UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

September 22, 2016

Mr. Victor M. McCree
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: PACIFIC GAS AND ELECTRIC DIABLO CANYON UNITS 1 AND 2 DIGITAL PROCESS PROTECTION SYSTEM UPGRADE LICENSE AMENDMENT REQUEST

Dear Mr. McCree:

During the 636th meeting of the Advisory Committee on Reactor Safeguards, September 8-10, 2016, we reviewed the Pacific Gas and Electric Company (PG&E) Diablo Canyon Power Plant (Diablo Canyon) Units 1 and 2 digital process protection system (PPS) replacement license amendment request (LAR) and the associated draft safety evaluation report (SER). Our Digital Instrumentation and Control Systems Subcommittee also reviewed this matter during meetings on February 18, 2014 and April 4, 2016. During these reviews, we had the benefit of discussions with the NRC staff and PG&E. We also had the benefit of the referenced documents.

RECOMMENDATION

The Diablo Canyon Units 1 and 2 digital process protection system replacement license amendment request should be approved.

BACKGROUND

The proposed LAR would provide a digital replacement of the existing digital PPS. The PPS monitors process variables and provides process protection functions for the reactor protection system (RPS).

The staff reviewed the proposed PPS replacement design against the relevant parts of the *Code of Federal Regulations* (CFR), General Design Criteria (GDC), regulatory guides, interim staff guides, and IEEE Standard 603-1991 including the correction sheet, dated January 30, 1995. Because the construction permits were issued in 1968 for Unit 1 and in 1970 for Unit 2, the Diablo Canyon licensing basis is the 1967 version of the GDC. This license amendment was evaluated against the current relevant GDCs in the 2015 version of the CFR. The NRC staff also compared each licensing basis GDC with current versions of the associated GDC to ensure compliance with the Diablo Canyon licensing basis is maintained.

Discussion

The proposed amendment would allow replacement of the existing Diablo Canyon Eagle 21 digital PPS with a new digital PPS, which is based on the Invensys Operations Management Tricon Programmable Logic Controller, Version 10, and the Westinghouse Electric Company field programmable gate array (FPGA)-based Advanced Logic System (ALS). The current Eagle 21 PPS was approved by the NRC in 1993. The Diablo Canyon Eagle 21 PPS system is being replaced to address obsolescence, diagnostic, maintenance, and reliability concerns.

The new digital PPS performs functions in support of the RPS comprised of the reactor trip system (RTS) and engineered safety features actuation system (ESFAS). The PPS provides signal processing (from existing input sensors), signal validation, and protection trip logic functions in support of these systems. Actuation signals from the digital PPS are input to the existing solid state protection system (SSPS) which performs the coincidence logic function for the RTS and ESFAS. The replacement system provides online self-testing and diagnostic functions to improve the availability of the system and to improve system maintainability. All functions currently performed by the Eagle 21 PPS will be maintained in the replacement digital PPS. The actuation signals to the SSPS voters are hardwired connections. They do not use any communications technology or digital technology.

The SSPS is composed of two redundant, essentially identical trains (A and B). These trains are physically and electrically separated. In addition to signals from PPS, SSPS also receives inputs from the nuclear instrument system and seismic instrumentation. The SSPS logic provides automatic reactor trip signals to the reactor trip switchgear. The SSPS also operates relay logic to actuate the engineered safety features. Manual reactor trip and ESFAS actuations are available from the main control board.

The existing SSPS, RTS, ESFAS, nuclear instrument system, anticipated transient without scram mitigation system actuation circuitry (AMSAC), and reactor trip switchgear that interface with the PPS replacement system are not being modified by this LAR.

The PPS replacement system consists of four redundant protection sets A, B, C, and D that will be installed into 16 racks in which the current Eagle 21 system is located.

Each of these protection sets is composed of a Tricon subsystem component and an ALS subsystem component. Each of the PPS system functions is assigned to one of these two PPS subsystems within each protection set. The allocation of functions to these subsystems was performed based on the results of the diversity and defense-in-depth (D3) analysis as follows:

- If diverse and independent automatic functions were available to mitigate the effects of a postulated common-cause failure concurrent with the Updated Final Safety Analysis Report, Chapter 15, “Accident Analyses” events, then the function was assigned to the software-based Tricon subsystem.

- Otherwise, the function was assigned to the ALS subsystem, which contains design features to establish built-in diversity.

Any existing plant digital replacement or new plant digital reactor trip and engineered safeguards systems must meet the fundamentals of reliable digital and software-based safety system instrumentation and control design: redundancy, independence, deterministic software cycle processing, diversity and defense-in-depth, and control of both external and internal access. The staff evaluated the Diablo Canyon LAR against these fundamentals as follows.

Redundancy

The replacement PPS design maintains the four division redundancy for the RTS and ESFAS functions.

