DIABLO CANYON POWER PLANT
PROCESS PROTECTION SYSTEM REPLACEMENT

Phase 0 Discussions March 3rd, 2010

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

Ken Schrader
Pacific Gas & Electric Co.
Avila Beach, CA
kjse@pge.com
805-545-4328

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

Ted Quinn
Altran Solutions Corp.
San Francisco, CA
tedquinn@cox.net
415-543-6111

Agenda

- Introductions
- Update on Project Schedule
- Diversity and Defense-in-Depth Evaluation
- Update on PG&E LAR schedule
- ISG-6 schedule and use
- Security
- Communications
- PG&E's plans for software development
- Public Comments
- Closing Comments/Adjourn

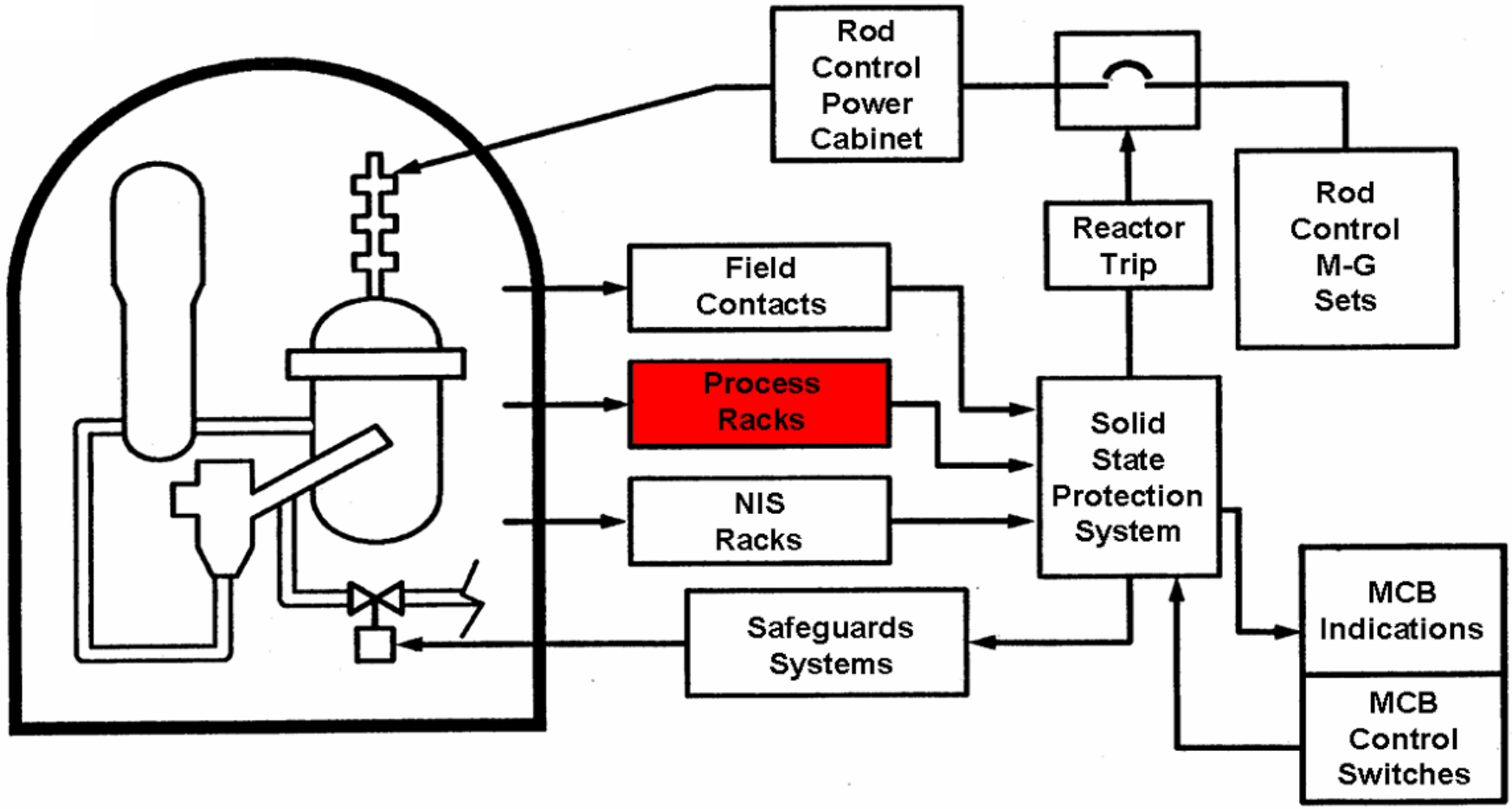
Update on Project Schedule

- Delays
  - 2010 budget was reduced which delayed our Process Control System (PCS) replacement by 20 months
    - PCS has to be installed prior to Process Protection System (PPS)
    - This pushed the PPS replacement schedule by 20 months
  - ISG 6 delayed until May 2010
    - Need this to be able to follow guidance and provide feedback as a pilot plant
