Enclosure
Attachment 6
PG&E Letter DCL-13-016

Westinghouse document LTR-RAM-I-13-002 NP-Attachment, Revision 0, "Justification for the Application of Technical Specifications Changes in WCAP-14333 and WCAP-15376 to the Tricon/ALS Process Protection System at the Diablo Canyon Power Plant"

LTR-RAM-I-13-002 NP-Attachment
January 31, 2013

Attachment

Justification for the Application of Technical Specification Changes in WCAP-14333 and WCAP-15376 to the TRICON/ALS Process Protection System at the Diablo Canyon Power Plant

Revision 0

R.E. Weber, Author

G.R. Andre, Verifier

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066

Table of Contents

List of Figures

List of Tables

LIST OF ACRONYMS AND ABBREVIATIONS

AC	Alternating Current
A/D	Analog/Digital
AFW	Auxiliary Feedwater
ALS	Advanced Logic System
AMSAC	ATWS Mitigation System Actuation Circuitry
ASU	ALS Service Unit
ATWS	Anticipated Transient without Scram
BIST	Built-In Self Test
C&L	Condition & Limitation
CCF	Common Cause Failure
CDF	Core Damage Frequency
CLB	Core Logic Board
COT	Combined Outage Time
CT	Completion Time
DAC	Digital-Analog Converter
DC	Direct Current
DCPP	Diablo Canyon Power Plant
DDC	Digital-Digital Converter
DFP	Digital Filter Processor
DLH	Data Link Handler
EAI	Eagle Analog Input
EAO	Eagle Analog Output
ECO	Eagle Contact Output
EPT	Eagle Partial Trip
ERI	Eagle RTD Input
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation Signal
FET	Field Effect Transistor
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FSARU	Final Safety Analysis Report Update
FW	Feedwater
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
IPE	Individual Plant Examination
LCP	Loop Calculation Processor
LOCA	Loss of Coolant Accident
LERF	Large Early Release Frequency
LPS	Loop Processor Subsystem
LTOP	Low Temperature Overpressure Protection
MAS	Main Annunciator System
MCB	Main Control Board

NI	Nuclear Instrumentation
NIS	Nuclear Instrumentation System
NR	Narrow Range
NRC	Nuclear Regulatory Commission
OA	Operator Action
PG&E	Pacific Gas & Electric Company
PORV	Power Operated Relief Valve
PLC	Programmable Logic Controller
PPS	Process Protection System
PRA	Probabilistic Risk Assessment
PWROG	Pressurized Water Reactors Owners Group
PZR	Pressurizer
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RPS	Reactor Protection System
RT	Reactor Trip
RTB	Reactor Trip Breaker
RTD	Resistance Temperature Device
RTS	Reactor Trip Signal
SER	Safety Evaluation Report
SI	Safety Injection
SSPS	Solid State Protection System
STI	Surveillance Test Interval
TCM	TRICON Communication Module
TMR	Triple Modular Redundant
TS	Technical Specifications
TSP	Tester Sequence Processor
V&V	Verification and Validation
VDC	Volts Direct Current
WOG	Westinghouse Owners Group
WR	Wide Range

1.0 Purpose

Demonstrate that the changes to the Diablo Canyon Power Plant (DCPP) Technical Specifications (TS) justified in WCAP-14333-P-A, Rev. 1 and WCAP-15376-P-A, Rev. 1 that are applicable to the Eagle 21 Process Protection System (PPS) are also applicable to the replacement TRICON/ALS PPS.

2.0 Background

WCAP-10271-P-A; WCAP-10271, Supplement 1-P-A; WCAP-10271-P-A, Supplement 2, Rev. 1; WCAP-14333-P-A, Rev. 1; and WCAP-15376-P-A, Rev. 1 (References 1-5) provide the justification for increasing completion times (CT), bypass test times, and surveillance test intervals (STI) for components of the reactor protection system. The reactor protection system components include the analog channels, logic cabinets, master and slave relays, and reactor trip breakers (RTB). The analysis supporting these changes is applicable to the Westinghouse 7100, 7300, and Eagle 21 process protection systems. The changes to the CT, bypass test time, and STI for the PPS justified in these WCAPs are provided in Table 2-1.

The Nuclear Regulatory Commission's (NRC) Safety Evaluation associated with WCAP-15376-P-A specifically stated "For future digital upgrades with increased scope, integration and architectural differences beyond that of Eagle 21, the staff finds the generic applicability of WCAP-15376-P, Rev. 0 to future digital systems not clear and should be considered on a plant-specific basis." Based on this statement, it is concluded that the applicability of the TS changes justified in WCAP-15376-P-A, Rev. 1 to digital systems other than Eagle 21 needs to be justified. A similar statement is not included in the NRC's Safety Evaluation for WCAP-14333-P-A, Rev. 1, but it would be prudent to provide such a justification.

The DCPP was initially licensed with the Westinghouse 7100 PPS. This was replaced with the digital Eagle 21 PPS in 1993. Due to obsolescence issues, the Eagle 21 PPS is now being replaced with a digital Advanced Logic System (ALS) and TRICON System combination. Only the PPS is impacted by this change; it is a complete replacement. The sensors, solid state protection system (SSPS) logic cabinets, RTBs, and master and slave relays will remain the same, as will the control board indications, the nuclear instrumentation system (NIS), interactions with control functions, and the ability to perform operator actions to actuate safety systems.

Eagle 21 was implemented with the CTs, bypass test times, and STIs justified in WCAP-10271 including Supplements 1 and 2. Subsequently, changes to these TS parameters justified in WCAP-14333-P-A and WCAP-15376-P-A were incorporated into the DCPP TS in 2005. Implementation of the WCAP changes on a plant-specific basis requires demonstrating the analyses supporting the changes are applicable to the plant. Implementation guidance is provided for WCAP-14333-P-A (Reference 6) and WCAP-15376-P-A (Reference 7) that is used to demonstrate applicability of the analyses.

Table 2-1: Technical Specification Process Protection Systems Parameters Justified in PWROG WCAPs				
Parameter	**Before WCAP-10271**	**WCAP-10271, w/Supplements 1 and 2**	**WCAP-14333**	**WCAP-15376**
Completion Time	1 hour	6 hours	72 hours	72 hours
Bypass Test Time	2 hours	4 hours	12 hours	12 hours
Surveillance Test Interval	1 month	3 months	3 months	6 months

3.0 Assessment Approach

[

]^{a,c}

4.0 System Descriptions

The following sections discuss the reactor protection system in general, followed by the Eagle 21 and TRICON/ALS systems and the signals processed by each PPS.

4.1 Reactor Protection System

The typical circuit used to develop reactor trip actuation signals consists of analog channels (field transmitters or process sensors, and the signal process control and protection system), combinational logic units (solid state logic cabinets), and RTBs. The typical circuit used to develop engineered safety feature actuation signals consists of analog channels, combinational logic units (solid state logic cabinets), and actuation relays. The analog channels, excluding the transmitters or process sensors, are replaced by digital processing with the Eagle 21 and TRICON/ALS systems. The boards within the logic cabinets control the operation of the RTB and actuation relays.

There are two trains of logic cabinets, RTBs, and actuation relays. The analog/digital (A/D) channels, usually arranged in one-out-of-two, two-out-of-three, or two-out-of-four logic combinations, provide signals to both logic cabinets (trains). The actuation relays are master and slave relays with the master relays controlling the slave relays. The slave relays actuate the required safety equipment. Figure 4-1 shows a simplified diagram of the RPS.

Any particular protective function, such as safety injection (SI) on pressurizer pressure low, will have two, three, or four separate A/D channels with each providing input to both logic cabinets. Actuation of the RTBs or master and slave relays requires a combinational logic of one-out-of-two, two-out-of-three, or two-out-of-four, as appropriate.

A typical analog channel consists of a sensor, loop power supply, signal conditioning circuits, and a comparator which is the output device to the logic cabinet. The sensor measures physical parameters such as temperature, pressure, level, etc. The measurement is converted to an electrical signal and transmitted to the protection racks for signal conditioning. The signal conditioning modules perform a number of functions including amplification, square root derivation, lead/lag compensation, integration, summation, and isolation. A signal comparator, usually a bistable device, compares the conditioned signal to a predetermined setpoint and turns the output off or on if the voltage exceeds the setpoint. Each bistable controls two relays; one for Train A logic and the other for Train B logic. A typical digital channel uses a similar configuration; however, the sensor output is converted using A/D interface module and processed digitally.

The combinational voting logic function is performed in the logic cabinet. Each SSPS train consists of the input cabinet which contains the input relays, the logic cabinet, and the output cabinet which contains the master and slave relays. The input bays are arranged such that all inputs are physically and electrically isolated. The logic cabinet is where all the logic decisions

are made and where the majority of system tests are performed. The output cabinets are the interface between the logic circuits and the safeguards equipment.

The inputs from the analog/digital channels are applied to universal logic boards which are the basic circuits of the protection system. These boards contain the logic circuits. Grounding of the appropriate number of universal board inputs will cause a signal to be generated. Output signals from the universal logic boards are connected to other universal logic boards to enable additional logic combinations, undervoltage driver output boards to trip the RTBs, or safeguard driver output boards to drive the master relays which in turn drive the slave relays. The slave relays then actuate equipment.

4.2 Test and Maintenance Activities

Test and maintenance activities are related to the analog/digital channels (PPS), logic cabinets, RTBs, and master and slave relays in the reactor trip system (RTS) and engineered safety features actuation signals (ESFAS) instrumentation systems. The protection system is designed to allow online testing. The testing and maintenance activities of interest in this assessment are those related to the digital channels of the PPS. With regard to the following assessment, the impact of test and maintenance activities on the reactor protection system is important since these activities are impacted by the changes to TS CTs, bypass test times, and STIs. Of specific interest is the impact on the reliability of protection system signals.