Independence

There are no interdivisional communications being implemented in this design. Within each division, the Tricon and ALS platforms have their own dedicated maintenance workstations. Connections from the maintenance work stations to the platforms are manually accomplished. The Tricon connection method uses a key switch which sets the Tricon operating modes between RUN, PROGRAM, STOP, and REMOTE. The key switch is a physical interlock that prevents Tricon bidirectional operation when the switch is in RUN and function out of service switches are off. For ALS, the receive connection from the maintenance workstation is physically disconnected. Its connection is controlled through administrative procedures. In addition, within each division, the Tricon and ALS platform systems do not use any software-based communication with each other. Trip signals from each subsystem (hardwired, discrete, non-software based signals) are sent independently to the SSPS for voting. Thus, possible software corruption and simultaneous lockup of all SSPS voting functions is eliminated.

Deterministic Software Cycle Processing

Tricon is a software-based computer platform. It uses a custom system executive to run the processor card and host the safety application, in this case the PPS application. A system executive is an operating system used to cyclically run a predetermined list of tasks. Tricon has three prioritized tasks controlled by three prioritized interrupts. There are no event-driven interrupts in this system. The scan structure guarantees that the Tricon scan cycle is predictable and repeatable from one scan to the next. The background task always runs, but it is the lowest priority task. Periodically, the communication interrupt is asserted to execute communication tasks.

The communication task is a higher priority and it runs for a fixed amount of time, then the background task is allowed to run again. The background and communication tasks cycle back and forth like this until it is time to start the next scan.

The start scan interrupt is asserted to start the next scan cycle. The scan task is the highest priority task and can only be interrupted by the watchdog timer, and it contains all of the functions that are critical to the safety application. In order, it resets the watchdog timer, reads fresh inputs, runs the algorithm, and writes the outputs, then determines when to start the next scan cycle. That is the end of the scan's task.

Thus, the scan time is a fixed value determined during system development to meet the particular system application time response requirements and is executed on a fixed timing cycle developed during the system application design. It overrides the background and communications process interrupts to ensure fixed cycle processing of all safety functions. A single failure would occur if the scan interrupt in one division fails to execute and run its scan cycle. This would not compromise the remaining independent divisions. Thus, even though the Tricon cycle processing is interrupt driven, it can be considered to be deterministic.

The ALS platform is an FPGA-based design (non-software based operating system). It does not embed microprocessor cores or use interrupts. The application of the ALS platform operates on fixed cycles where a deterministic sequence of 1) acquire inputs, 2) perform logic operations, such as compare processed variables against a trip set point, and 3) generate output signals, is followed without the use of a microprocessor core or interrupts.

Diversity and Defense-in-Depth

D3 is accomplished through the use of a software-based Tricon platform and an independent FPGA-based ALS platform within each protection set.

Within each protection set, the Tricon subsystem has three layers of redundancy from input terminal to output terminal called triple mode redundancy (TMR). The TMR architecture allows continued system operation in the presence of any single point of failure within the system. The TMR architecture also allows Tricon to detect and correct individual faults during system operation, without interruption of monitoring, control, or protection capabilities. However, the TMR architecture remains vulnerable to malfunctions of the common application software for each processor.

The diverse ALS portion of the PPS replacement system uses FPGA hardware logic technology. The ALS uses two diverse sets of logic cores programmed by two independent design teams to achieve enhanced diversity. The ALS has two design attributes intended to mitigate the likelihood of common cause programming failures as sources that could disable a safety function: core diversity and embedded design diversity. Core diversity generates two redundant logic implementations within each FPGA for each standardized circuit board. The redundant logic implementations use the same hardware descriptive language files per standardized circuit board. Embedded design diversity results in two versions of hardware descriptive language files for each standardized circuit board.

The D3 assessment topical report describes the allocation of reactor trip and ESFAS actuation signals between the Tricon and ALS platforms. The allocation removes several sources of potential common cause failures that are present in the current Eagle 21 system design. During our review of the D3 assessment, we noted that three particular ESFAS functions are allocated as follows:

- Signals to actuate auxiliary feedwater flow are developed only in the Tricon platform. The existing AMSAC logic provides a diverse backup to those signals for events that occur when reactor power is above 40%. The AMSAC logic is not affected by the PPS upgrade.

- Signals to close the main steam isolation valves (MSIVs) after a steam line break outside the containment are developed only in the Tricon platform. If a common cause failure disables those signals, operator actions are needed to close the MSIVs manually from the main control room. The same actions apply for the current Eagle 21 system design, and they are addressed by the existing Diablo Canyon licensing basis.

- Signals to actuate safety injection and containment isolation functions after a loss of coolant accident are developed only in the ALS platform. As noted above, the ALS design provides internal core signal processing diversity for those functions.

The PPS upgrade also retains all existing manual backup capabilities for reactor shutdown and safeguards actuation. Based on these considerations, we conclude that the upgraded design provides adequate diversity for all reactor protection and ESFAS functions.

