Diablo Canyon Power Plant
Digital Process Protection System Replacement
Diversity and Defense-in-Depth

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, Ste 1120
San Francisco, CA 94104
john.hefler@altran.com

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

ABSTRACT

Diablo Canyon Power Plant (DCPP) is replacing the existing digital Westinghouse Eagle 21 Process Protection System (PPS) to address maintenance and obsolescence issues. Eagle 21 was installed in 1994 to replace the original analog Westinghouse 7100 PPS. The License Amendment for replacement of the Eagle 21 PPS was submitted to NRC on October 26, 2011. Key to submittal of the PPS replacement LAR was resolution of the need for Diversity and Defense-in-Depth (D3) in the replacement design to mitigate the potential for a common design error to disable redundant channels of the protection systems through common-cause failure (CCF).

The D3 evaluation reviewed the Diablo Canyon Final Safety Analysis Report Update (FSARU) to determine the events that required the PPS for primary or backup protection to identify available automatic means to prevent PPS software CCF from adversely affecting the mitigation of FSARU Chapter 15 accidents or events. PG&E developed a replacement PPS design based on DI&C ISG-02 diversity guidance that is Class 1E, nuclear safety-related and that automatically performs all the protection functions credited in the FSARU with automatic operation. Further, the replacement PPS provides safety-related automatic mitigation functions for the events where the Eagle 21 Safety Analysis credited manual operator action given a postulated concurrent CCF to the PPS.

PG&E submitted the PPS Replacement Project D3 Assessment Topical Report to NRC in April, 2010, and revised it in September, 2010 to incorporate responses to Requests for Additional Information (RAI). PG&E received NRC approval of the D3 Topical Report in April, 2011.

This paper discusses the methodology by which PG&E assessed the diversity requirements of the Diablo Canyon Power Plant (DCPP) digital PPS relative to current regulations and guidance, and the coping strategy that provides sufficient built-in diversity to meet USNRC DI&C ISG-02 Staff Positions 1-3 without a Diverse Actuation System (DAS).

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

1 INTRODUCTION

Diablo Canyon Power Plant (DCPP) is replacing the existing digital Westinghouse Eagle 21 Process Protection System (PPS) to address maintenance and obsolescence issues. The Eagle 21 PPS was installed in 1994 to replace the original analog Westinghouse 7100 PPS. The analog PPS possessed design depth and diversity such that two or more diverse protective actions would terminate an accident before consequences adverse to public health and safety could occur [1]. Existing diverse RPS functions, including the ATWS Mitigation System Actuation Circuitry (AMSAC) that was installed to meet 10CFR50.62 [2] are not affected by the PPS replacement. The Eagle 21 PPS met the requirements for D3 that existed at the time it was licensed; however, manual operator action was credited for several mitigation scenarios where both primary and backup protection functions were performed in the Eagle 21 PPS.

The current USNRC staff position regarding manual operator action credited in D3 evaluations is set forth in Interim Staff Guidance (ISG)-02 [4] as follows:

"(1) When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room. The preferred independent and diverse backup method is generally an automated system. The use of automation for protective actions is considered to provide a high-level of licensing certainty.…

"(2) If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF and should be sufficient to maintain plant conditions within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident…

"(3) If manual operator actions are used as backup, a suitable human factors engineering (HFE) analysis should be performed to demonstrate that plant conditions can be maintained within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident...

Using the guidance of DI&C ISG-02, PG&E reviewed the DCPP Final Safety Analysis Report (FSAR) [3] Chapter 15 licensing basis accident analyses and the Nuclear Regulatory Commission (NRC) Eagle 21 Safety Evaluation Report (SER) [5] in accordance with USNRC Branch Technical Position (BTP) 7-19 [6]. The review considered the CCF to cause failure of the entire Process Protection System (PPS) concurrent with each Chapter 15 event and accident for which primary or backup mitigative action by the PPS was credited in the analysis. The goals of the review were to identify available automatic means to prevent concurrent PPS software CCF from adversely affecting the mitigation of FSARU Chapter 15 accident or events; and to develop a coping strategy without crediting manual operator actions to mitigate events where diverse automation sufficient to meet above Positions (1) and (2) did not exist outside the existing PPS. PG&E considered that the Human Factors Evaluation (HFE) study to demonstrate adequate operator response per above Position (3) presented an unacceptable degree of project risk with respect to the additional Staff review time that would be required for evaluation and the potential uncertainty of the outcome.