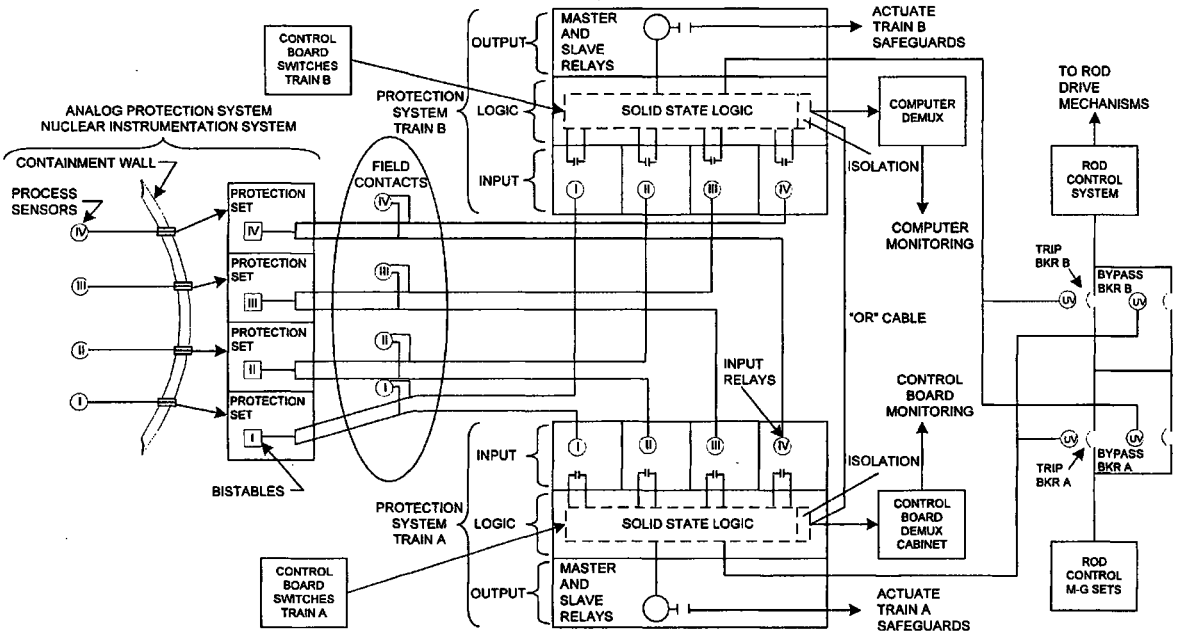

Figure 4-1: Simplified Diagram of the Reactor Protection System

4.3 Eagle 21 System Description

The following information is taken from Section 2 of Reference 8.

Architecture of the Westinghouse Eagle 21 PPS, which replaced the original analog DCPP PPS, is illustrated in Figure 4-2. Functions generated by Eagle 21 are shown in Figure 4-3. The Eagle 21 PPS is comprised of four Protection Sets. Each Protection Set is further comprised of two or more processors, each of which is made up of three major modules: the Digital Filter Processor (DFP), the Loop Calculation Processor (LCP) and the Tester Subsystem, which contains the Test Sequence Processor (TSP). For each of the three processor modules, the application software is similar, but not identical across the four protection sets.

The DFP converts analog input signals to digital signals, filters them and makes the data available to the LCP. The DFP performs onboard diagnostics and auto calibrations. The DFP writes the input digital signals to a memory section that is read on a 100 msec cycle by the LCP.

The LCP periodically transfers the input signal information from the DFP to its own memory, performs the calculations required for protective functions and compares the data to the channel trip setpoints. Outputs from the LCP are directed to:

- Digital-Analog Converter (DAC) for analog control and indication outputs: Isolated signals for use by process control functions are provided by Eagle Analog Output (EAO) cards.

- Digital-Digital Converter (DDC) for protective outputs: When a no trip required condition exists for a given channel in the LCP, the LCP signals the DDC to provide a pulse train to the Eagle Partial Trip (EPT) board.

When a trip required condition exists, the LCP signals the DDC to halt the pulse train to the EPT. The channel is tripped if the pulse train halts for any reason.

The Tester Subsystem interconnects all Eagle 21 subsystems to monitor and test overall system performance. The TSP controls Tester Subsystem functions such as surveillance testing, data transfer during parameter update operations and monitoring for DFP and LCP failures. The TSP generates outputs to the Main Annunciator System (MAS) if it detects a failure.

If the TSP itself fails, hardware watchdog timers in the Eagle Contact Output (ECO) cards will not be reset periodically and will generate MAS alarm outputs. More detailed information about the self-test features built into Eagle 21 can be found in Section 5.2.

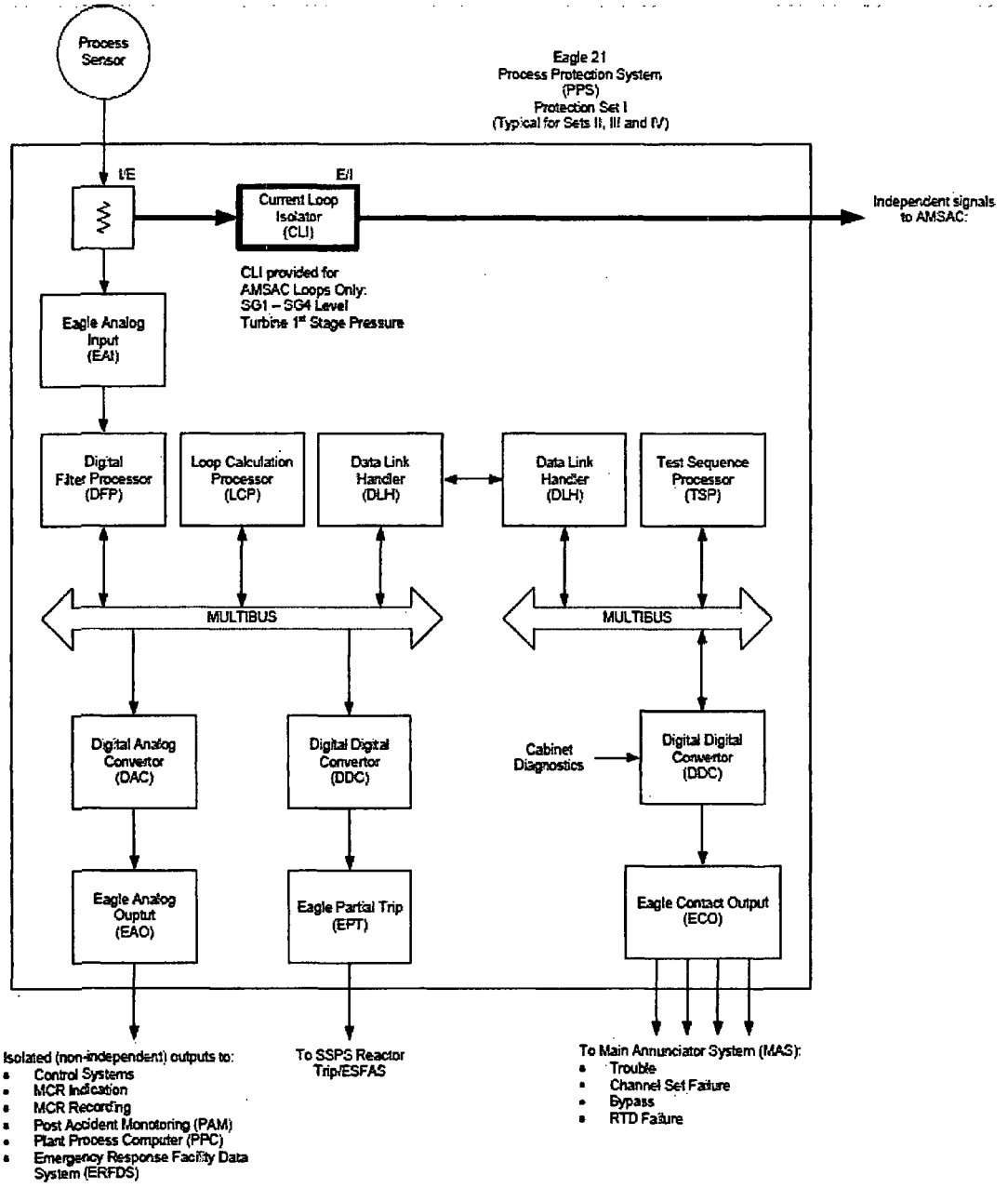

Figure 4-2: Eagle 21 Block Diagram

Figure 4-3 shows the process sensor inputs, the reactor trip signals, and the ESFAS signals generated by the Eagle 21. The existing nuclear instrumentation signals, signals from Class II contacts, and the anticipated transient without scram (ATWS) mitigating system actuation circuitry (AMSAC) signals are not processed via the Eagle 21 System; therefore, these signals are not impacted by the proposed change (Figure 4-4).