  - These delays allow more time to prepare and understand the requirements
  - Expected LAR submittal is May 2011, Reference documents earlier

Diversity and Defense-in-Depth Evaluation

- PG&E Internal Reviews are complete
- ALS Topical Report submittal required before we submit the D3 Evaluation ?
  - Our D3 Evaluation takes credit for features of this platform
    - Specifically that it is not susceptible to CCF
    - Without this feature, the architecture will need to change
  - Forecast for ALS Topical Report submittal is late March
  - Expected Approval ?
- Tricon version 10.5 Topical Report is under review
  - Expected approval is Fall 2010
- The architecture that we are proposing provides a safety improvement over the existing architecture
- Once our D3 Evaluation is submitted, we suggest a meeting to discuss the details

Project Scope



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

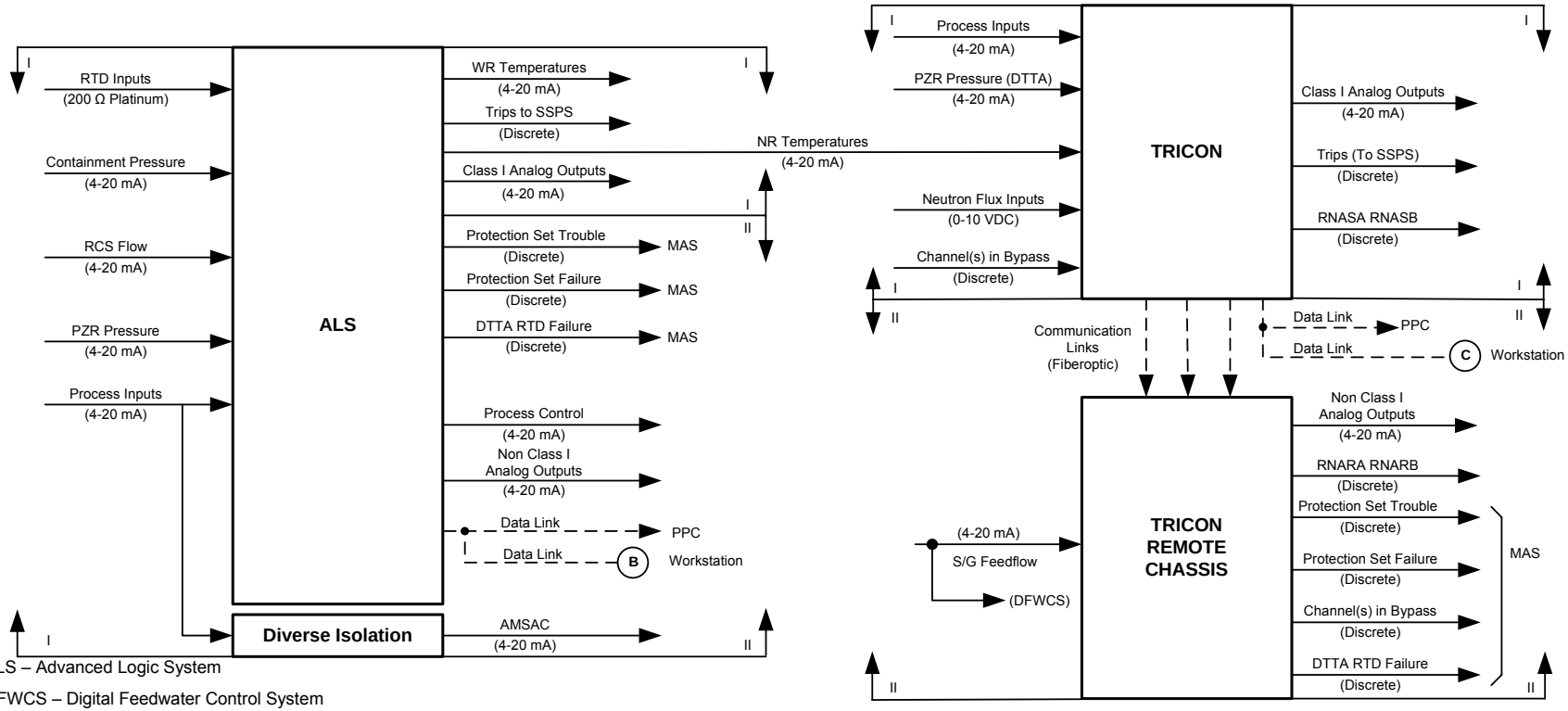
Proposed Replacement PPS Addresses CCF Without an Additional DAS or Manual Actions

