DIABLO CANYON POWER PLANT
PROCESS PROTECTION SYSTEM REPLACEMENT

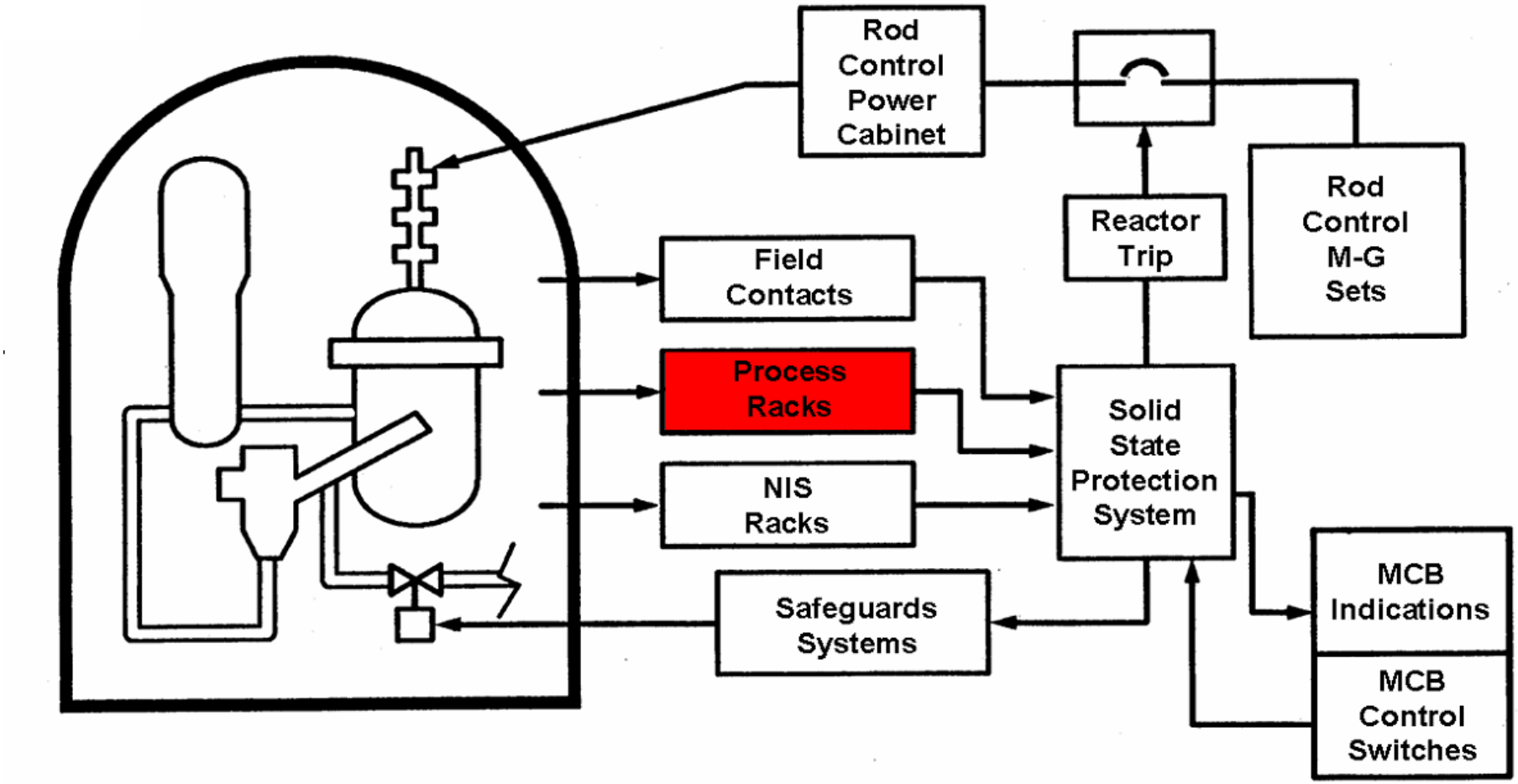
Scott B. Patterson, PE, PMP
Pacific Gas & Electric Co.
Avila Beach, CA
sbp1@pge.com
805-545-4082