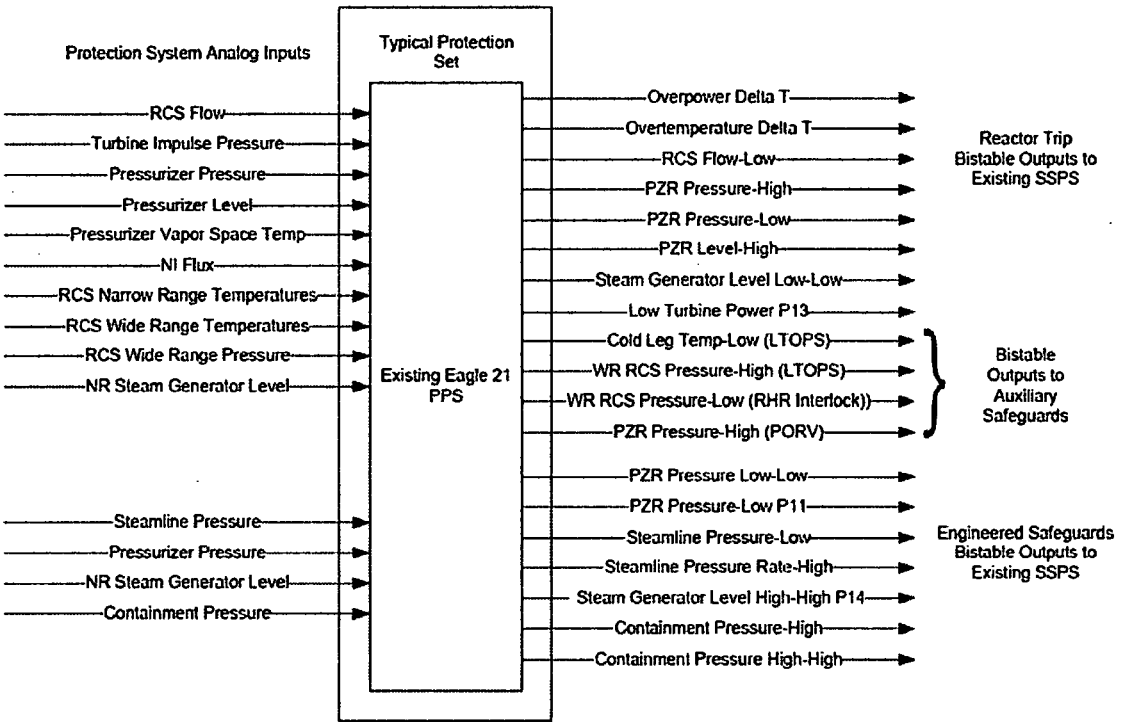

Figure 4-3: Typical Existing Eagle 21 PPS Functions

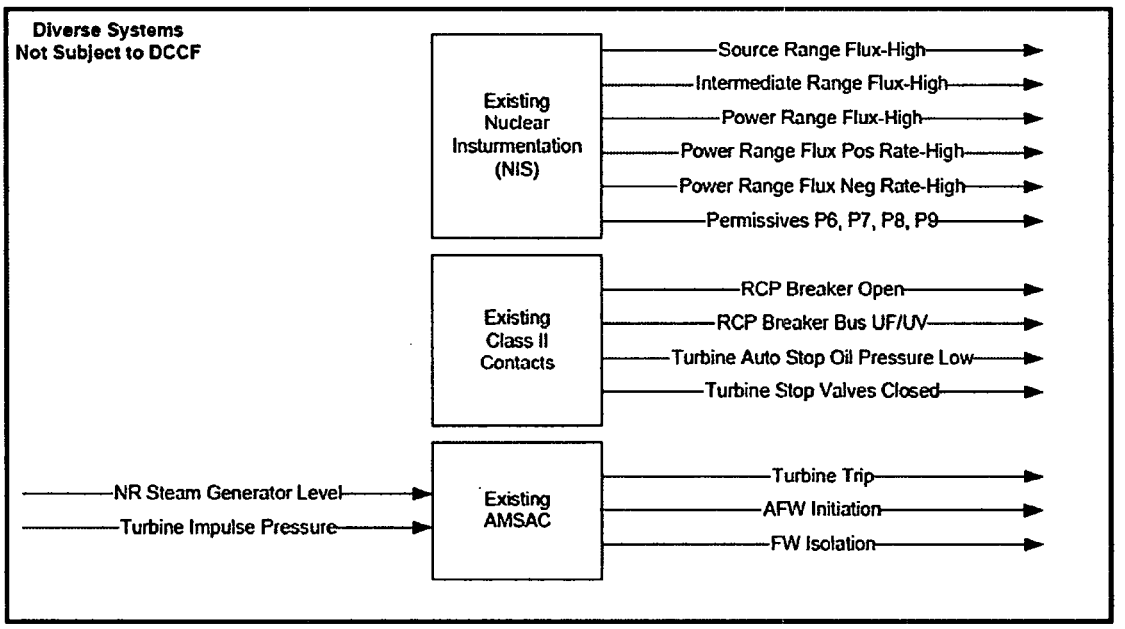

Figure 4-4: Signals Not Affected by the PPS Upgrades

4.4 TRICON/ALS System Description

The TRICON/ALS replacement PPS processes a variety of plant parameters and then outputs signals to the SSPS. The ALS and TRICON portions of the PPS provide diverse protection to automatically mitigate plant events. A high level block diagram of the signals processed by the TRICON/ALS replacement PPS is shown below in Figure 4-5. As with the Eagle 21 system, the existing nuclear instrumentation signals, signals from Class II contacts, and the AMSAC signals are not processed via the Eagle 21 System; therefore, these signals are not impacted by the proposed change (see Figure 4-4).

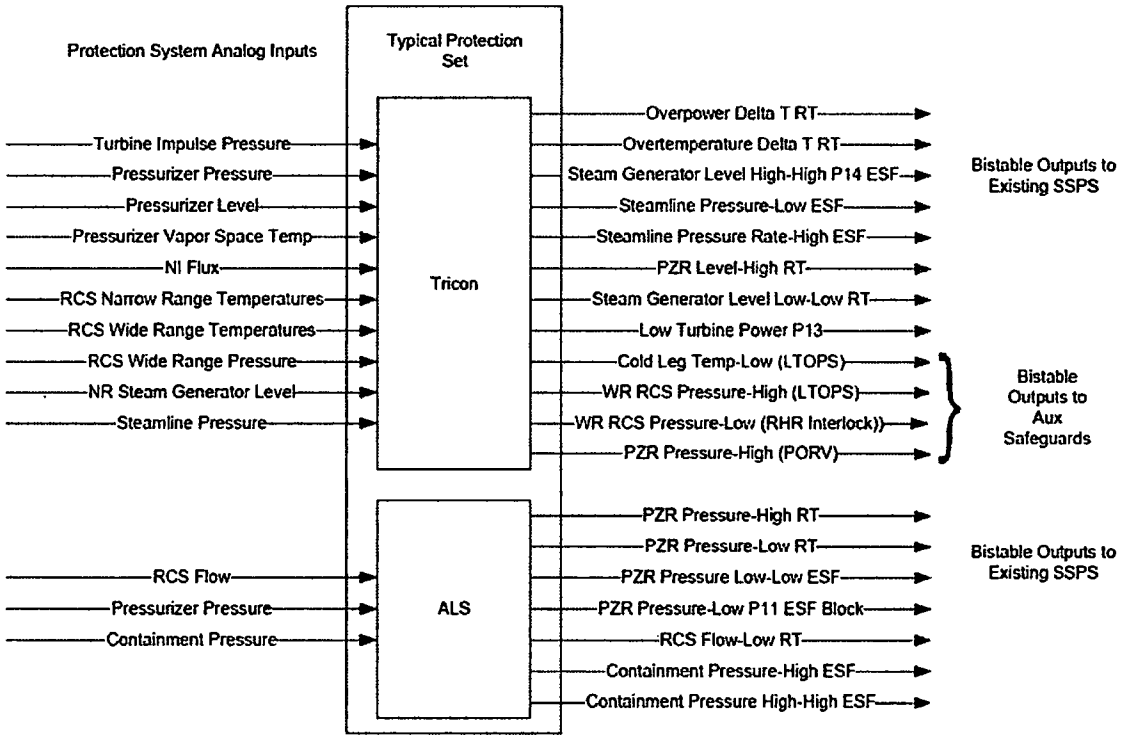

Figure 4-5: TRICON/ALS Replacement PPS

4.4.1 TRICON-Based Replacement PPS

The following information was taken from Reference 11.

The TRICON is a mature commercial Programmable Logic Controller (PLC) that was designed from its inception for highly reliable use in safety systems. High reliability and system availability is achieved through the triple modular redundant (TMR) architecture. This design enables the TRICON System to be highly tolerant to hardware failures, to identify and annunciate faults that inevitably occur, and to allow replacement of modules with the system online so that faults are repaired before they become failures. The TRICON V10 platform was approved by the NRC in a Safety Evaluation report issued April 12, 2012 (Reference 21).

The TRICON Platform consists of the input modules, the TRICON processor, communications, output modules, and diagnostic functions (Figure 4-6).

The input modules include both analog and digital modules. All TMR input modules contain three separate, independent processing systems, referred to as legs, for signal processing (Input Legs A, B, and C). The legs receive signals from common field input termination points. The microprocessor in each leg continually polls the input points, and constantly updates a private input data table in each leg's local memory. Any signal conditioning, isolation, or processing required for each leg is also performed independently. The input modules possess sufficient leg-to-leg isolation and independence so that a component failure in one leg will not affect the signal processing in the other two legs.

The diagnostic routine for the digital input module compares the input table data for the three legs. Any data discrepancies are reported to the respective main processor modules, which maintain diagnostic information in local memory. The main processor module fault analyzer routines determine whether a fault exists on a particular module at the end of each scan. Should a main processor module diagnose a faulty leg, a fault indicator will be illuminated on that particular input module.

Each analog input module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault, and may continue to operate properly with some multiple faults.

A TRICON System utilizes three main processor modules to control three separate legs of the system. Each main processor module operates independently with no shared clocks, power regulators, or circuitry. Each module owns and controls one of the three signal processing legs in the system, and each contains two 32-bit processors. One of the 32-bit processors is (1) a dedicated, leg-specific I/O communication microprocessor that processes all I/O with the system I/O modules, and (2) a dedicated, leg-specific processor manages interfaces with all Communication Modules in the system.

Diagnostics at the main processor module level validate the health of its circuitry as well as make decisions about the health of each I/O module and communication module in the system.

The modules compare memory, basic processor instructions and operating modes, verify communication between shared memory and the I/O communication microprocessor, verify communication between the I/O communication microprocessor and the I/O modules, and verify the TriClock/TriTime and TRIBUS interfaces.

The TRICON communication module (TCM) communicates with all three main processors over three separate communication buses, one to each main processor. The TCM module has a dedicated communication port for each communication bus. Hence the TCM will continue to communicate with the main processors upon the failure of a main processor or a communication port. The TCM can be used to transmit safety relevant data, provided the receiving main processors check for proper validity of the message and check to make sure the messages are being received at the required update rate. If the received data is not valid, delayed, or not received, then the data will be set to the fail safe state.

The output modules consist of digital and analog output modules. All output modules contain three identical and isolated legs. Each leg includes an I/O microprocessor that receives its output table from the Main processor's I/O communication processor associated with that leg. All of the digital output modules use special quadruplicated output circuitry that votes on the individual output signals. This voter circuitry is based on parallel-series paths that pass power if the driver for legs A and B, or legs B and C, or legs A and C command them to close (i.e. two-out-of-three vote). Any single leg failure, any single switch failure, or corrupted signal from a main processor module will be compensated for or filtered out by the voter logic at the output module level.

A simplified diagram of the TRICON Chassis is shown in Figure 4-6. Refer to Figure 4-5 for signals processed by the TRICON portion of the PPS upgrade at DCPP.