- 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

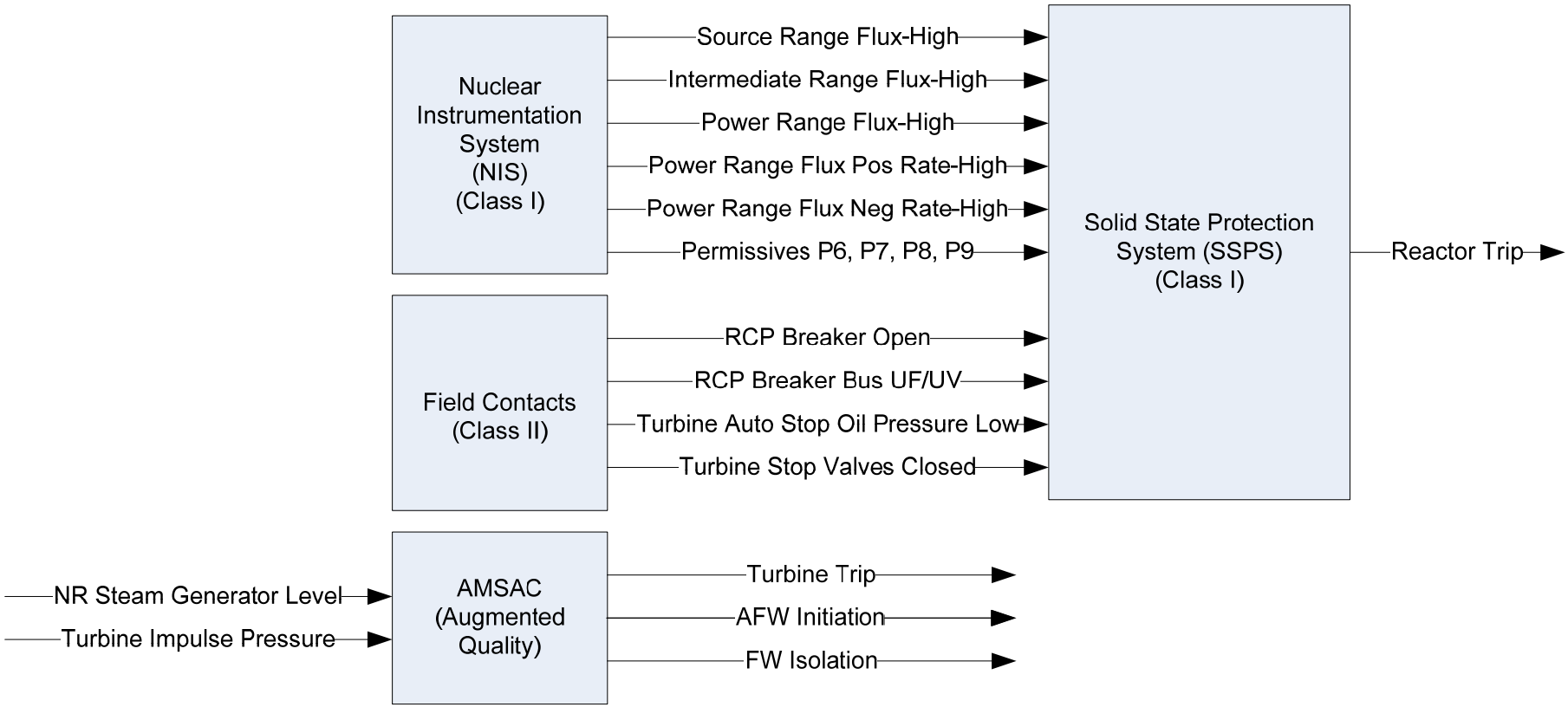
RTD – Resistance Temperature Detector

RCS – Reactor Cooling System

SSPS – Solid State Protection System

WR – Wide Range

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

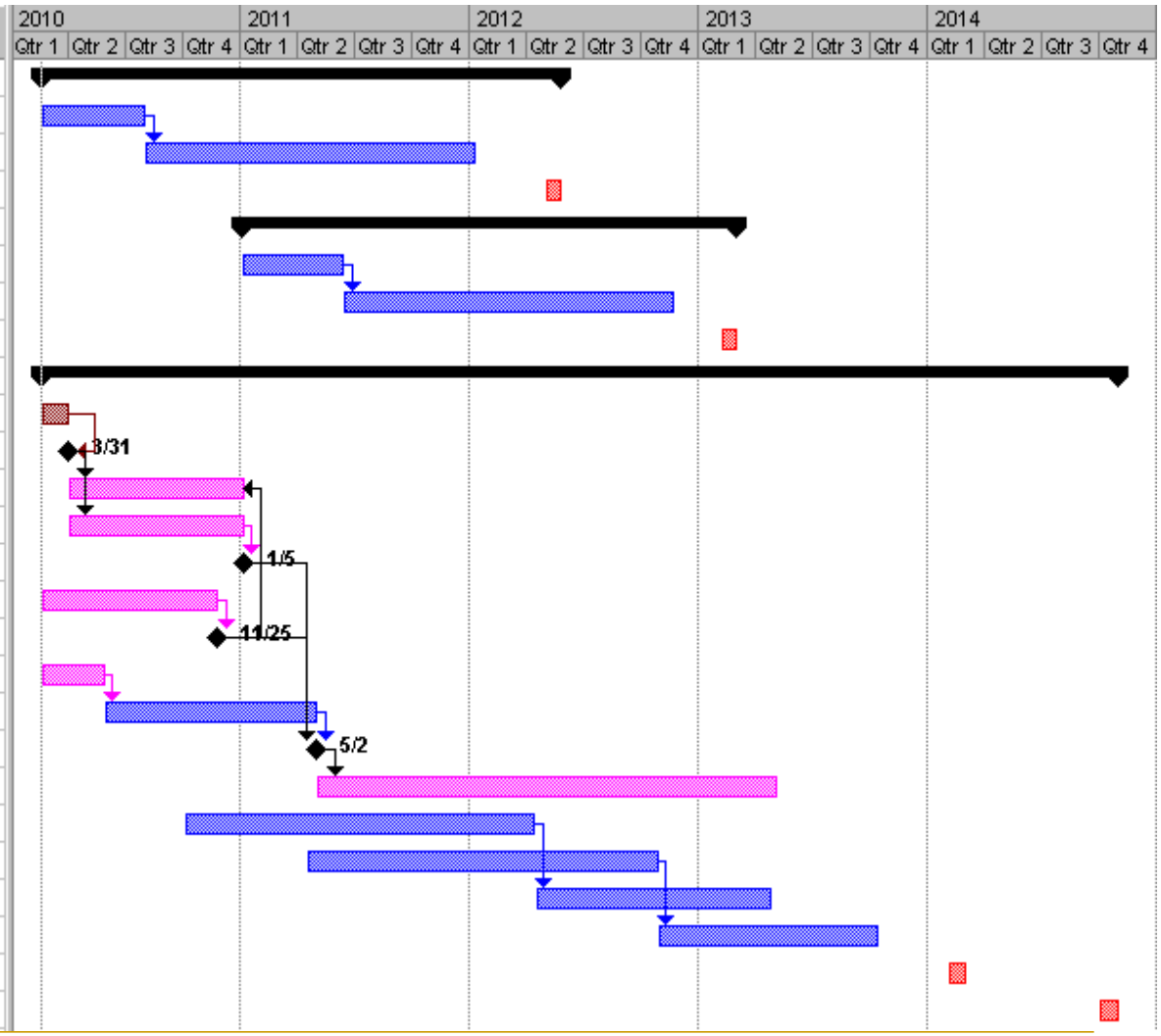


Interim Staff Guidance 6

- ISG 6 draft is out for review
- March 24th Review of Industry Comments
- Issue Final ISG 6 in May
- The Final ISG 6 is essential for DCPP to commit resources to the LAR
  - Need the new guidance to minimize confusion/time on what and when to submit
  - We only want to do this once
- Intention is to submit our LAR as Tier 1 referencing two approved generic Topical Reports – ALS and Tricon
  - Only address plant specific items
  - Need both Topical Reports approved prior to LAR submittal