John W. Hefler, PE
Altran Solutions Corp.
San Francisco, CA
jhefler@altransolutions.com
415-543-6111

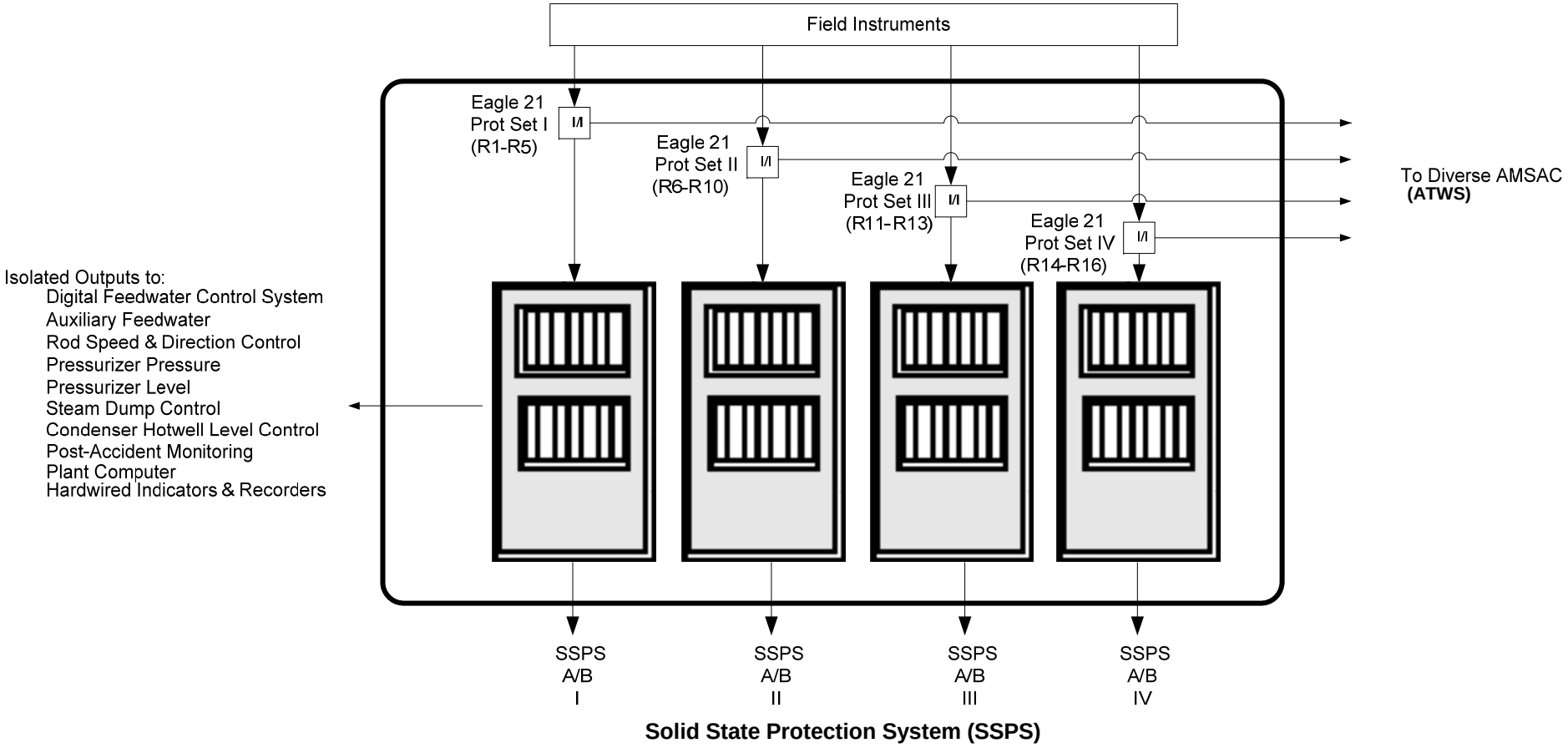
Agenda

- Scope of project
- Eagle-21 Replacement Platform
- Diversity and Defense in Depth
- Cyber Security
- Communications
- PG&E LAR and Schedule