PG&E submitted the PPS Replacement Project D3 Assessment Topical Report to NRC in April, 2010 [7], and revised it in September, 2010 [8] to incorporate responses to Requests for Additional Information (RAI). PG&E received NRC approval of the D3 Topical Report in April, 2011 [9]. The License Amendment for replacement of the Eagle 21 PPS was submitted to NRC on October 26, 2011. Approval is anticipated in May, 2013.

1.1 Method

The DCPP digital PPS replacement D3 assessment describes the integrated digital PPS system design proposed for the replacement. The assessment describes the diversity between the PPS software and the plant control systems, indications, alarms and readouts, and manual circuitry. The assessment evaluated design-basis transients and accidents with the assumed concurrent CCF to demonstrate that plant responses to these transients and accidents can successfully comply with the defined acceptance criteria. Diverse systems and/or operator actions required to meet acceptance criteria were noted.

The evaluation comprised three basic tasks:

1. Identification of the set of transients and accidents to be considered in combination with the assumed CCF of the digital PPS.
2. An evaluation of these transients and accidents which could challenge BTP 7-19 acceptance criteria given a CCF of the PPS; that is, where primary and backup protection functions resided in the PPS, thus potentially susceptible to the postulated CCF.
3. Determination of a coping strategy to address the events where BTP 7-19 acceptance criteria could be challenged given a design basis accident or event with a concurrent CCF to the PPS.

The first two tasks identify the FSAR Chapter 15 design basis events to be considered. Each design basis accident or event in the existing FSAR analyses was then screened for one of the following four categories based on the assumption of PPS failure due to CCF:

Category 1:	Events that do not require the PPS for primary or backup protection
Category 2:	Events that do not require the PPS for primary but require the PPS for backup protection
Category 3:	Events that require the PPS for primary protection but also receive automatic backup protection from systems other than the PPS
Category 4:	Events that assume the PPS for primary and backup protection signals for some aspect of the automatic protection

The events of the first three categories required no further analysis because the postulated concurrent CCF will not adversely affect event mitigation. The remaining Category 4 events are potentially challenging to BTP 7-19 acceptance criteria and require further analysis with respect to the coping strategy.

1.2 Architecture of the Replacement PPS

The PPS Replacement Project replaces in its entirety the Westinghouse Eagle 21 PPS hardware as illustrated in the shaded portion of Figure 1. Equipment in the unshaded portion of Figure 1 is not being replaced or modified by this project. Thus, the PPS Replacement Project maintains the Westinghouse 4-channel, 2-train architecture without affecting existing diverse systems (Nuclear Instrumentation System, ATWS Mitigation System, and Solid State Protection System).

Figure 2 illustrates a typical allocation of the specific signals used to implement Reactor Trip System (RTS) and Engineered Safety Feature (ESF) functions between the Tricon and the ALS for one of the four (4) redundant replacement Protection Sets. The ALS provides Class IE signal conditioning for the Pressurizer Vapor Space temperature, RCS wide range temperature and narrow range RTD inputs to the OPDT and OTDT thermal trip functions. These temperature signals are passed from the ALS to the Tricon for processing by the Tricon portion of the PPS replacement. Figure 2 further illustrates the diverse systems not subject to CCF (i.e, NIS, direct contacts, and AMSAC) that are not affected by the PPS replacement.