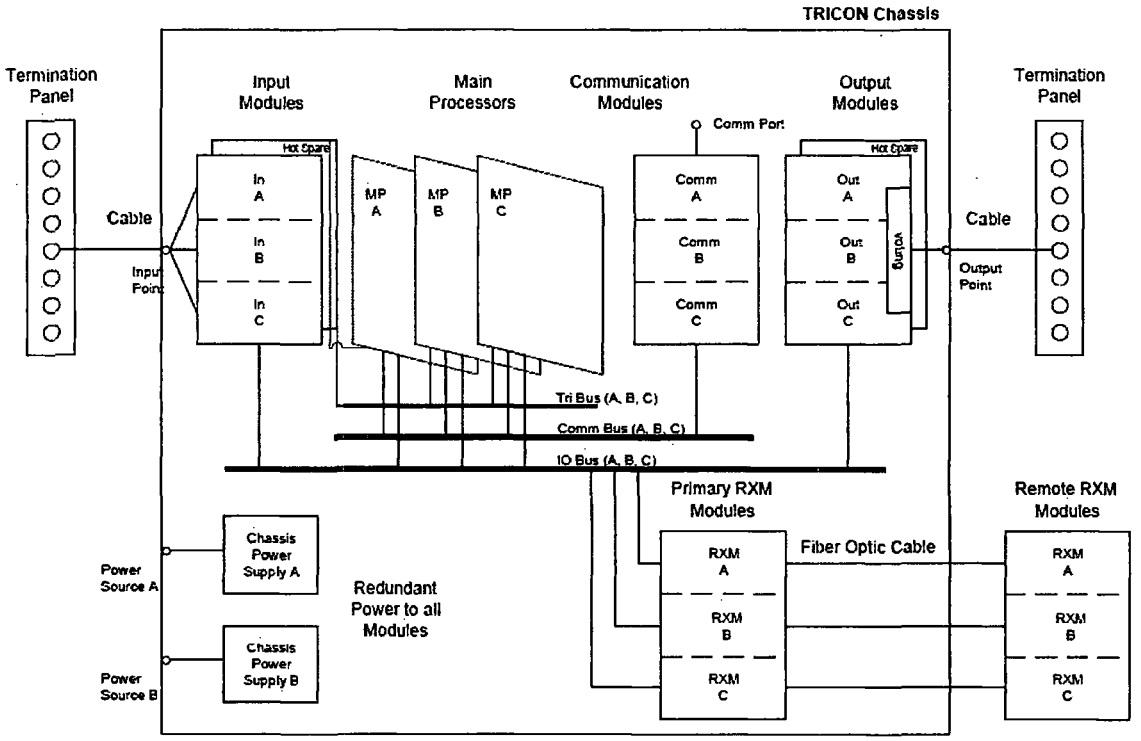

Figure 4-6: Simplified Block Diagram of the TRICON System

4.4.2 Advanced Logic System (ALS) Replacement PPS

The following information is taken from the ALS Platform Overview (Reference 9).

The ALS is a logic based platform which does not utilize a microprocessor or software for operation, but instead relies on a simple hardware architecture. The ALS platform incorporates advanced features to allow for diagnostics, testability, and modularity. Diagnostics and testing capabilities are designed into the ALS platform to ensure there is a systematic approach to maintaining and testing the system.

The ALS incorporates advanced failure detection and isolation techniques. The operation of the system is deterministic in nature and allows the system to monitor itself for validation of the desired function. The ALS platform is based on autonomous boards working together. The system utilizes advanced logic to perform distributed control where no single failure will result in an erroneous plant event while maintaining the ability to perform the intended safety function. The ALS is both an analog and digital platform based on solid-state devices, such as opto-couplers, FPGAs, line drivers, and power FETs. The ALS does not utilize a microprocessor and therefore has no software component for the operation of the system. The concern for software common mode failures is eliminated by incorporating a full hardware system which only uses proven design practices and methodologies for implementation of the hardware.

The ALS supports advanced diagnostics features using the ALS Service Unit (ASU). The ASU is a dedicated piece of test equipment which can be connected to the ALS rack during diagnostics or testing by plant personnel which allows plant personnel to access detailed status and configuration information of the system while the system is online. In addition, post event analysis information about the system is available to plant personnel for evaluation of the event after it has occurred.

As described in Section 2.4 of Reference 9, signal flow in the ALS rack is simple and straight forward. The following outlines the basic principles of ALS operation. The generic ALS architecture is shown in Figure 4-7. Refer to Figure 4-5 for signals processed by the ALS portion of the PPS upgrade at DCPP.

The ALS operation is accomplished by a fundamental cycle with three phases, the cycle is explained below:

1) **Sampling Field Inputs** – On a given input board there will be a number of input channels each responsible for conditioning, sensing, filtering, and sampling the field inputs, such as, transmitters and sensors. In the event an input channel changes due to a field input change (i.e., contact transition from open to close) the signal conditioning circuit will detect this transition and change state. Each channel is described with state information and integrity information. If a channel fails self-test it will be marked as invalid in the integrity information. The Core Logic Board (CLB) retrieves the state and integrity information during the regular polling of data from the input board.

2) **Performing Logic Decisions** – Input state and integrity information are retrieved from the input boards and are stored in the input register bank in the CLB. When all input data is present the application specific core logic circuit within the CLB will perform its logic function. Based on the current state of the system, input states and integrity information, the CLB will determine a new output state for all outputs. The application specific logic functions consist of timers, random logic gates, finite state machines, 2/4-voters, etc. The decision making process is instantaneous. All system level integrity and data checks are performed during this phase of operation. The results of the application specific logic circuit are stored in an output register bank within the CLB FPGA and from there the information is transmitted to the output boards.

3) **Driving Field Outputs** – The output boards receive information from the CLB. The digital circuits will immediately drive the signal conditioning circuit and perform the intended output function. In this case, provide outputs to the logic cabinet input bays.

The ALS platform uses a combination of design and test strategies in order to maintain a high reliability. These include redundancy, built-in self-test, and inherent self-test. All ALS FPGAs contain redundant digital logic to reduce the likelihood of a single failure causing the board to fail. The built-in self-test exercises all critical functions within a board which checks for failures that can cause the system to be inoperable in an undetectable state, until the channel operability test is performed. The inherent self-test features are factored into the design by ensuring some failures are detected immediately.

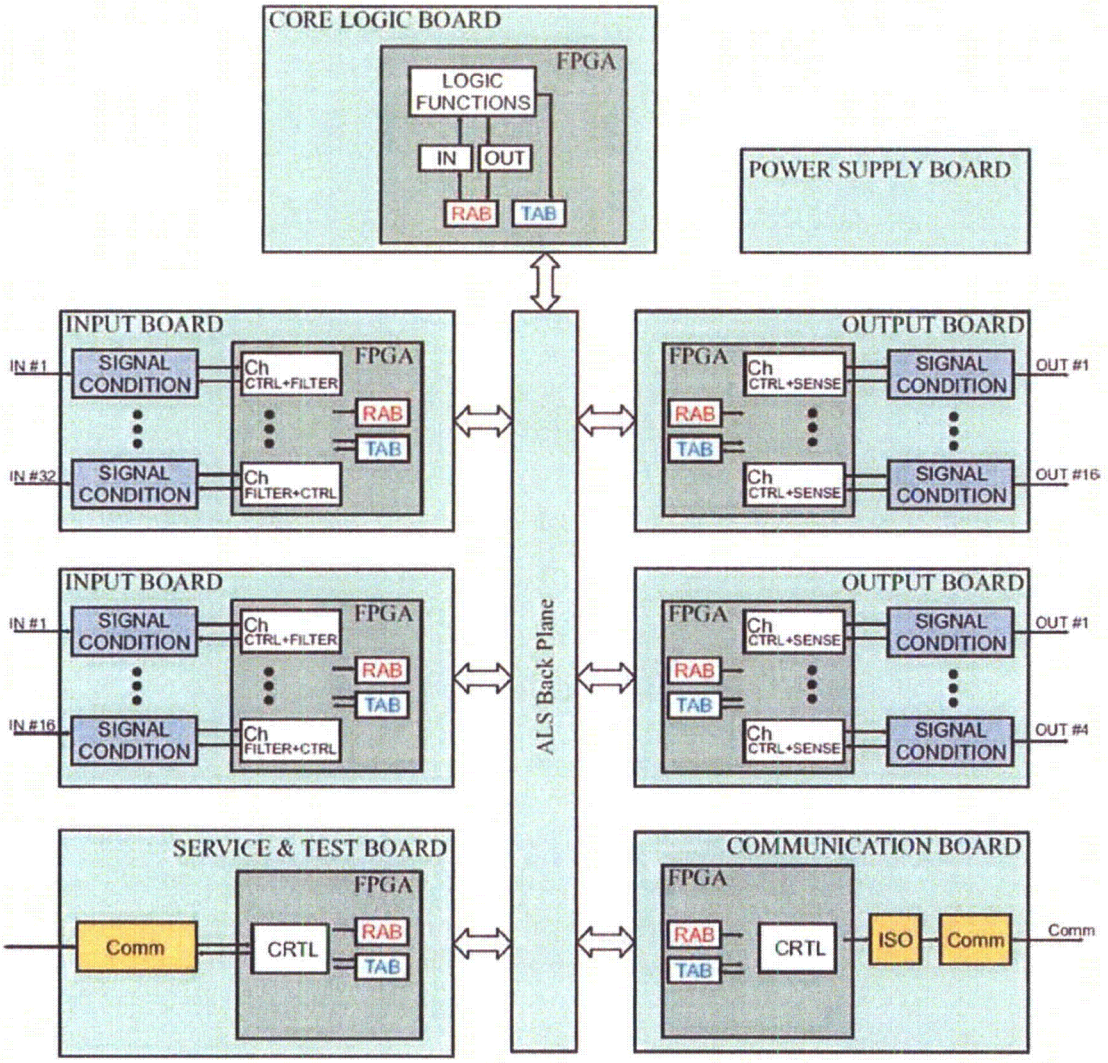

Figure 4-7: Simplified Block Diagram of the ALS

4.5 Design Standards

The TRICON/ALS system has been designed to meet the following recent Standards and Guidance:

IEEE Standard 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

IEEE Standard 308-1980, "Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations"

IEEE Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

IEEE Standard 384-1981, "Standard Criteria for Independence of Class 1E Equipment and Circuits"

EPRI TR-107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants"

Regulatory Guide 1.152, Rev. 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", July 2011

Regulatory Guide 5.71, Rev. 0, "Cyber Security Programs for Nuclear Facilities", January 2010

US NRC, Digital Instrumentation and Controls, Rev. 1, "DI&C-ISG-04, Task Working Group #4: Highly Integrated Control Rooms – Communication Issues (HICR)", March 6, 2009

The hardware and software development process complies with IEEE Standard 603-1991 and IEEE Standard 7-4.3.2-2003. This provides a high quality and well defined development process that results in a quality protection system. The V&V effort and the software configuration control management used for the TRICON/ALS system is consistent with the process and activities that comply with IEEE Standard 7-4.3.2-2003. This ensures that the new system meets the specified functional requirements and criteria, and controls the system and programming throughout its development and use.

Regulatory Guide 1.152 "describes a method that the NRC staff deems acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and a secure development and operational environment for the use of digital computers in the safety systems of nuclear power plants." This Regulatory Guide specifically references IEEE Standard 603-1991 and IEEE Standard 7-4.3.2-2003. Regulatory Guide 5.7.1 "provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1."

Following the current Industry Standards, NRC Regulatory Guides, and industry guidance documents ensures that the replacement PPS will meet the industry's and NRC's design and operational requirements and result in a highly reliable system. Since these requirements are more stringent than those in place when the Eagle 21 system was developed, the TRICON/ALS replacement PPS is expected to meet and exceed the performance of the Eagle 21 system.