Update on LAR Schedule

Task Name	Start	Finish
U1 PCS Replacement	**Fri 2/19/10**	**Fri 5/25/12**
DCP	Fri 2/19/10	Mon 8/2/10
Integration and Testing	Tue 8/3/10	Mon 1/9/12
1R17 - Installation	Mon 4/30/12	Fri 5/25/12
U2 PCS Replacement	**Mon 1/3/11**	**Fri 3/1/13**
DCP	Mon 1/3/11	Tue 6/14/11
Integration and Testing	Wed 6/15/11	Tue 11/20/12
2R17 - Installation	Mon 2/4/13	Fri 3/1/13
PPS Replacemet	**Fri 2/19/10**	**Wed 10/29/14**
ALS Topical Report Submitted	Fri 2/19/10	Wed 3/31/10
Diversity Defense in Depth	Wed 3/31/10	Wed 3/31/10
D3 NRC Review	Thu 4/1/10	Wed 1/5/11
ALS TR Review	Thu 4/1/10	Wed 1/5/11
ALS TR Approval	Wed 1/5/11	Wed 1/5/11
Tricon TR Review	Fri 2/19/10	Thu 11/25/10
Tricon TR Approval	Thu 11/25/10	Thu 11/25/10
ISG 6	Fri 2/19/10	Fri 5/28/10
LAR Preparation	Mon 5/31/10	Mon 5/2/11
LAR Submittal	Mon 5/2/11	Mon 5/2/11
LAR Review	Tue 5/3/11	Thu 5/2/13
U1 Design Change Package	Mon 10/4/10	Fri 4/13/12
U2 Design Change Package	Mon 4/18/11	Fri 10/26/12
U1 Integration and Testing	Mon 4/16/12	Thu 4/25/13
U2 Integration and Testing	Mon 10/29/12	Fri 10/11/13
1R18 - U1 PPS Installation	Mon 2/3/14	Fri 2/28/14
2R18 - U2 PPS Installation	Mon 9/29/14	Wed 10/29/14



Security

- Diablo Canyon is responsible to ensure compliance with the applicable 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 responsible departments

Implementation of 10 CFR 73.54

- To fully implement 10 CFR 73.54, a licensee must integrate Security Controls in existing programs, procedures, and processes:
  - Engineering Design Control / SQA
  - Maintenance
    - Work Orders
    - M&TE
  - Corrective Action Program
  - Training program
  - Operations training program