Project Scope

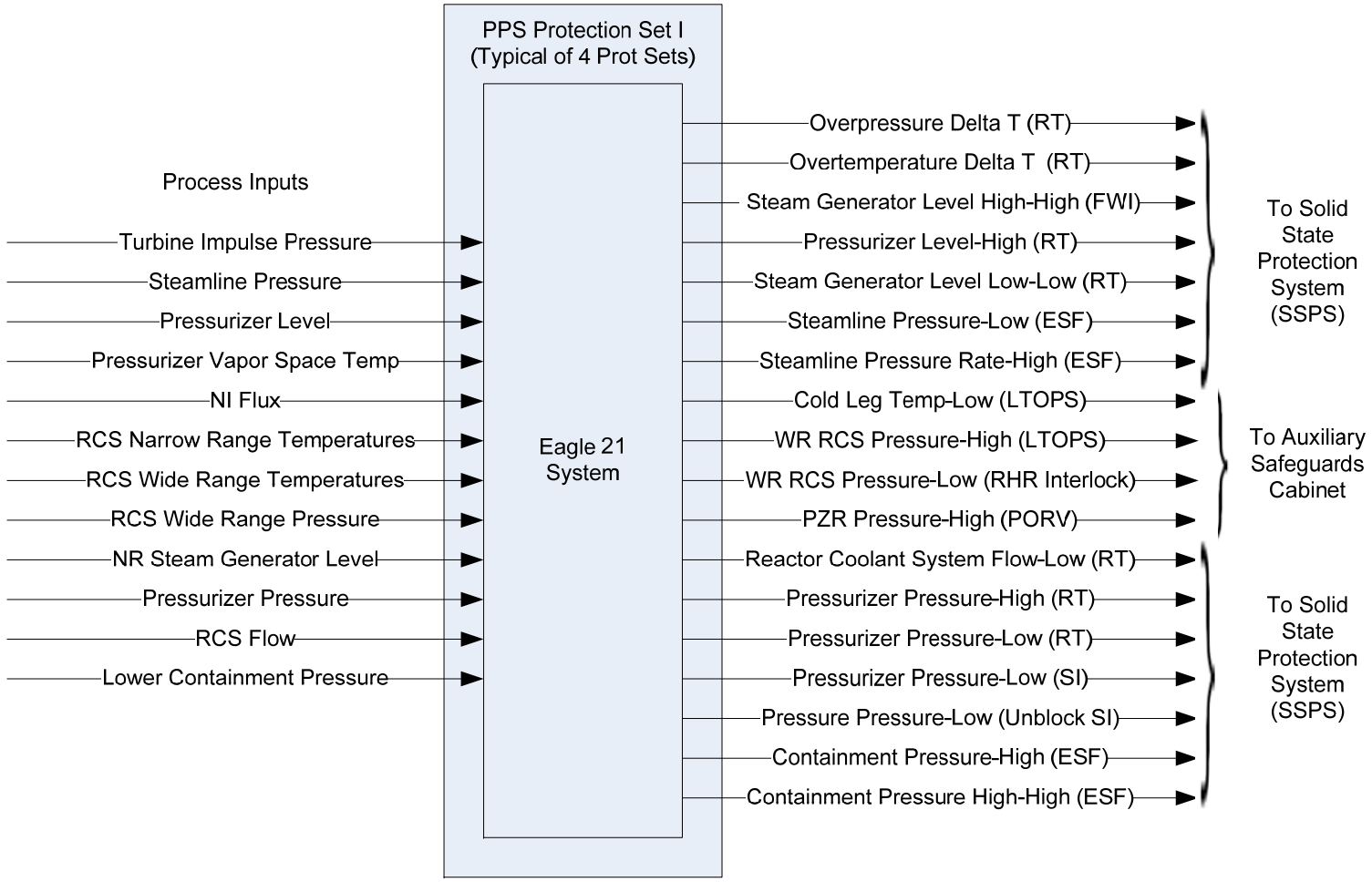


Diablo Canyon Eagle 21 PPS