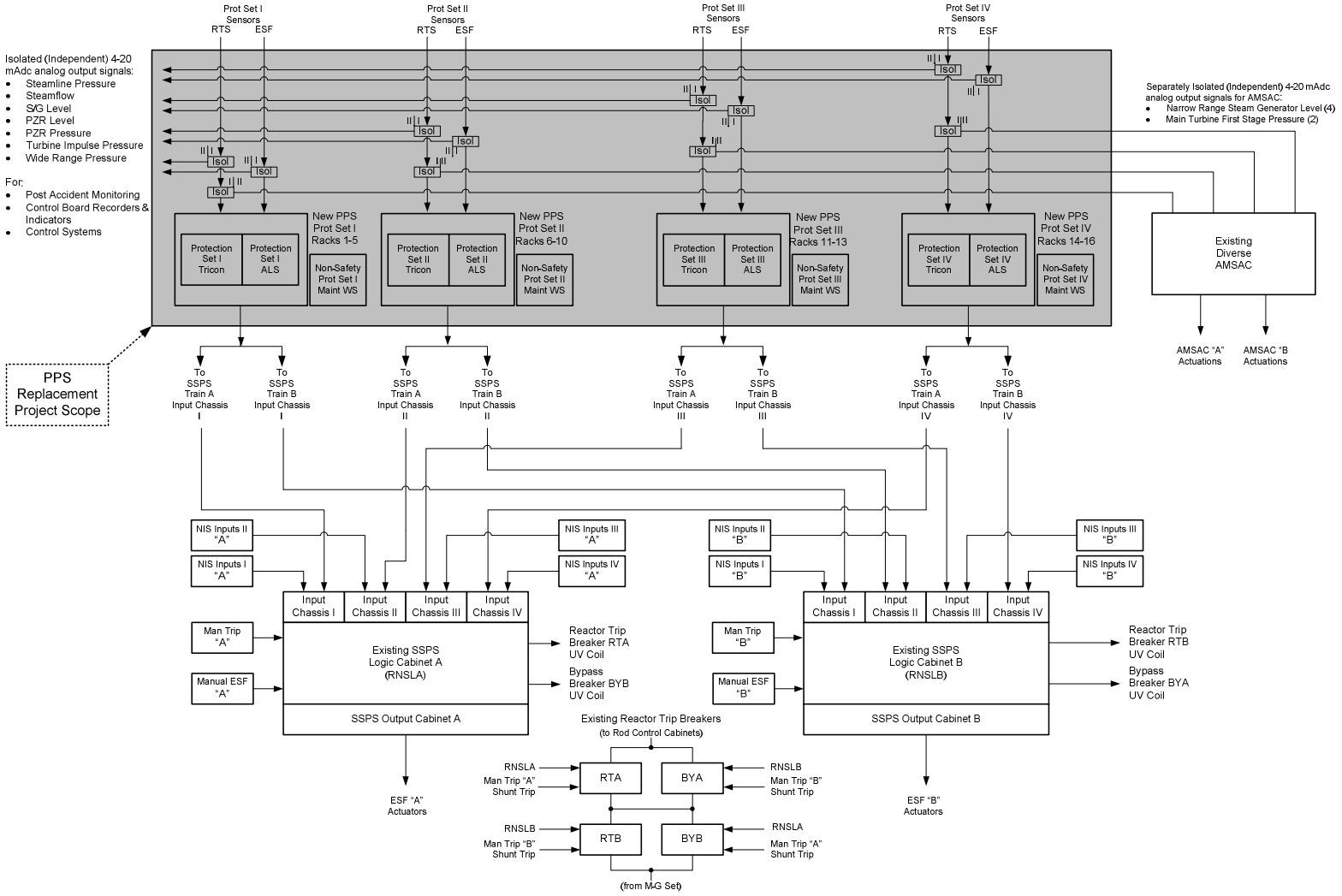

Figure 1: Simplified Diablo Canyon Process Protection System Replacement

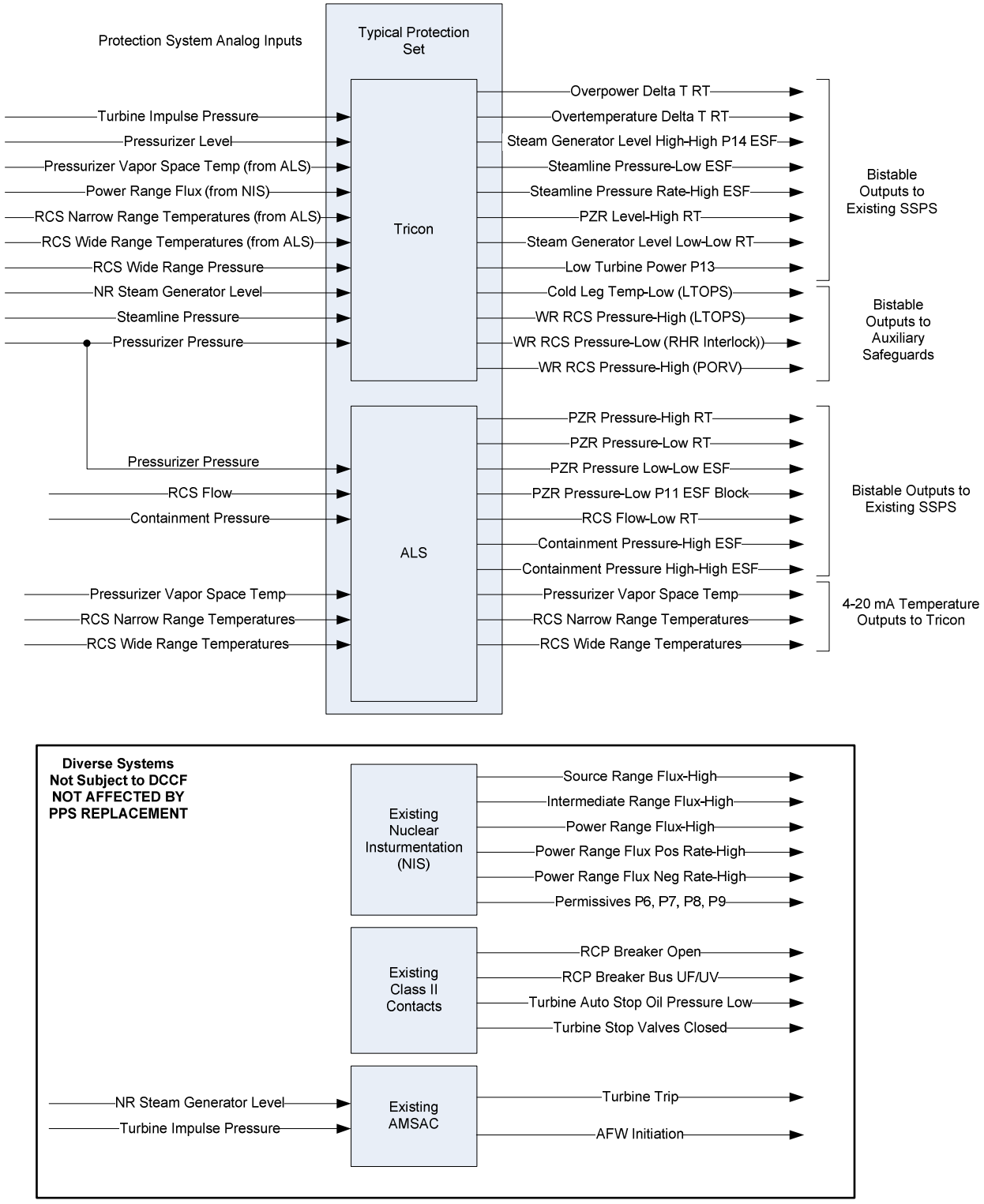

Figure 2. Typical Replacement Process Protection Set

PPS replacement functions are implemented in the same four (4) redundant Protection Sets as the existing Eagle 21 PPS. Each Protection Set uses a software-based Triconex Tricon processor described in Tricon V10 Topical Report Submittal [10] to mitigate events automatically where the PPS Replacement D3 Assessment determined that existing diverse and independent automatic mitigating functions are available to mitigate the effects of postulated CCF concurrent with FSAR [3] Chapter 15 events that were credited with automatic mitigation . For the events where this assessment determined that additional diversity measures were necessary to preclude manual mitigative action, automatic protective functions are performed in the diverse safety-related CSI ALS shown in the shaded portion of Figure 1. The ALS is described in the ALS Topical Report Submittal [11].