Diablo Canyon Eagle-21 Replacement

- This design change process involves project engineering procedures at Diablo Canyon and two vendors who are providing hardware and software to replace the Eagle-21:
  - Invensys Operations Management (IOM) - Tricon
  - CS Innovations (CSI) - Advanced Logic System

Eagle-21 Replacement Vendors

- Both IOM and CSI are implementing security programs following the guidelines of NRC Regulatory Guide 1.152 Rev. 2.
- The security of computer systems is established by:
  - Designing in security features to meet the licensee's security requirements
  - Developing the systems without undocumented codes (e.g., back doors), including viruses, worms, Trojan horses and bomb codes
  - Installing and maintaining those systems IAW station admin procedures and licensee's security program.

NRC Reg. Guide 1.152 Rev. 2

- Security
  - Uses waterfall lifecycle phases:
    - Concepts
    - Requirements
    - Design
    - Implementation
    - Test
    - Installation, Checkout and Acceptance Testing
    - Operation
    - Maintenance
    - Retirement

Security Summary

- Diablo Canyon will comply with the applicable guidance on 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.
- Diablo Canyon will address RG 5.71 separately

Communications

- ISG-04, Highly Integrated Control Rooms – Communications Issues (ISG #4)
- Three General Areas of Interest
  - General Areas of Interest
  - Interdivisional Communications (Staff Position 1)
  - Command Prioritization (Staff Position 2)
  - Multidivisional Control & Display Stations (Staff Position 3)

- NOTE: Phase 0 discussion today only addresses Staff Position 1. All Staff Positions will be addressed by Diablo Canyon and the vendors in separate submittals

Interdivisional Communications (Staff Position 1)

- Safety-to-safety – not applicable for the Eagle-21 replacement as no safety-to-safety channel communication will occur.

- Safety-to-non-Safety - the Tricon and ALS systems communicate with two non-safety digital systems:
  - Plant Process Computer – one-way, display only
  - MVDU (Maintenance Video Display Unit) – bidirectional
- The qualified Tricon Communications Module (TCM) isolates external communications from the Main Processors (MP) to ensure that the non-safety communications functions do not disrupt safety-related operation.
- ALS communications to PPC are isolated, one-way, and point to point.
- ALS communications to the MVDU are bidirectional and controlled by an external hardware keyswitch

Interdivisional Communications (Staff Position 1)

- The Tricon keyswitch is a physical interlock that controls the mode of the Tricon
- The position of the keyswitch is continuously monitored by the three Tricon main processor modules (MPs)
- The MPs vote on the position of the keyswitch
- Multiple failures are necessary in order to inadvertently allow software programming of the Tricon

Safety-to-non-Safety Digital Communication Interfaces

- 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)
    - This connection will use a data isolation device like the NetOptics Network Port Aggregator referenced in the Oconee SER to ensure one-way communications to the PPC