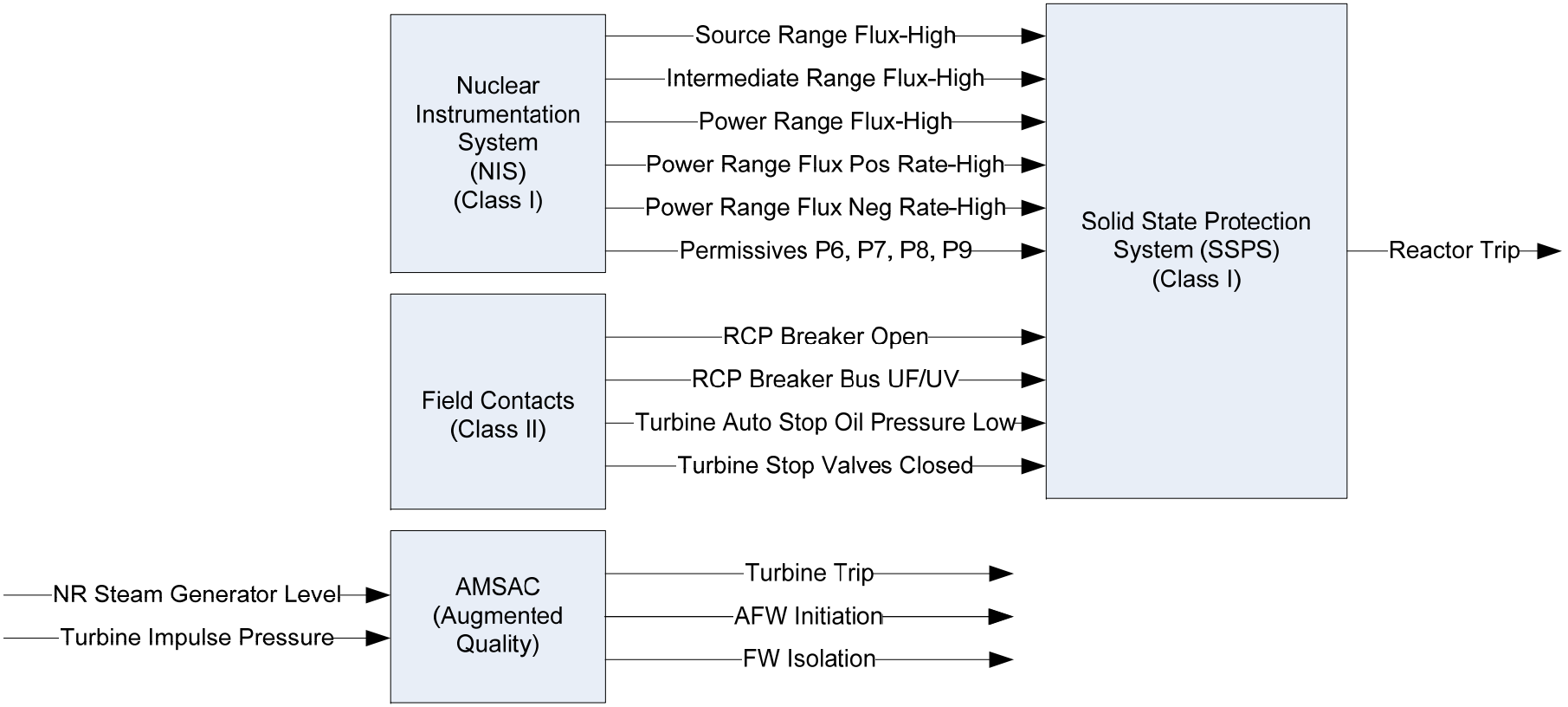
Note – Protection Set and Division can be interchanged