The Tricon is Triple Modular Redundant (TMR) from input terminal to output terminal, each input and output module includes three separate and independent input or output circuits or legs. These legs communicate independently with the three Main Processor modules. Standard firmware is resident on the Main Processor modules for all three microprocessors as well as on the input and output modules and communication modules, which are not shown in the figure. The TMR architecture allows continued system operation in the presence of any single or multiple faults within the system. The TMR architecture also allows the Tricon to detect and correct individual faults on-line, without interruption of monitoring, control, and protection capabilities. In the presence of a fault, the Tricon alarms the condition, removes the affected portion of the faulted module from operation, and continues to function normally in a dual redundant mode. The system returns to the fully triple redundant mode of operation when the affected module is replaced.

The diverse ALS portion of the PPS replacement platform utilizes Field Programmable Gate Array (FPGA) hardware logic rather than a microprocessor and has no software component required for operation of the system. Concern for ALS software CCF is minimized through incorporating additional design diversity in the FPGA-based hardware system and using qualified design practices and methodologies to develop and implement the hardware. The ALS subsystem provides two complete and diverse execution paths “A” and “B” with independent design and V&V teams for the Core Logic Boards (CLB), input boards and output boards as shown in Figure 3. Appropriate V&V activities ensure that the output from each development team is indeed diverse from the other. Each CLB has its own set of input and output boards (“A” for CLB “A” and “B” for CLB “B”). The diverse execution path outputs are combined in hardwired logic to ensure that the protective action is taken if directed by either path. A single failed path cannot prevent a protective action.

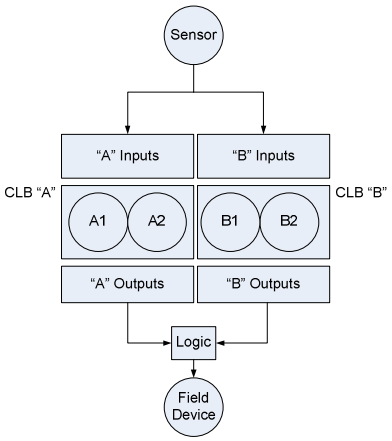

Figure 3. ALS Diversity Architecture for DCPP PPS Replacement

Each FPGA in an execution path contains two sets of redundant hardware logic ("A1" & "A2"; "B1" & "B2"), which perform the application-specific functions independently and in parallel. Diversity between the two sets of logic within a CLB is achieved by changing the logic implementation during the synthesis process. A CLB that detects a mismatch between its logic core outputs identifies itself as failed and sets its outputs to a fail-safe state before halting operation.

Safety-related information (i.e., Pressurizer vapor space temperature and RCS narrow and wide range temperatures) is transmitted from the FPGA logic-based ALS to the software-based Tricon via analog signals. There is no digital communication of safety-related information from the software-based Tricon to the logic-based ALS. There is no software-based communication between or among redundant or diverse Protection Sets. No database information or equipment that uses software is shared between the Tricon and the diverse ALS or between redundant Protection Sets within Tricon or ALS portions of the replacement PPS, except for the analog temperature signals discussed above.

The built-in diversity of the ALS subsystem ensures that the PPS replacement will perform the required safety functions automatically in the presence of a postulated Tricon CCF without an adverse impact on the operator's ability to diagnose the event or perform previously credited manual actuation activities. A Tricon CCF cannot affect ALS safety function.

In other words, a CCF may be assumed that causes the "A" ALS subsystem to fail, but the "B" ALS subsystem will remain functional because the built-in diversity provided by the "A" and "B" execution paths prevents both "A" and "B" paths from being disabled by the same CCF. Conversely, a CCF may be assumed that causes the "B" ALS subsystem to fail, but the "B" ALS subsystem will remain operational.

1.3 Results of the Evaluation

The DCPP D3 assessment assumed that a worst-case CCF results in a total failure of the Tricon portion of the PPS system, similar to the Eagle 21 D3 evaluation. The Eagle 21 diversity assessment assumed a postulated CCF caused all automatic protection functions generated in the Eagle 21 PPS to fail to perform the protection functions described in DCPP FSAR Chapter 15.