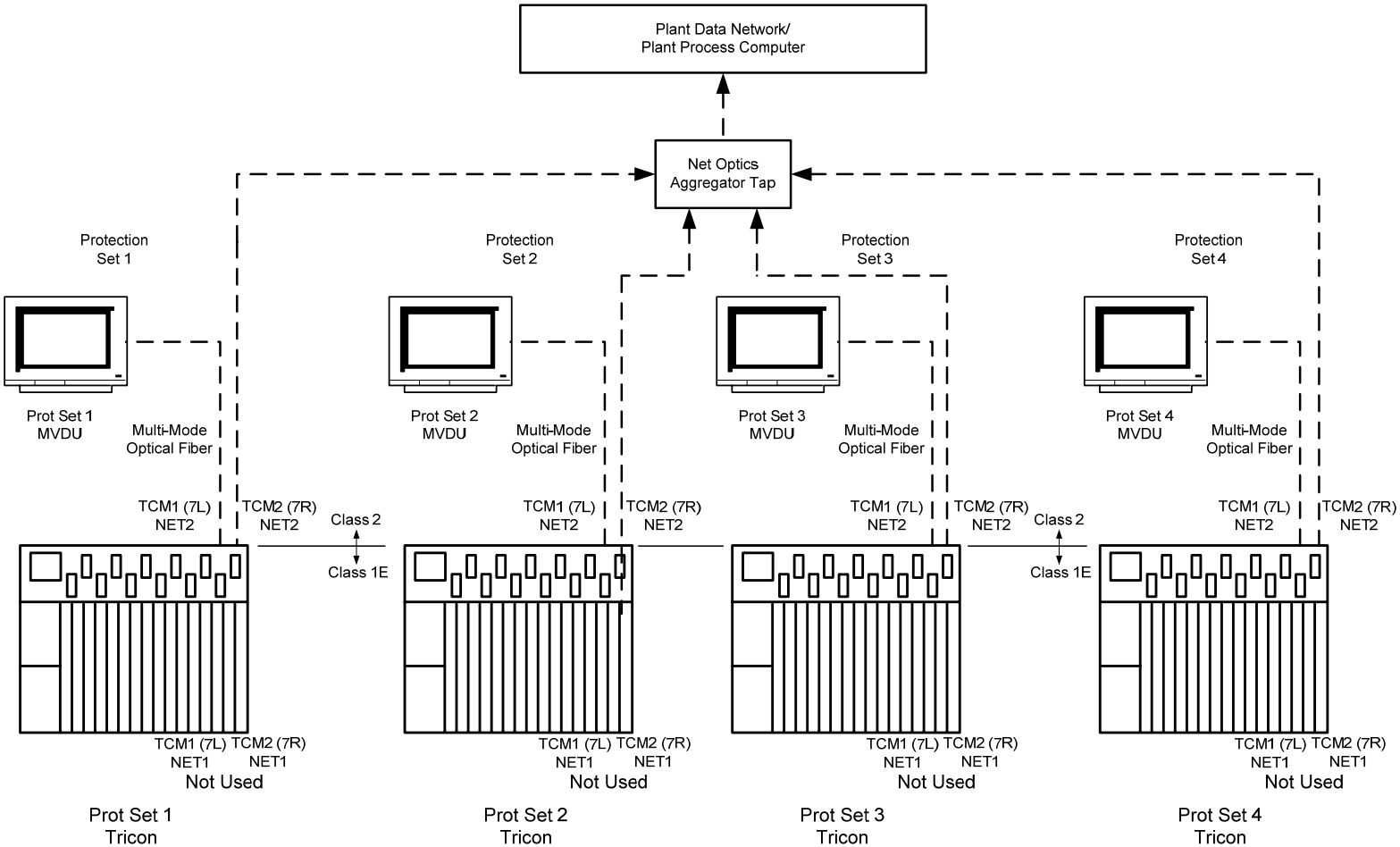
Safety-to-non-Safety Digital Communication Interfaces

- MVDU – Maintenance Video Display Unit
  - Functions
    - Removing a channel from service (bypass, trip, defeat alarms, etc.)
    - Updating specific tunable parameters like:
      - Full Power Delta-T
      - Full Power Tavg
      - Normalization of Steam Flow, RCS Flow Indication
    - Calibrating Analog and Digital Outputs
    - Troubleshooting and Diagnostics
    - Alarm logger
  - Need the ability to update parameters with a MVDU and take only the affected channel out of service
  - Need the ability to perform troubleshooting and diagnostics without taking the channel out of service