Typical Eagle 21 Protection Set



Note – Protection Set and Division can be interchanged

Diverse Equipment Not Subject to Common Cause Failure (CCF)
(Unaffected by Replacement PPS Project)



Replacement Process Protection System (PPS) Licensing Concept

- Start with Eagle 21 Safety Evaluation Report (SER) for Diablo Canyon
- Determine differences between the SER and current Diversity and Defense-in-Depth Guidance (USNRC ISG #2)
- Develop approach that addresses ISG #2 guidance with minimal impact on existing protection system design

Existing FSAR Chapter 15 Event Analyses That Take Credit for Manual Operator Action

(where both primary and backup protection are in Eagle 21)

- Loss of Forced Reactor Coolant Flow, Locked Rotor (Single loop > P8)
  - Operator action within 5 minutes – Reactor Trip
  - Mitigating function is RCS Flow
- Loss of Coolant Accidents (SBLOCA, LBLOCA)
  - Operator action within 10 minutes – Safety Injection and Containment Spray
  - Mitigating functions are Pressurizer Pressure and Containment Pressure

ISG-02 Guidance

- ISG-02 Section 5 states that there are two design attributes that are sufficient to eliminate consideration of CCF:
  - "(1) Diversity …[if] sufficient diversity exists in the protection system such that the common cause failures within channels can be considered to be fully addressed without further action…no additional diversity would be necessary in the safety system.
  - "(2) Testability - A system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses.

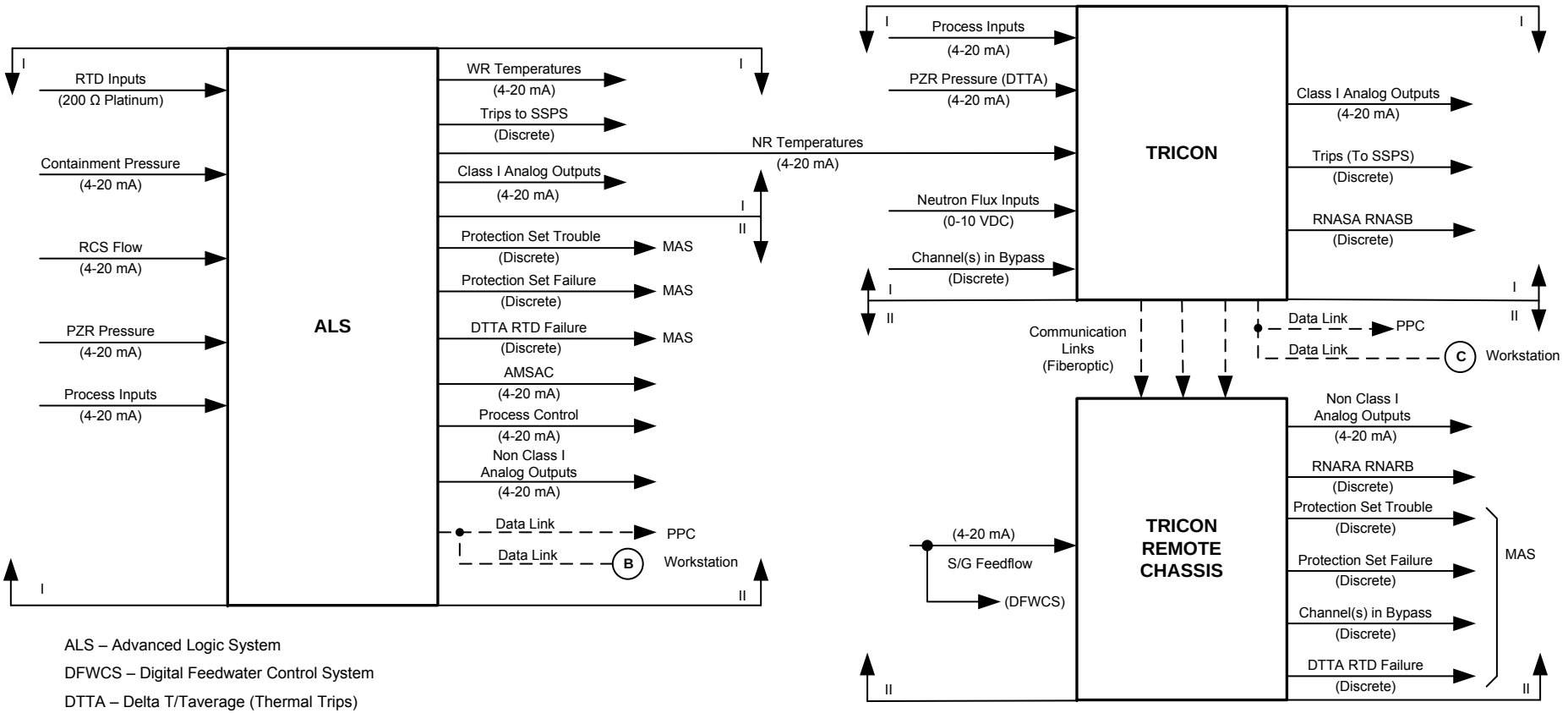
Proposed Replacement PPS Addresses CCF Without an Additional DAS or Manual Actions