Category 1 protection functions are processed through systems other than the PPS. The FSAR Chapter analysis of the events crediting these independent and diverse protective functions either: (1) takes credit for independent primary mitigating functions; or (2) does not require a primary mitigating function. Mitigation of these D3 Assessment Category 1 events is unaffected by CCF of the PPS.

Process Variable	**D3 Assessment Category 1 Protection Functions**
Neutron Flux	Power Range High-Flux (Low Setting) Reactor Trip
	Power Range High-Flux (High Setting) Reactor Trip
	Power Range Positive Flux Rate Reactor Trip
	Power Range Flux Control Rod Stop
	Intermediate Range High-Flux Reactor Trip
	Source Range High-Flux Reactor Trip
	Input to Over Power Delta Reactor Trip
	Input to Over Temperature Delta T Reactor Trip
AMSAC(Steam Generator Low Level)	Turbine Trip Above C-20 Permissive
Main Turbine Stop Valve Position	Turbine Trip Reactor Trip
Turbine Auto Stop Oil Pressure Low	
RCP Bus Undervoltage	Reactor Trip
RCP Bus Underfrequency	Reactor Trip
RCP Circuit Breaker Open	Reactor Trip

Category 2 and 3 protection functions either: (1) do not require the PPS for primary protection but assume PPS for backup protection (Category 2); or (2) require the PPS for primary protection but receive automatic backup protection from systems other than the PPS (Category3). These protection functions are performed in the software - based Tricon subsystem of the replacement PPS. Independent and diverse primary or backup protection is available for these functions. Mitigation of these Category 2 and 3 events is not adversely affected by CCF of the PPS Tricon subsystem.

Process Variable	**D3 Assessment Category 2 and 3 Protection Functions**
Pressurizer Level	Pressurizer High-Level Reactor Trip
RCS Narrow-Range Temperature	Input to Over Temperature Delta T Reactor Trip
	Input to Over Power Delta T Reactor Trip
	Input to SG Low-Low Level Trip Time Delay
Steam Generator Level	Steam Generator Low-Low Level Reactor Trip
	Hi-Hi Level Feedwater Isolation
	Hi-Hi Level Turbine Trip
	Hi-Hi Level MFW Pump Trip
	Low-Low Level AFW Actuation (Process Sense performed by RTS; AMSAC utilizes independently isolated level signals and independent turbine impulse pressure channels to provide diverse function)
Steam Line Pressure	High-Negative Pressure Rate SLI
	Low-Pressure SI
	Low-Pressure SLI
Turbine Impulse Pressure	Permissive 13 Low Turbine Power Permissive (Input to P-7 Low Power Reactor Trip Permissive)

Category 4 protection functions require the PPS for both primary protection and backup protection. Manual operator action is credited in the existing Eagle 21 SER to mitigate these events given a concurrent CCF in the PPS. In the replacement PPS, these protection functions are performed in the logic based ALS subsystem of the replacement PPS where built-in diversity ensures continued automatic protection given a concurrent CCF. Mitigation of Category 4 events is not affected by CCF of the PPS Tricon or ALS subsystem. The ALS is not affected by a Tricon CCF. The ALS “A” and “B” execution paths are not disabled by the same CCF.

Table 1 shows how the PPS functions performed by the diverse ALS subsystem preclude the manual operator actions otherwise required to mitigate events in the presence of a concurrent CCF. Each of the Category 4 events listed in the left hand column of the table required manual operator action for accident mitigation in the presence of a CCF in the Eagle 21 PPS SER [5]. The "X" in the associated PPS function column identifies the ALS functions that will remain operational due to the built-in diversity characteristics of the ALS system.

The need for manual operator action is eliminated by the diversity built into the replacement PPS design and plant safety is improved without the need for a DAS.