Control of Access

There are no communications between division protection sets. There are no software-based communications between the Tricon and ALS platforms within each division protection set. Bidirectional communication from the Tricon and ALS platforms with their respective maintenance workstations is physically disabled during in-service operations and must be physically enabled by operators.

The Tricon connection method uses a key switch which sets the Tricon operating modes between RUN, PROGRAM, STOP, and REMOTE. The key switch is a physical interlock that prevents Tricon bidirectional operation when the switch is in RUN and function out of service switches are off. Bidirectional communication can occur when the Tricon key switch is in the PROGRAM or REMOTE position. An alarm will be annunciated in the main control room whenever the key switch is not in the RUN position. Online testing and maintenance can be performed on selected functions without removing the entire Tricon PPS from service, while the key switch is in the RUN position. Manual out-of-service switches independent of the PPS instrumentation will be provided to perform these actions. The out-of-service switch only removes the selected function from service and no other function will be affected. In addition, an alarm will be annunciated in the main control room when a function is taken out-of-service. For ALS, the receive connection from the maintenance workstation is physically disconnected. Its connection is controlled through administrative procedures. Thus, Tricon and ALS maintain adequate internal plant control of access.

Tricon communication of protection set data to the external plant computer system is accomplished through a set of internal division operational amplifiers that prohibit the reverse flow of data from the plant computer system. ALS communication to the external plant computer system is accomplished with devices that have their receive capability physically disabled by hardware. Therefore, unidirectional hardware-based communications prevent external plant electronic access to the PPS.

Based on these considerations, there is reasonable assurance that the health and safety of the public will not be endangered by operation of the Diablo Canyon replacement PPS in the proposed manner.

We recommend that the PG&E Diablo Canyon Units 1 and 2 digital PPS replacement LAR be approved.

Sincerely,

/RA/

Dennis Bley
Chairman

REFERENCES

1. Pacific Gas and Electric Company, "License Amendment Request 11-07 Process Protection System Replacement, October 26, 2011 (ML113070457).

2. U.S. Nuclear Regulatory Commission, "Safety Evaluation of Pacific Gas and Electric License Amendment Request for Digital Plant Protection System Replacement at Diablo Canyon Power Plant," March 23, 2016 (ML16054A212) Proprietary.

3. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," June 27, 1991.

4. Pacific Gas and Electric Company, Topical Report, "Process Protection System Replacement Diversity& Defense-in-Depth Assessment," Revision 1, August 2010 (ML102580725).

5. Westinghouse Electric Company, Topical Report, "Advanced Logic System Topical Report," Revision 4, September 2013 (ML13298A094).

6. U.S. Nuclear Regulatory Commission, NUREG-0800, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 6, July 2012 (ML110550791).

7. Invenysis, Topical Report, "Nuclear Qualification of V10 Tricon Triple Modular Redundant (TMR) PLC System," Revision 4, May 15, 2012 (ML12146A010).

8. U.S. Nuclear Regulatory Commission, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 for Topical Report, 'Process Protection System Replacement Diversity and Defense-in-Depth Assessment'," April 19, 2011 (ML110480845).

Based on these considerations, there is reasonable assurance that the health and safety of the public will not be endangered by operation of the Diablo Canyon replacement PPS in the proposed manner.

We recommend that the PG&E Diablo Canyon Units 1 and 2 digital PPS replacement LAR be approved.

Sincerely,
/RA/
Dennis Bley
Chairman

REFERENCES

1. Pacific Gas and Electric Company, "License Amendment Request 11-07 Process Protection System Replacement, October 26, 2011 (ML113070457).

2. U.S. Nuclear Regulatory Commission, "Safety Evaluation of Pacific Gas and Electric License Amendment Request for Digital Plant Protection System Replacement at Diablo Canyon Power Plant," March 23, 2016 (ML16054A212) Proprietary.

3. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," June 27, 1991.

4. Pacific Gas and Electric Company, Topical Report, "Process Protection System Replacement Diversity& Defense-in-Depth Assessment," Revision 1, August 2010 (ML102580725).

5. Westinghouse Electric Company, Topical Report, "Advanced Logic System Topical Report," Revision 4, September 2013 (ML13298A094).

6. U.S. Nuclear Regulatory Commission, NUREG-0800, Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 6, July 2012 (ML110550791).

7. Invenysis, Topical Report, "Nuclear Qualification of V10 Tricon Triple Modular Redundant (TMR) PLC System," Revision 4, May 15, 2012 (ML12146A010).

8. U.S. Nuclear Regulatory Commission, "Diablo Canyon Power Plant, Unit Nos. 1 and 2 for Topical Report, 'Process Protection System Replacement Diversity and Defense-in-Depth Assessment'," April 19, 2011 (ML110480845).

Accession No: **Publicly Available** Y **Sensitive** N
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	MLBanks	ADVeil	ADV for DCB
DATE	09/22/16	09/22/16	09/22/16	09/22/16	09/22/16

OFFICIAL RECORD COPY