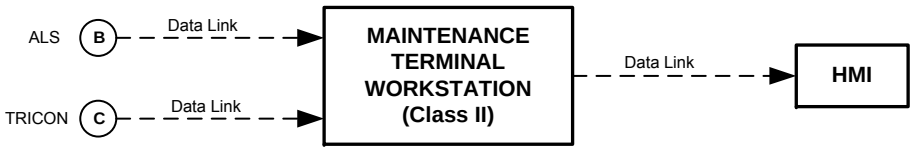
- The Control System Innovations Advanced Logic System (ALS) architecture is internally diverse, logic-based and is not susceptible to CCF due to software.
  - Implements key design attributes, which (when combined with appropriate application development V&V) are sufficient to address Common Cause Failure issues.
- The Tricon architecture is software-based; CCF must be considered and addressed.
  - Sufficient external, automatic diverse functions exist for channels processed through Tricon (Unchanged from Diablo Canyon Eagle 21 SER).
  - Functions previously credited with automatic mitigation in the Diablo canyon Eagle 21 SER continue to be mitigated automatically.
- Provides controls and indications unaffected by CCF (BTP 7-19 Position 4):
  - Independent of any digital software processing
  - Isolated as needed to prevent potential control/protection interaction
- The proposed replacement automates the three functions previously credited for manual mitigation in the Eagle 21 SER.
  - *Eliminating manual actions enhances safety.*

Replacement PPS Concept

(ALS Provides Inherently Diverse Front-End Isolation and Actuation)

Note: SSPS & AMSAC are original equipment; not being replaced.





ALS – Advanced Logic System
DFWCS – Digital Feedwater Control System
DTTA – Delta T/Taverage (Thermal Trips)
HMI – Human Machine Interface
PPC – Plant Process Computer
PZR – Pressurizer
RNARA/RNARB – Auxiliary Relay Cabinets
RTD – Resistance Temperature Detector
RCS – Reactor Cooling System
SSPS – Solid State Protection System
WR – Wide Range

Cyber Security – ISG-01

- Diablo Canyon is responsible to ensure compliance with the applicable cyber security regulations and guidance during all life cycle phases of the plant upgrade following 10 CFR 73.54, Regulatory Guide 1.152 Rev. 2 and ISG-01.
- Applicable to:
  - Vendor equipment software development
  - Diablo Canyon software development and maintenance
- Two Vendors have been selected
  - Invensys - Tricon
  - CS Innovations (CSI) - Advanced Logic System

Cyber Security Summary

- Diablo Canyon intends to fully comply with the applicable guidance on cyber security both for the vendor design program (offsite) and the onsite installation, testing and later phases as called for in NRC Reg. Guide 1.152, ISG-01 and the applicable Regulations.