Accident Analysis/Event		Primary Protection System Functions Performed by Diverse ALS Sub-System							
FSAR Section	D3 Topical Report Category 4 Events	PZR Pressure Low SI (Note 1)	PZR Pressure High RT	PZR Pressure Low RT	Cont. Pressure High SI	Cont. Isolation Phase A	Cont. Isolation Phase B	Cont. Pressure High Containment Spray	RCS Flow Low RT
15.2.5	Loss of Forced RCS Flow								X
15.2.13	RCS Depressurization			X					
15.3.1 15.4.1	SBLOCA / LBLOCA	X		X	X	X	X	X	
15.4.2.1	Steam Line Break	X				X	X	X	
15.4.2.2	Main Feed Pipe Rupture		X		X	X			
15.4.3	SG Tube Rupture	X		X					

Note 1: Automatic reactor trip occurs on safety injection due to low pressurizer pressure or high containment pressure.

Table 1. Diverse ALS Protection Functions

2 CONCLUSIONS

Diablo Canyon Units 1 and 2 FSARU Chapter 15 licensing basis accident analyses were reviewed to determine which events required the Eagle 21 Process Protection System for primary or backup protection. Those transients identified as requiring the Process Protection System for primary protection system response were reviewed to determine if diverse means of automatically mitigating the transient are available, or annunciators and indicators are available to allow the operator to diagnose the event and bring the plant to a safe shutdown condition in a timely manner. For most transients no operator action is required since sufficient non-PPS-based automatic functions exist; i.e., the Nuclear Instrumentation System (NIS), Solid State Protection System (SSPS) and the AMSAC. For several events, however, some operator action was necessary. In these cases, backup protection system functions, alarms, and indicators processed independently of Eagle 21, along with existing Diablo Canyon operating procedures and Emergency Operating Procedures, were credited to bring the plant to a safe shutdown condition.

Each of the eight Category 4 functions shown in Table 1would be rendered inoperable due to the effects of a postulated CCF under the existing Eagle 21diversity scheme [5], because both primary and backup protection functions are performed by the Eagle 21 PPS. The replacement PPS design, which incorporates the safety-related ALS subsystem with built-in system diversity, will ensure that these functions will be performed automatically without adverse impact to the operator's ability to diagnose or perform previously credited manual actuation activities.

In their SER, NRC Staff determined [8] that the Class IE, nuclear safety-related DCPP replacement PPS design provides reasonable assurance that appropriate diverse means of actuation exist to mitigate DCPP Chapter 15 event events automatically, should a CCF occur in either the Tricon or ALS subsystems of the PPS system concurrent with the events for which automatic mitigation by the PPS is credited. Therefore, the replacement PPS design addresses the ISG-02 Staff Positions adequately and will meet BTP 7-19 acceptance criteria without a Diverse Actuation System (DAS).

3 REFERENCES

1. Westinghouse Electric Corporation WCAP-7306, “Reactor Protection System Diversity in Westinghouse Pressurized Reactors,” (1969) Non-Proprietary Class 3.
2. Title 10 Code of Federal Regulations Article 50.62, “Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants,” (January, 2003).
3. Diablo Canyon Power Plant Final Safety Analysis Report (FSAR).
4. U.S. Nuclear Regulatory Commission, Digital Instrumentation and Controls, Revision 2, “DI&C-ISG-02 Task Working Group #2: Diversity and Defense-in-Depth Issues Interim Staff Guidance,” June 5, 2009 (ADAMS Accession No. ML091590268)
5. USNRC, “Safety Evaluation Report Eagle 21 Reactor Protection System Modification With Bypass Manifold Elimination, PG&E, Diablo Canyon Power Plant, “ (October 7, 1993).
6. USNRC Branch Technical Position (BTP) 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems,”
7. PG&E, “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
8. PG&E, “Diablo Canyon Power Plant Topical Report, Process Protection System Replacement Diversity & Defense-in-Depth Assessment,” September 9, 2010 (ADAMS Accession No. ML102580726)
9. 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)
10. Invensys Operations Management , Topical Report 7286-545-1, Revision 4, “Triconex Topical Report,” December 20, 2010, (ADAMS Accession No. ML110140443)
11. CS Innovations Document No. 6002-00301-NP, Revision 1, “ALS Topical Report and Supporting Documents Submittal,” August 11, 2010 (ADAMS Accession No. ML102570797)