5.0 Justification for TS Requirements

[

]^{a,c}

5.1 Overall Comparison of Eagle 21 and TRICON/ALS Systems

The PPS replacement at DCPP is a one for one replacement of the Eagle 21 PPS with the TRICON/ALS PPS. Only the process racks shown in red Figure 5-1 are being replaced, nothing else in the RPS or ESFAS is being changed. Figures 5-2 and 5-3 represent the Eagle 21 PPS concept and the replacement TRICON/ALS PPS concept, respectively.

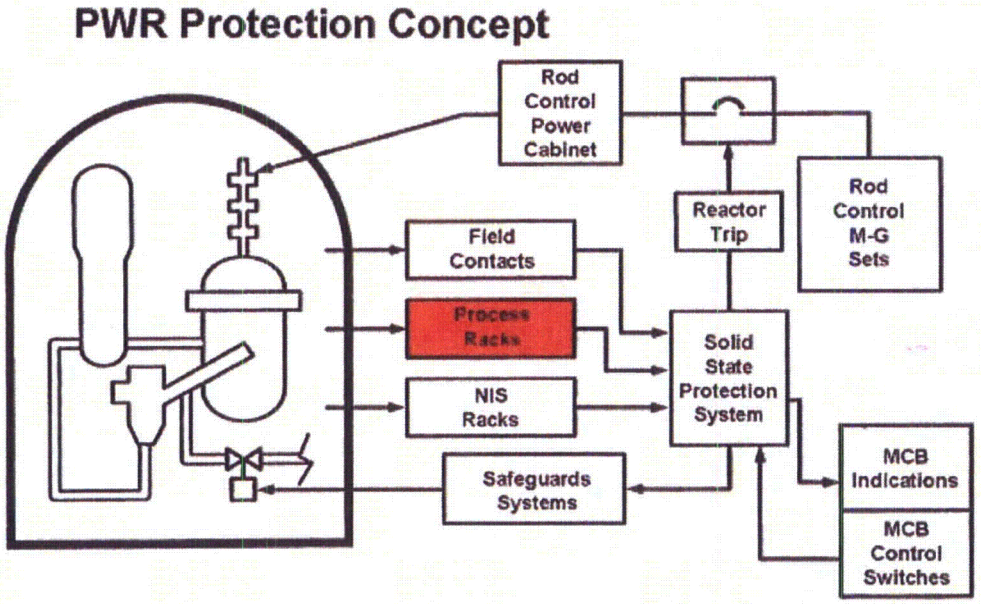

Figure 5-1: Westinghouse PWR Protection Concept (from Reference 8)

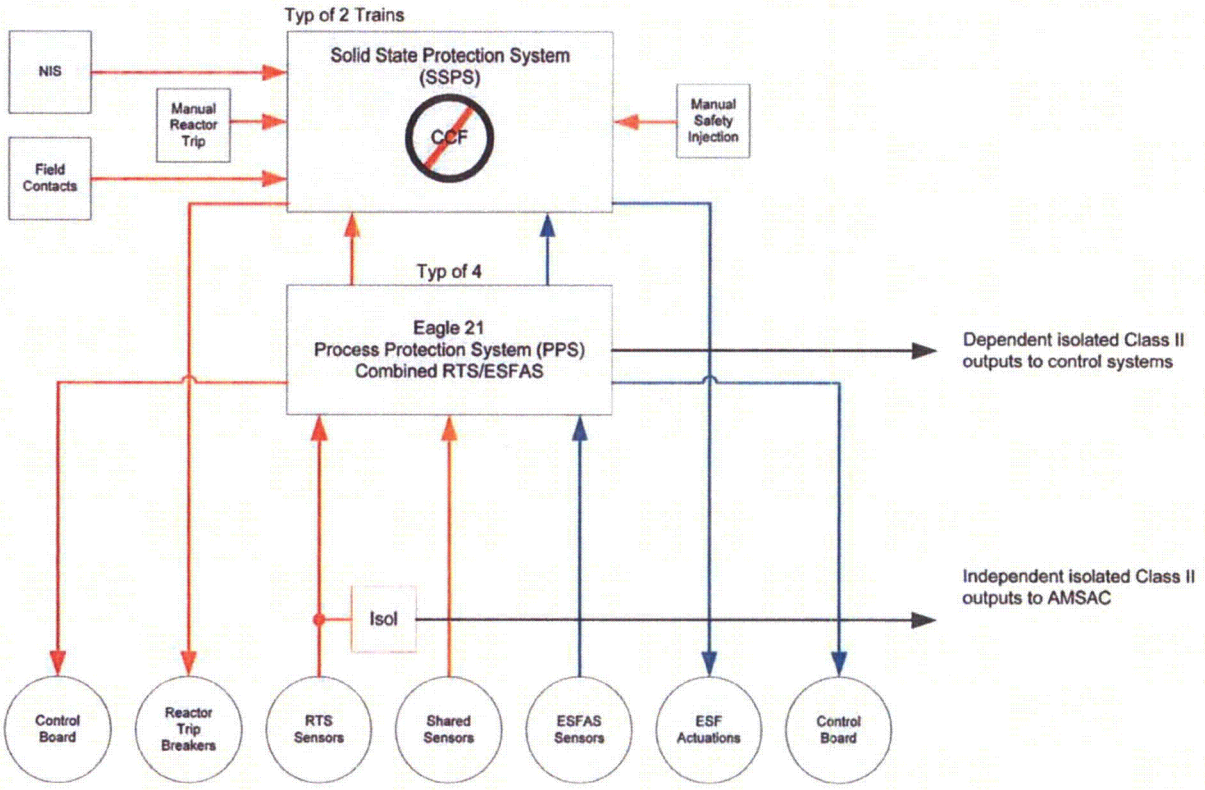

Figure 5-2: Existing Eagle 21 PPS Concept (from Reference 8)

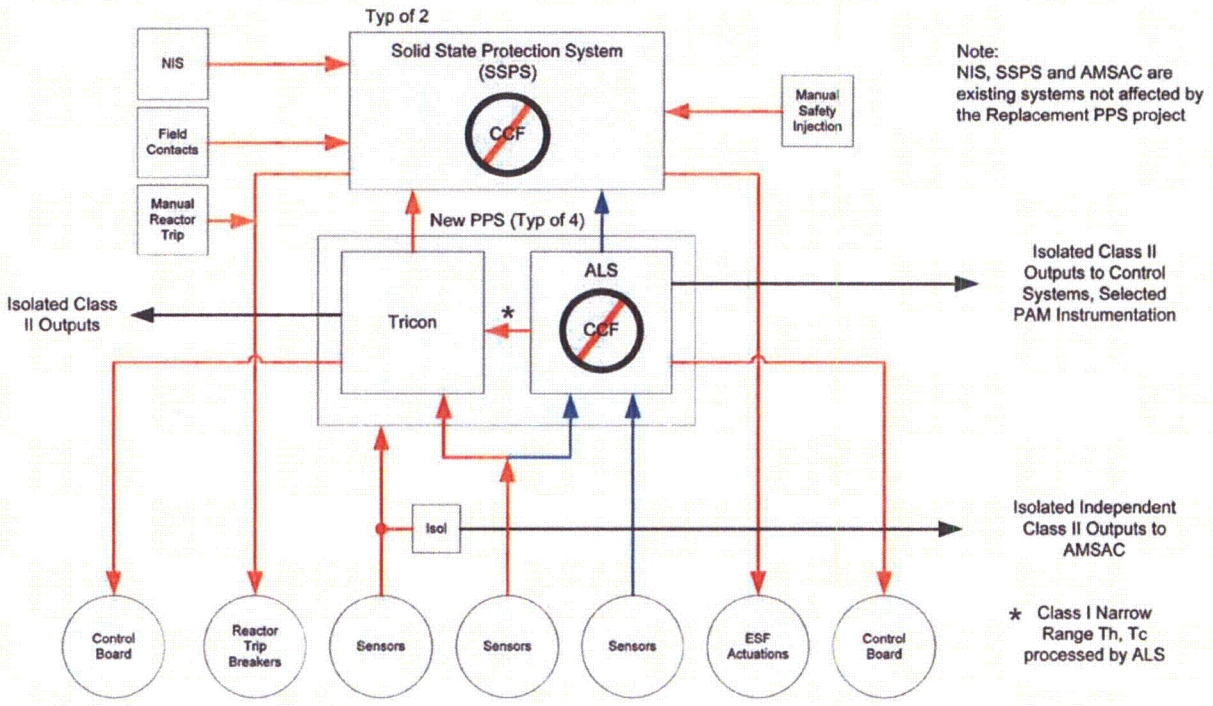

Figure 5-3: Replacement TRICON/ALS PPS Concept (from Reference 8)

[

]a,c

5.2 Qualitative Reliability Assessment of the Eagle 21 System

To qualitatively assess the reliability of the Eagle 21 system, the Eagle 21 Failure Modes and Effects Analysis (FMEA) and the DCPP Eagle 21 Safety Evaluation Report (SER), Reference 10 and Reference 12 respectively, were reviewed and information relevant to signal generation reliability is provided in the following sections.

5.2.1 Eagle 21

The Eagle 21 FMEA (Reference 10) evaluation assessed each circuit card needed to process signals required for the system to perform its safety function. This FMEA was specifically done to address the system time response, but the information is also applicable to signal development. The FMEA did not access the Tester Subsystem or the outputs to various monitoring devices (annunciators, indications, etc.) because these components are not directly related to signal generation and propagation of the signals to the SSPS. The power supply subsystem was not analyzed by itself, but rather with each of its respective circuit cards. Loss of any power supply in Eagle 21 will be detected via indications. The following components were analyzed by the FMEA, see Figure 4-2 for a block diagram of the Eagle 21 System.

Input Boards

- Eagle Analog Input (EAI)
- Eagle RTD Input (ERI)

Loop Processor Subsystem

- Loop Calculation Processor (LCP)
- Digital Filter Processor (DFP)
- Digital/Digital Converter (DDC)
- Digital/Analog Converter (DAC)
- Data Link Handler (DLH)
- Multibus

Output Boards

- Eagle Partial Trip (EPT)

The Eagle 21 FMEA divided each of the cards above into hardware function blocks which were assigned functional failure modes with their respective effects. The FMEA then looked at the associated failures effect on normal operation (board's ability to perform its safety function) and also how/if the failure would be detected (during normal operation which includes self-test features and partial trips) or via automatic tests which are performed during the periodic channel operability test.

