is normally performed after a protection system design is developed, PG&E instead used the assessment to evaluate and optimize the initial PPS replacement design prior to its submittal to the NRC for approval.

To perform the D3 assessment, PG&E reviewed the *Diablo Canyon Final Safety Analysis Report Update* (FSARU) Chapter 6 and 15 licensing basis accident analyses and the NRC's Safety Evaluation Report for the current Eagle 21 protection system to determine the events that required the PPS for primary or backup protection. The assessment, which was performed in accordance with BTP 7-19, considered a PPS software CCF concurrent with each Chapter 6 and 15 event and accident for which a mitigating action by the PPS was credited in the accident 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 accidents/events, given a concurrent CCF that disables the PPS.

Three cases were identified where both primary and backup protection are provid-

ed by the PPS, and manual operator action was being credited to mitigate the associated events given a concurrent CCF that disabled the PPS. The Class 1E Westinghouse ALS platform was chosen to perform the diverse automatic protective functions in these cases where the existing design analyses credited manual action to mitigate events that occur with a concurrent CCF.

ISG-06 application tiers

ISG-06 provides various approaches to licensees for use in the preparation of an LAR when using previously approved digital platforms, and it designates three tiers of NRC review that have different support documentation requirements, as follows:

- *Tier 1* is applicable to LARs within the envelope of the generic approval of a previously approved topical report. A Tier 1 NRC review relies heavily upon the previous review efforts and documents that have already been reviewed and approved by the NRC. Licensees that submit an ISG-06 Tier 1 application obtain substantial benefits, including high licensing certainty, a large reduction in material to be submitted, and resources to prepare the application.
- *Tier 2* is applicable to LARs referencing a previously approved topical report with deviations, which could include a revised software development process, new hardware, or deviations from the approved topical report.
- *Tier 3* is applicable to LARs proposing to use a new digital I&C platform or component(s) with no generic approval. Tier 3 reviews require the submission of the greatest number of documents to support the review, including documentation on the platform, software, developmental tools, and developmental methods.

PG&E's PPS replacement LAR originally consisted of a Tier 2 application for the use of the Tricon Version 10 system and a Tier 3 application for the use of the ALS. Both platforms were subsequently approved by the NRC staff, allowing for the completion of the LAR review as a Tier 1 review and significantly simplifying the NRC safety evaluation.

Preparation of the LAR as a Tier 2 application for the use of the Tricon Version 10 system and a Tier 3 application for the ALS required diligence to ensure that all ISG-06–specified documentation was either submitted by the vendors or prepared to support the PPS replacement. Since the vendors had submitted many of the required documents to the NRC, the LAR referenced the submitted vendor documentation in many cases and was approximately 250 pages, substantially smaller than prior digital I&C protection system LARs. Since the majority of digital I&C vendors are now obtaining NRC generic approval of their platforms, it is expected that the majority of future licensee LARs can be submitted as Tier 1 reviews, significantly reducing the effort required to prepare the LAR documentation compared to that required for PG&E's LAR.

The LAR itself was prepared as a nonproprietary LAR to facilitate the NRC's preparation of a safety evaluation that did not include proprietary vendor information. Certain security-related information (concerning cybersecurity and the secure development and operational environment) was submitted separately in a letter requesting that it be withheld under 10 CFR 2.390.

ISG-06 documentation prep

DI&C-ISG-06, Enclosure B and Enclosure E, describe the information and supporting documents that must be submitted to the NRC with an LAR (Phase 1 information) and that must be submitted within one year of requested approval (Phase 2 information). It was realized that efficient communication and project management would be required to prepare the ISG-06–specified documents on schedule. Multiple project team meetings with vendor personnel were held each year, and a spreadsheet matrix was used as a tool for scheduling, for identifying document interdependencies and required inputs, and for tracking the completion of each of the areas of information specified by ISG-06. The matrix was pro-

vided to the staff during later NRC Phase 0 meetings and was also included as an attachment to the LAR. The NRC staff utilized the matrix extensively during the review of the LAR.

PG&E submitted most of the required Phase 2 documentation within a year of the LAR submittal. Some of the documents, however (on setpoints, reliability analysis, and failure modes and effects analysis), required two years to prepare, and some (on independent verification, test plans, and factory acceptance testing) required three years. The primary cause for the delays in generating the Phase 2 documents was the additional vendor effort required for first-of-its-kind engineering to complete the documents and the resolution of issues and changes to the Functional Requirements Specification (FRS). The resolution of NRC requests for additional information during the LAR review was performed efficiently using an "open items" table during periodic public phone calls.

Detailed design, verification

The originally proposed PPS design employed a shared non-safety-related maintenance computer for the Tricon and ALS subsystems that is connected to the PPS during normal operations in each of the four protection channels (a total of four maintenance computers). This design feature received focused NRC attention during the Phase 0 meetings and LAR review. The use of a separate maintenance computer for each protection channel eliminated issues related to the use of a multidivisional maintenance computer. During the LAR review, the staff requested information on how the proper operation of the vendor software would be verified following software updates on the maintenance computer. In order to eliminate complex and time-consuming test procedures that would be required to support vendor software updates on a shared maintenance computer, PG&E implemented a minor design change, using a separate non-safety-related maintenance computer for each of the Tricon and ALS subsystems in each of the four protection channels (a total of eight maintenance computers). This has been the only design change resulting from the NRC review.

PG&E issued a single FRS for the project covering both the Tricon and ALS platforms that did not specify which vendor was responsible for each individual specification. Instead, vendor responsibility was included in the contracts for each vendor, which (1) resulted in unnecessary difficulty for each vendor to develop a detailed design; and (2) contributed to each of the vendors' not meeting all applicable requirements during the initial detailed design and having to submit deviation requests for approval. This complicated the NRC's review and resulted in the identification of NRC audit issues for each vendor. In addition, during PG&E's review of the initial detailed design, it was determined that the vendors did not fully understand the meaning of some of the functional requirements. The changes required to address all applicable functional requirements for each vendor resulted in redesign, resubmittal of revised vendor documentation, and an extension of the detailed design schedule. This situation demonstrated the importance of utilities' proactively ensuring that vendor design and verification personnel have a clear understanding of all functional requirements.

The FRS document did not include functionality to support troubleshooting and maintenance expected by I&C maintenance personnel until well into the detailed design phase. As a result, FRS revisions were required during the detailed design phase. The vendors then had to perform a redesign to meet the new functional requirements that were added to support maintenance activities.

The schedule time for each of the vendors to complete the detailed design and independent verification and validation (IV&V) activities required an additional one and a half to two years from the originally planned time. The vendors encountered unexpected issues during the detailed design that are typical in first-of-its-kind digital I&C applications. Issues that had to be resolved included those related to equipment qualification, core memory limitations, circuit board overheating, excessive signal noise, and inaccuracy exceeding specifications. These issues are not expected to arise in the next application of the Tricon and ALS platforms.

ISG-06 experience

PG&E found the NRC's DI&C-ISG-06 to be an excellent process to follow in preparing the LAR for the Diablo Canyon PPS replacement project. NRC staff feedback that was provided on the diversity, communication, maintenance terminal, isolation between Class 1 and Class 2 circuits, 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.

The issues that arose during the detailed design and IV&V phase of the project, related to the FRS document and the first-of-its-kind application for each vendor, were not related to the ISG-06 process and are not expected to occur for the next application of the Tricon and ALS platforms, or for utilities that apply the lessons learned during PG&E's PPS replacement project.

The ISG-06 process is a significant improvement over that for licensing a current digital I&C system, and its use will be a key component in improving safety in nuclear power plants. NN