ISG-04, Highly Integrated Control Rooms – Communications Issues

- Four Areas of Interest
  1. Interdivisional Communications
     - Area of Interest is listed as Data Communications
  2. Command Prioritization
  3. Multidivisional Control & Display Stations
  4. Digital System Network Configuration
     - This is only referenced in the Appendix of ISG-04 as integrated w/ other sections

Data Communications

- Safety-to-non-Safety digital communication interfaces:
  - Plant Process Computer (PPC) – obtains data from all four divisions (read only)
    - Currently this is an analog out from Eagle 21 and an analog in to the PPC (less accurate, requires calibrations, not all desired parameters available)
  - Maintenance Video Display Unit (MVDU) – one per division (read/write)

Data Communications

- MVDU – Maintenance Video Display Unit
  - Functions
    - Removing a channel from service (bypass, trip, defeat alarms, etc.)
    - Updating specific tunable parameters
    - Calibrating Analog and Digital Outputs
    - Troubleshooting and Diagnostics
  - Need the ability to update parameters with a MVDU and only taking the affected channel out of service
  - Need the ability to perform troubleshooting and diagnostics without taking the channel out of service

Data Communications

- MVDU – Maintenance Video Display Unit
  - The vendors need to provide details on an approved process to change a selected number of tunable parameters that routinely change due to plant conditions
    - Full Power Delta-T
    - Full Power Tavg
    - Streaming Constants for Thot
    - Normalization of Steam Flow, RCS Flow Indications
  - Highly desired for the MVDU to be non-safety
  - This will most likely be a combination of hardware, software and administrative controls

ISG-04 Appendix - Priority List Items

1. Communication between safety divisions – N/A
2. Control of both safety and non-safety components from a non-safety VDU – N/A
3. HMI to multiple divisions of safety digital systems (Area of Interest 3) – One MVDU (read/write) per Division, PPC (read only) connected to all Divisions
4. Operating a reactor using information displayed on a non-safety VDU for all plant conditions – N/A
5. Requirements for priority modules – N/A
6. Safety HMI control on non-safety components – N/A
7. Design Requirements for Non-Safety devices involved in inter-channel (inter-divisional?) communication (non-safety VDU, shared sensors) (Area of Interest 3) – Plant Computer (read only)
8. Communication involving diverse non-safety systems (Area of Interest 1) – AMSAC (not changing) analog interface only
9. Safety Communications Protocols (Profibus between safety divisions, Ethernet between digital safety systems and safety HMI) (Area of Interest 4??) – Network Configuration

License Amendment Request and Schedule

- Implementation for the first unit – 4/30/12
- Based on a 2 year review time submittal of LAR would need to be by April 2010
- If this is a Tier 1 submittal, NRC has advertised a 10 to 13 month review time
  - This depends on having an approved Topical from each vendor to reference
- This would move the latest required LAR submittal date to March of 2011
  - More time for submitting a complete package and for resolving any issues in Phase 0

LAR Schedule (cont)

- Unclear how much detailed design needs to be complete (final) before the LAR is submitted
- When do we submit our D3 evaluation?
  - Our goal is to submit and get approval prior to LAR submittal
- DCPP has requested to be a pilot plant for the ISG-06 Licensing process
  - What are the expectations for this process?
  - In order for this to be effective, ISG-06 needs to be mostly complete

Questions