The Eagle 21 is equipped with a tester subsystem that monitors the performance of the cabinet and provides access to maintenance routines. Of particular importance for this analysis are failures that are detected by the self-testing features and displayed via alarm or trouble status lights, and also those detected by the periodic channel operability test (done with automatic test feature). The detectable failures are important because if failures are displayed to the operators or maintenance personnel then they would be addressed in a timely manner and the Eagle 21 would be able to perform its intended safety functions. On the other hand, failures that are not detected by the self-test features could remain failed until the system is needed to perform its function or until the next channel operability test. Failures identified by the channel operability test are of particular interest since this program is to determine the appropriate interval for this test. Failures not alarmed automatically and corrected in a timely manner could prevent Eagle 21 from performing its intended safety functions.

The TSP, part of the Eagle 21 tester subsystem, runs diagnostic routines on the Loop Processor Subsystem. The TSP diagnostic alarm algorithms produce the following control room annunciator signals:

- "CHANNEL SET FAILURE" annunciator, when problems develop that cause a channel to be inoperable, such as a loss of both 15-VDC power supplies
- "BYPASS" annunciator, when any EPT channel is in the bypass mode
- TROUBLE status light, when a 15-VDC power supply fails, an input/output board is removed, a cabinet overtemperature condition exists, or other abnormal conditions are discovered by system diagnostic routines

With these key test/alarm features in mind, the Eagle 21 FMEA was reviewed to determine which components in the Eagle 21 system were susceptible to failures that would be detected only by the channel operability test. A summary of this review is provided below.

Input Boards – [

]^{a,c}

Loop Processor Subsystem (LPS) – [

]^{a,c}

Output Boards – [

]^{a,c}

5.2.2 Eagle 21 SER

The Safety Evaluation provided by the NRC noted that the Eagle 21 System utilizes the same software and hardware for all four channels. Because of this Eagle 21 could be subject to common cause failure in redundant equipment. In response to this, DCPP credited mitigating such common cause failures by taking a defense-in-depth approach. This approach involved crediting diverse means to mitigate events that would normally rely on Eagle 21 for primary and/or backup protection. Diverse means to actuate mitigation equipment include the AMSAC system for auxiliary feedwater start and turbine trip, and nuclear instrumentation system signals, direct contact inputs, and operator actions for all other mitigation systems.

5.3 Qualitative Reliability Assessment of the TRICON/ALS System

To qualitatively assess the reliability of the TRICON/ALS systems, the TRICON FMEA (Reference 11) and the ALS FMEAs (References 13 through 18), along with the SER for the DCPP Topical Report on the PPS Replacement Diversity and Defense in Depth Assessment (Reference 19) were reviewed and information relevant to signal generation reliability is provided in the following sections.

5.3.1 TRICON Qualitative Reliability Assessment

The V10 TRICON platform FMEA (Reference 11) is a comprehensive analysis of all chassis and module types used in the generic TRICON design. Because of this, the list below was generated and only includes components that are used for the specific DCPP PPS replacement (Reference 20).

Input Modules:

- Analog Inputs 3703EN and 3721N
- Digital Inputs 3501TN2 and 3503EN2
- Input Termination Panels

Processor/Communication Modules:

- Main processor 3008N

Output Modules:

- Analog Outputs 3805HN
- Digital Outputs 3601TN
- Output Termination Panels

The TRICON self-test features are a strength of the TRICON design and allow the system to identify a high number of system failures without dependence on the channel operability test. Those failures identified by the self-test feature enables corrective action to be taken and the failures can be addressed in a timely manner. This can significantly reduce the length of time a component of the TRICON system can be undetected in a failed state. The microprocessors on each leg test for known or expected signal values within a certain tolerance. If the signals reaching the leg microprocessors are within the allowed tolerance, the leg will self-calibrate its A/D converter to null out any undesirable offsets or gains. Failure of any diagnostic on any leg activates the module fault indicator, which in turn activates the chassis alarm signal. The alarm contact on at least one main chassis power module is actuated when a power module fails, primary power to a power module is lost, low battery condition exists, or power module overtemperature condition exists.

The FMEA was reviewed to identify failures which would prevent the TRICON from performing its safety functions. The FMEA was also reviewed to determine which of these failures would be detected by the self-test features built into the TRICON and which are dependent on the channel operability test. Failures that are not detected by the self-test features could remain failed until the system is needed to perform its function or until the next channel operability test. Failures identified by the channel operability test are of particular interest since this program is to determine the appropriate interval for this test. The failure categories deemed to be important to support this analysis were Category C3a & C3b which are single failure conditions where the PLC is unable to perform all of its safety functions and multiple failure conditions (common cause) where the PLC is unable to perform its safety functions.

With these key test/alarm features in mind, the TRICON FMEA was reviewed to determine which components in the TRICON were susceptible to failures that would be detected only by the channel operability test. A summary of this review is provided below.

Input Modules – [

]^{a,c}

Processor Modules – [

]^{a,c}

Output Modules – [

]^{a,c}

5.3.2 ALS Qualitative Reliability Assessment

The ALS FMEAs (References 13 through 18) provide a "bottom-up" look at each component in order to identify potential failures and their effects at the board level. The following components are used at DCPP and were analyzed in the FMEAs:

Input Boards:

- RTD Input Card ALS-311-1
- Analog Input Card ALS-321-1
- Digital Input Card ALS-302-1

Core Logic Boards:

- Core Logic Board / Communication Card ALS-102

Output Boards:

- Analog Output Card ALS-421-1/2
- Digital Output Card ALS-402-1/2

The ALS has a Built in Self-Test (BIST) and is used for exercising all critical functions within a board. This is done to ensure that latent failures cannot build up in the system and make the system inoperable without the knowledge of plant personnel. The BIST will typically apply input stimuli on the inputs to a sub-circuit and validate the correct response on the output.

The ALS also utilizes an inherent self-test which is a method for implementing high integrity directly into the logic circuits by constructing it in a way that latent STUCK-AT or OPEN failures will be instantly detected.

The detectable failures are important because if failures are displayed to the operators or maintenance personnel then they would be addressed in a timely manner and the ALS would be able to perform its intended safety functions. This reduces the dependence of the ALS system on the operability test to identify failures. However, failures that are not detected by the self-test features could remain failed until the system is needed to perform its function or until the next channel operability test. Failures identified by the channel operability test are of particular interest since this program is to determine the appropriate interval for this test. Failures not alarmed automatically and corrected in a timely manner could prevent ALS from performing its intended safety functions.

With these key test/alarm features in mind, the ALS FMEA was reviewed to determine which components in the ALS were susceptible to failures that would be detected only by the channel operability test. A summary of this review is provided below.

Input Boards – [

]^{a,c}

Core Logic Boards – [

]^{a,c}

Output Boards – [

]^{a,c}

[

]^{a,c}

5.4 Summary of the Defense-in-Depth and Diversity Assessments

The DCPP PPS Replacement Diversity and Defense-in-Depth Assessment (Reference 8) for the TRICON/ALS system considered licensing basis accidents to determine which events required the PPS for primary or backup protection. Those events identified as requiring the PPS for primary protection system response were reviewed to determine if a timely diverse means of automatically mitigating the transient was available or annunciators and indicators were available to allow the operator to diagnose the event and bring the plant to a safe shutdown condition in a timely manner.

It was concluded from this study that for many events, no operator action is required since sufficient non-PPS based automatic functions exist; i.e., the NIS, field contacts, and the AMSAC. For several events, however, some operator action was credited in the NRC Eagle 21 Safety Evaluation Report (Reference 12). In these cases, backup protection system functions, alarms, and indicators processed independent of the PPS, along with existing Diablo Canyon operating procedures and Emergency Operating Procedures, were credited to bring the plant to a safe shutdown condition. Depending upon the event, operator action was required in ten minutes or less.

Per NRC ISG-02, automatic actuation not affected adversely by software CCF is preferred where operator action otherwise would be required to mitigate a FSARU Chapter 15 accident or event with a concurrent CCF. Therefore, where previous evaluations relied upon manual operator action to mitigate several such events, automatic mitigation functions are generated in the independent, inherently diverse ALS portion of the proposed replacement PPS for those events.

The proposed replacement ALS/TRICON PPS design provides defense-in-depth and diversity through monitoring numerous variables by different means such that two or more diverse automatic protective actions terminate each FSARU Chapter 15 event that requires an automatic function before unacceptable consequences can occur. This also applies to the functions credited with manual operator action in the Eagle 21 SER (Reference 12) to mitigate events that occurred with a concurrent postulated CCF to the PPS. This conclusion applies to the proposed replacement PPS even after assuming that CCF disables the computer-based TRICON portion of the replacement PPS while both subsystems of the logic-based ALS portion of the replacement PPS are not affected adversely by the same software CCF, and remain available to perform safety functions automatically.

Therefore, the inherent diversity provided by the logic-based ALS portion of the proposed replacement PPS ensures that all accidents and events credited with automatic PPS mitigation in DCPP FSARU Chapter 15 analyses continue to be mitigated automatically with a concurrent software CCF on the TRICON portion of the PPS. Thus, the proposed PPS provides automatic

mitigation for events that currently require manual protective action should a CCF disable the Eagle 21 primary and backup protection functions.

As documented in Reference 19, the NRC staff has reviewed the DCPP Diversity and Defense-in-Depth Assessment for the proposed digital PPS upgrade. This assessment was performed with the assumption that a software CCF would result in a failure of the TRICON portion of the PPS, but not affect the ALS portion of the PPS. The designed-in diversity of the ALS portion of the proposed replacement PPS ensures that all accidents and events credited with automatic PPS mitigation in the DCPP FSARU Chapter 15 analyses continue to be mitigated automatically with a concurrent software CCF without reliance on other systems or manual operator actions. The NRC staff concluded that the changes being made to the digital PPS do not adversely impact the safety determination that was made for the Eagle 21 digital PPS system. Based on the above, the NRC staff concluded there is adequate diversity and defense-in-depth within the proposed replacement PPS such that the plant responses to the design basis events concurrent with potential software CCF meet the acceptance criteria.

5.5 Comparison of Signals Processed by Eagle 21 vs. TRICON/ALS

The PPS processes a number of inputs from the plant's sensors which monitor parameters, such as pressure, temperature, and neutron flux, to provide inputs to the solid state protection system. The SSPS then does the combinational logic to trip the reactor or actuate safety functions. With the current system, the signal processing is done by the Eagle 21 system or the NIS. With the TRICON/ALS system the processing is done by the TRICON System, ALS system, or the NIS.

The function and signals that initiate the safety systems required for the DCPP safety analyses are provided in the DCPP Technical Specifications. Table 5-1 provides a summary of the signal processing for the reactor trip signals, that is, is the signal processed by the Eagle 21 system, NIS, TRICON System, or ALS system and Table 5-2 provides a similar summary for the engineered safety features actuation signals. This is provided only for the automatic actuation signals.

[

]^{a,c}

[

]a,c

Table 5-1: Reactor Trip Actuation Signals – Signal Processing		
Technical Specification Function	**Eagle 21 System**	**TRICON/ALS System**
2. a. Power range neutron flux – high	NIS	NIS
2.b. Power range neutron flux - low	NIS	NIS
3. a. Power range neutron flux rate – high positive rate	NIS	NIS
3.b. Power range neutron flux rate – high negative rate	NIS	NIS
4. Intermediate range neutron flux	NIS	NIS
5. Source range neutron flux	NIS	NIS
6. Overtemperature ΔT	NIS, Eagle 21	NIS, TRICON
7. Overpower ΔT	NIS, Eagle 21	NIS, TRICON
8.a. Pressurizer pressure - low	Eagle 21	ALS
8.b. Pressurizer pressure - high	Eagle 21	ALS
9. Pressurizer water level - high	Eagle 21	TRICON
10. Reactor coolant flow - low	Eagle 21	ALS
11. Reactor coolant pump breaker position	Existing Class II Contacts	Existing Class II Contacts
12. Undervoltage reactor coolant pumps	Existing Class II Contacts	Existing Class II Contacts
13. Underfrequency reactor coolant pumps	Existing Class II Contacts	Existing Class II Contacts
14.a. Steam generator water level – low-low	Eagle 21	TRICON
14.b. Steam generator water level – low-low trip time delay	Eagle 21	TRICON
15. not used	--	--
16.a. Turbine trip – low auto-stop oil pressure	Existing Class II Contacts	Existing Class II Contacts
16.b. Turbine trip – turbine stop valve closure	Existing Class II Contacts	Existing Class II Contacts

Table 5-2: Engineered Safety Features Actuation Signals – Signal Processing		
Technical Specification Function	**Eagle 21 System**	**TRICON/ALS System**
1. Safety injection on:		
c. Containment pressure – high	Eagle 21	ALS
d. Pressurizer pressure – low	Eagle 21	ALS
e. Steam line pressure – low	Eagle 21	TRICON
2. Containment spray on:		
c. Containment pressure – high-high	Eagle 21	ALS
3. Containment isolation on:		
b. Phase B isolation on: 3. Containment pressure - high-high	Eagle 21	ALS
4. Steam line isolation on:		
c. Containment pressure – high-high	Eagle 21	ALS
d.1. Steam line pressure - low	Eagle 21	TRICON
d.2. Steam line pressure – negative rate - high	Eagle 21	TRICON
5. Feedwater isolation		
b. SG water level – high-high	Eagle 21	TRICON
6. Auxiliary feedwater		
d.1. SG water level – low-low	Eagle 21	TRICON
d.2. SG water level - low-low trip time delay	Eagle 21	TRICON
g. Undervoltage reactor coolant pump	Existing Class II Contacts	Existing Class II Contacts
7. Residual heat removal pump trip		
On refueling water storage tank level - low	Process Control System (not PPS)	Process Control System (not PPS)

5.6 Qualitative Reliability Assessment Comparison

The previous sections discussed the methods of detecting failures of the Eagle 21 and TRICON/ALS systems and also the diversity of signals available to actuate mitigation systems. From this it is concluded:

[

]^{a,c}

From this it is concluded that the TRICON/ALS system is expected to be as reliable or more reliable than the Eagle 21 system.

5.7 Demonstration of the Applicability of the WCAP-14333 and WCAP-15376 Analyses

As previously noted, implementation guidelines were developed for utilities to follow when implementing the TS changes justified in WCAP-14333-P-A, Rev. 1 and WCAP-15376-P-A, Rev. 1 at their plants. The purpose of these guidelines was to 1) demonstrate that the plant is built and operated consistent with the analysis supporting the proposed changes and 2) provide guidance on how to address the Limitations and Conditions the NRC Staff imposed.

As previously discussed, PG&E previously implemented the WCAP-14333-P-A and WCAP-15376-P-A TS changes at DCPP. For implementation, the Conditions and Limitations (C&L) the NRC provided for each WCAP were addressed, except for Condition #5 for WCAP-15376-P-A which was not applicable. The following re-establishes the applicability of the WCAP analyses to the DCPP RPS with the TRICON/ALS PPS by again addressing the Conditions and Limitations provided in the NRC's Safety Evaluation.

5.7.1 Applicability of WCAP-14333-P-A, Rev. 1

The Staff's Safety Evaluation on WCAP-14333-P included the following two Conditions. Note that the NRC's Safety Evaluation is included in WCAP-14333-P-A, Rev. 1 which is the approved version of the WCAP.

1. Confirm the applicability of the WCAP-14333-P analyses for their plant.
2. Address Tier 2 and 3 analyses including the Configuration Risk Management Program insights, by confirming that these insights are incorporated into the referencing licensee's decision making process before taking equipment out of service.

WCAP-14333-P-A, Condition 1: The implementation guidance to address Condition #1 consists of three tables (Reference 6). The first table addresses general parameters related to the test intervals, including channel calibration interval and component maintenance intervals, and several plant specific values related to core damage frequency and transient event frequency, and AMSAC actuation of auxiliary feedwater. The second table addresses the RPS signals available to trip the reactor for the various initiating events. The WCAP-14333 analysis made assumptions regarding the availability of reactor trip signals for the different initiating events; for some events a reactor trip signal is not required, for some events only a non-diverse signal will be available, and for other events diverse signals will be available. Assumptions were also made with regard to the availability of operator actions to trip the reactor for these events. The third table addresses the actuation signals available to initiate the ESF for the various events. The safety features included safety injection, auxiliary feedwater pump start, main feedwater isolation, steamline isolation, containment spray actuation, containment isolation, and containment cooling. The WCAP-14333 analysis made assumptions regarding the availability of ESF actuation signals for the different initiating events. Again, assumptions were also made with regard to the availability of operator actions to initiate the safety systems for these events. For the WCAP analyses to be applicable, the plant must be built and operated consistent with these assumptions.

Since this WCAP extended the CT and bypass test times, the associated maintenance and test intervals are important to determining the unavailability of components of the RPS and how these unavailability values change with the increased CTs and bypass test times. The test intervals used in the analysis were consistent with the values justified in WCAP-10271, with Supplements 1 and 2. Since WCAP-14333 only changed the CT and bypass test times for the RPS, how often the components are subject to test and maintenance activities is important to the unavailability of the components and the risk impact. Replacing the Eagle 21 system with

the TRICON/ALS system only impacts the channels of the PPS, therefore, only the channel parameters are of interest now. The WCAP-14333 analysis was based on channel parameters of:

- Test interval – 3 months
- Calibration interval – 18 months
- Maintenance interval – 24 months

Table 5-3 compares the plant specific parameters against those used in the WCAP analysis. Since the DCPP has a SSPS, the parameters related to a relay protection system are marked as not applicable (NA). Other parameters not associated with the PPS are not important to this assessment and are marked as "Not impacted by the PPS change". The information provided on this table indicates that the listed parameters at DCPP with the TRICON/ALS system are consistent with the WCAP-14333-P-A analysis.

Table 5-4 compares the reactor trip signals and operator actions to trip the reactor credited, or assumed to be available, in the WCAP-14333-P-A analysis against those signals available in DCPP. "Agree" listed in the table for DCPP indicates that the plant design and operation is consistent with this analysis, that is, the noted reactor trip signals are available at a minimum. The information provided on this table indicates that the reactor trip signals and backup operator actions at DCPP with the TRICON/ALS system are consistent with the WCAP-14333-P-A analysis.

Table 5-5 compares the ESF actuation signals and operator actions to initiate safeguards equipment credited, or assumed to be available, in the WCAP-14333-P-A analysis against those signals available in DCPP. "Agree" listed in the table for DCPP indicates that the plant design and operation is consistent with this analysis, that is, the noted ESF actuation signals and backup operator actions are available at a minimum. The information provided on this table indicates that the listed parameters at DCPP with the TRICON/ALS system are consistent with the WCAP-14333-P-A analysis.

From this it is concluded that the analysis supporting WCAP-14333-P-A is applicable to DCPP.

WCAP-14333-P-A, Condition 2: The Tier 2 and 3 analyses and insights are not impacted. The same Tier 2 requirements identified in WCAP-14333-P-A (WOG response to RAI #18) remain applicable. These are related to the logic cabinets which are not impacted by the proposed change. Since the proposed change is full replacement of the Eagle 21 PPS with the TRICON/ALS system, and the test and maintenance activities on the TRICON/ALS system will be completed consistent with the approach used for the Eagle 21 system, and consistent with the WCAP-14333 assumptions and TS requirements, one train at a time, no additional Tier 2 requirements are required. With regard to Tier 3 analyses and insights, Tier 3 evaluations will continue to be done consistent with the DCPP process defined in AD7.DC6 "On-Line Maintenance Risk Management".

Conclusion: Based on the above discussion, it is concluded that the WCAP-14333 CT, bypass test time, and STI changes for the channels are applicable to the DCPP RPS with the TRICON/ALS PPS.

5.7.2 Applicability of WCAP-15376-P-A, Rev. 1

The Staff's Safety Evaluation on WCAP-15376-P included the following five Conditions and Limitations (C&L), and one additional C&L:

1. A licensee is expected to confirm the applicability of the topical report to their plant, and to perform a plant-specific assessment of containment failures and address any design or performance differences that may affect the proposed changes.
2. Address the Tier 2 and Tier 3 analyses including risk significant configuration insights and confirm that these insights are incorporated into the plant-specific configuration risk management program.
3. The risk impact of concurrent testing of one logic cabinet and associated reactor trip breaker needs to be evaluated on a plant-specific basis to ensure conformance with the WCAP-15376-P, Rev. 0 evaluation, and RGs 1.174 and 1.177 guidance.
4. To ensure consistency with the reference plant, the model assumptions for human reliability in WCAP-15376, Rev. 0 should be confirmed to be applicable to the plant-specific configuration.
5. For future digital upgrades with increased scope, integration and architectural differences beyond that of Eagle 21, the staff finds the generic applicability of WCAP-15376-P, Rev. 0 to future digital systems not clear and should be consistent on a plant-specific basis.

WCAP-15376-P Additional Commitment: Each plant must confirm that their RTS and ESFAS setpoint analysis uncertainty assumptions, including drift, remain valid for extending the frequency of the COT from 3 months to 6 months.

WCAP-15376-P-A, C&L 1 (First Part – Confirm the Applicability of the WCAP Analysis):
[

]^{a,c}

[

]a,c

[

]a,c

From this it is concluded that the analysis supporting WCAP-15376-P-A is applicable to DCPP.

WCAP-15376, C&L 1 (Second Part - Confirm the Applicability of the Component Failure Probabilities): [

]a,c

WCAP-15376, C&L 1 (Third Part – Containment Failure Assessment): [

]a,c

WCAP-15376, C&L 2: The Tier 2 and 3 analyses and insights are not impacted. The same Tier 2 requirements identified in Sections 8.5 and 8.6 of WCAP-15376-P-A remain applicable. These are related to the RTBs and logic cabinets which are not impacted by the proposed change. Since the proposed change is full replacement of the Eagle 21 PPS with the TRICON/ALS system, and the test and maintenance activities on the TRICON/ALS system will be completed consistent with the approach used for the Eagle 21 system, and consistent with the WCAP-15376 assumptions and TS requirements, one train at a time, no additional Tier 2 requirements are required. With regard to Tier 3 analyses and insights, Tier 3 evaluations will continue to be done consistent with the DCPP process defined in AD7.DC6 "On-Line Maintenance Risk Management".

WCAP-15376, C&L 3: Concurrent testing of a logic cabinet and the associated reactor trip breaker is not impacted by the PPS change. Therefore, the risk impact on a plant specific basis does not need to be re-evaluated.

WCAP-15376, C&L 4: [

]a,c

WCAP-15376, C&L 5: This document specifically addresses the applicability of these changes to the TRICON/ALS PPS.

WCAP-15376-P, Additional Commitment: A separate study on setpoint drift is being performed for DCPP with the TRICON/ALS PPS to address drift related issues.

Table 5-3: WCAP-14333 Implementation Guidelines: Applicability of the Analysis General Parameters		
Parameter	**WCAP-14333 Analysis Assumptions**	**DCPP Specific Parameter**
Logic Cabinet Type (1)	Relay and SSPS	SSPS
Component Test Intervals (2)		
• Analog channels	3 months	3 or 6 months (See Note 10)
• Logic cabinets (SSPS)	2 months	Not impacted by the PPS change
• Logic cabinets (Relay)	1 month	NA
• Master Relays (SSPS)	2 months	Not impacted by the PPS change
• Master Relays (Relay)	1 month	NA
• Slave Relays	3 months	Not impacted by the PPS change
• Reactor trip breakers	2 months	Not impacted by the PPS change
Analog Channel Calibrations (3)		
• Done at-power	yes	Yes (See Note 11)
• Interval	18 months	18 months (See Note 11)
Typical At-Power Maintenance Intervals (4)		
• Analog channels	24 months	$\geq$24 months (See Note 12)
• Logic cabinets (SSPS)	18 months	Not impacted by the PPS change
• Logic cabinets (Relay)	12 months	NA
• Master relays (SSPS)	infrequent (5)	Not impacted by the PPS change
• Master relays (Relay)	infrequent (5)	NA
• Slave relays	infrequent (5)	Not impacted by the PPS change
• Reactor trip breakers	12 months	Not impacted by the PPS change
AMSAC (5)	Credited for AFW pump start	Yes

Table 5-3: WCAP-14333 Implementation Guidelines: Applicability of the Analysis General Parameters		
Parameter	**WCAP-14333 Analysis Assumptions**	**DCPP Specific Parameter**
Total Transient Event Frequency (6)	3.6	1.73
ATWS Contribution to CDF (current PRA model) (7)	8.4E-06	1.48E-07/yr
Total CDF from Internal Events (current PRA model) (8)	5.8E-05	1.08E-05/yr
Total CDF from Internal Events (IPE) (9)	Not Applicable	7.9E-05/yr

Notes for Table 5-3:

1. Indicate type of logic cabinet; SSPS or Relay (both are included in WCAP-14333).
2. Fill in applicable test intervals. If the test intervals are equal to or greater than those used in WCAP-14333, the analysis is applicable to your plant.
3. Indicate if channel calibration is done at-power and, if so, fill in the interval. If channel calibrations are not done at-power or if the calibration interval is equal to or greater than that used in WCAP-14333, the analysis is applicable to your plant.
4. Fill in the applicable typical maintenance intervals or fill in "equal to or greater than" or "less than". If the maintenance intervals are equal to or greater than those used in WCAP-14333, the analysis is applicable to your plant.
5. Indicate if AMSAC will initiate AFW pump start. If yes, then the WCAP-14333 analysis is applicable to your plant.
6. Include total frequency for initiators requiring a reactor trip signal to be generated for event mitigation. This is required to assess the importance of ATWS events to CDF. Do not include events initiated by a reactor trip.
7. Fill in the ATWS contribution to core damage frequency (from at-power, internal events). This is required to determine if the ATWS event is a large contributor to CDF.
8. Fill in the total CDF from internal events (including internal flooding) for the most recent PRA model update. This is required for comparison to the NRC's risk-informed CDF acceptance guidelines.
9. Fill in the total CDF from internal events from the IPE model (submitted to the NRC in response to Generic Letter 88-20). If this value differs from the most recent PRA model update CDF provide a concise list of reasons, in bulletized form, describing the differences between the models that account for the change in CDF.
10. The current channel test interval is 6 months following implementation of WCAP-15376-P-A, Rev. 1. When WCAP-14333-P-A, Rev. 1 was implemented, the test interval was 3 months.
11. Channel calibrations are done either at-power or during shutdown on a $\geq$ 18 month basis.
12. Based on the assessment of the reliability of the channels provided in the previous section, the maintenance interval per channel is expected to be greater than 24 months.

Table 5-4: WCAP-14333 Implementation Guidelines: Applicability of Analysis Reactor Trip Actuation Signals

a,c

[

]^{a,c}

Table 5-5: WCAP-14333 Implementation Guidelines: Applicability of Analysis Engineered Safety Features Actuation Signals

a,c

Table 5-5: WCAP-14333 Implementation Guidelines: Applicability of Analysis Engineered Safety Features Actuation Signals

a,c

Table 5-6: WCAP-15376 Implementation Guidelines: Applicability of the Analysis General Parameters

a,c

Table 5-6: WCAP-15376 Implementation Guidelines: Applicability of the Analysis General Parameters

a,c

Table 5-7: WCAP-15376 Implementation Guidelines: Applicability of the Human Reliability Analysis

a,c

6.0 Conclusions

The following is concluded about the reliability of the TRICON/ALS PPS compared to the Eagle 21 PPS.

[

]^{a,c}

From this it is concluded that the TRICON/ALS system is expected to be as reliable as or more reliable than the Eagle 21 system with respect to its protection function.

The following is concluded about the applicability of the WCAP-14333-P-A and WCAP-15376-P-A CT, bypass test time, and STI TS changes to the TRICON/ALS PPS.

- As stated above, the TRICON/ALS system is expected to be as or more reliable than the Eagle 21 system with respect to its protection function.

- The analysis supporting the changes approved in WCAP-14333-P-A, CT and bypass test time changes for the PPS, remains applicable to the DCPP RPS with the change to the TRICON/ALS PPS.
- The analysis supporting the changes approved in WCAP-15376-P-A, STI changes for the PPS, remains applicable to the DCPP RPS with the change to the TRICON/ALS PPS.

From this it is concluded that the following TS parameters are applicable DCPP RPS with the TRICON/ALS PPS.

- Channel Operability Test Interval – 6 months
- Channel Completion Time – 72 hours
- Channel Bypass Test Time – 12 hours

7.0 References

1. "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," WCAP-10271-P-A, May 1986.
2. "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System, Supplement 1," WCAP-10271, Supplement 1-P-A, May 1986.
3. "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP-10271-P-A, Supplement 2, Revision 1, May 1989.
4. "Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times," WCAP-14333-P-A, Rev. 1, October 1998.
5. "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," WCAP-15376-P-A, Rev. 1, March 2003.
6. WOG-98-245, "Implementation Guideline for WCAP-14333-P-A, Rev. 1 (Proprietary), 'Probabilistic Risk Analysis of the RPS and ESFAS Test Times and Completion Times'", December 2, 1998.
7. WOG-04-233, "Transmittal of Revised Implementation Guidelines for WCAP-15376-P-A, Rev. 1, 'Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times'", May 6, 2004.
8. Pacific Gas and Electric Company Topical Report, "Process Protection System Replacement, Diversity & Defense-in-Depth Assessment", Revision 1, August 2010.
9. 6002-00026, CS Innovations Document, "ALS Platform Overview", Revision 1, July 29, 2008.
10. RE-034/94, Westinghouse Document, "Transmittal of EAGLE 21 Time Response FMEAs", May 12, 1994.
11. 9600164-531 (-NP), "Failure Modes and Effects Analysis (FMEA) for the TRICON Version 10.2 Programmable Logic Controller", Revision 1.2, August 3, 2012.
12. ML022350074, Enclosure 3, "Safety Evaluation Report By The Office Of Nuclear Reactor Regulation Related To Amendment No. 84 To Facility Operating License No. DPR-80 and Amendment No. 83 To Facility Operating License No. DPR-82 Eagle 21 Reactor Protection System Modification with Bypass Manifold Elimination, Pacific Gas and Electric Company, Diablo Canyon Power Plant, Units 1 And 2, Docket 50-275 and 50-323", October 7, 1993.
13. 6002-10212, CS Innovations Document, "ALS-102 FPA FMEA and Reliability Analysis", Revision 2, October 8, 2012.
14. 6002-30212, CS Innovations Document, "ALS-302 FPA, FMEA, and Reliability Analysis", Revision 2, October 8, 2012.
15. 6002-31112, CS Innovations Document, "ALS-311 FPA FMEA and Reliability Analysis", Revision 2, October 11, 2012.
16. 6002-32112, CS Innovations Document, "ALS-321 FPA FMEA and Reliability Analysis", Revision 2, October 8, 2012.

17. 6002-40212, CS Innovations Document, "ALS-402 FPA FMEA and Reliability Analysis", Revision 2, October 8, 2012.

18. 6002-42112, CS Innovations Document, "ALS-421 FPA FMEA and Reliability Analysis", Revision 2, October 11, 2012.

19. "Safety Evaluation Report By The Office Of Nuclear Reactor Regulation Regarding Diablo Canyon Power Plant, Units 1, and 2 Topical Report "Process Protection System Replacement Diversity & Defense-in-Depth Assessment", Docket NOS. 50-275 and 50-323, April 19, 2011.

20. DIT-50072308-28-00, Design Input Transmittal, Email from R. Schaffer to J. Hefler dated October 18, 2012 for list of Invensys components used for the DCPP PPS replacement.

21. ML120900889, "Final Safety Evaluation for Invensys Operations Management 'TRICONEX Topical Report' (TAC No. ME2435)", April 12, 2012.