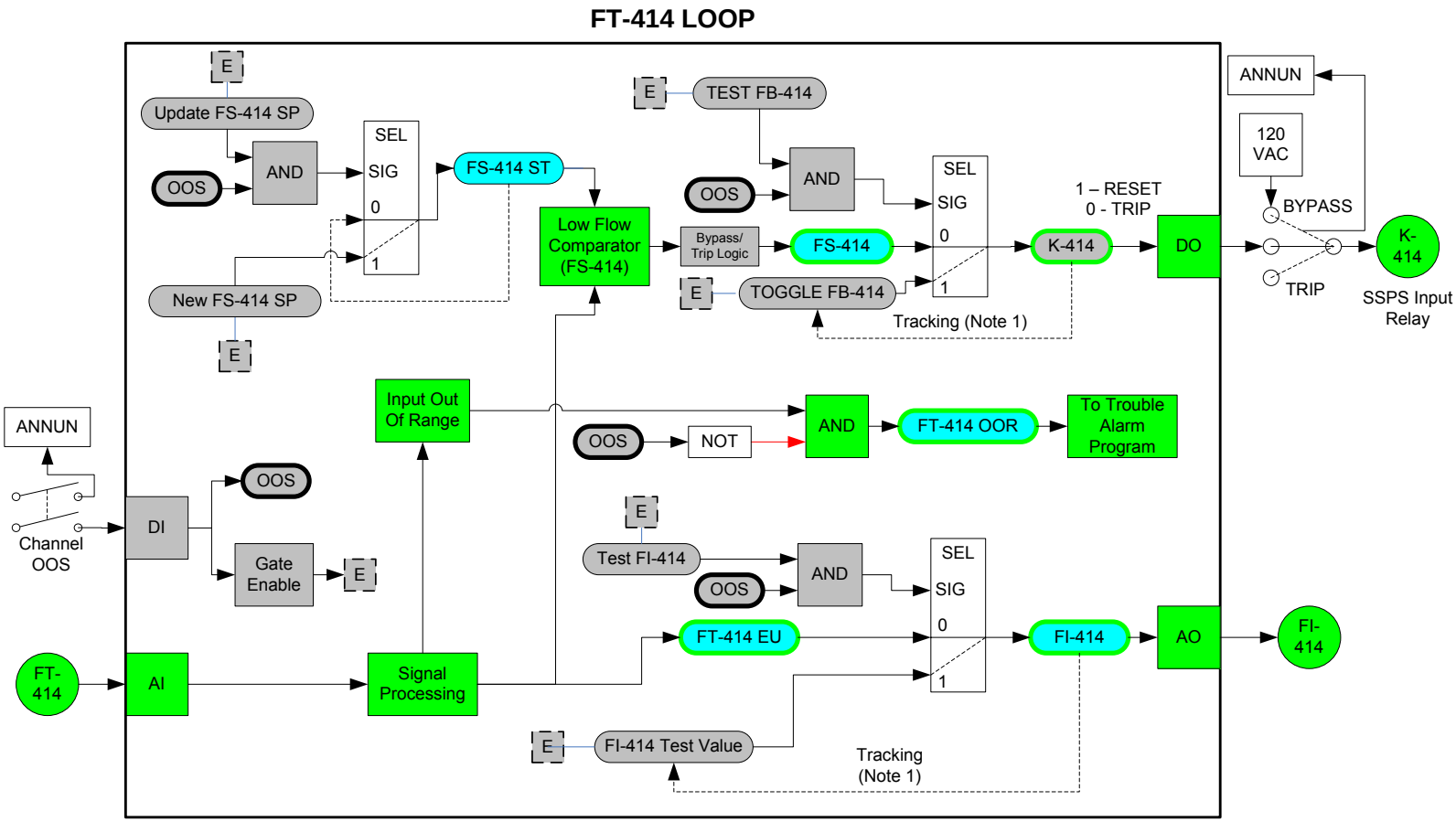
Safety-to-non-Safety Digital Communication Interfaces

- MVDU Controls to Ensure Changes are Accurate
  - Safety Related Controls
    - Hardware switch directly tied to a digital input removes channel from service
    - Software Partitioned by Instrument Loop
    - Safety related software V&V
    - Access Control to the area and cabinet
      - Vital Area access
      - Key required for cabinet door
    - Approved Procedures required to perform testing and updates
      - During update the values are limited to pre-determined ranges
  - Non-Safety Controls
    - One MVDU per Channel/Protection Set
    - MVDU Password Protected to make changes
      - Limited people with account and password
      - Access privileges dependent upon procedure (e.g., instrument loop test versus setpoint change)
    - Software V&V integrated with the final system
    - HMI software will be partitioned by Instrument Loop
    - Channel check of indications after maintenance

Non-Safety Communication Diagram



Typical Loop

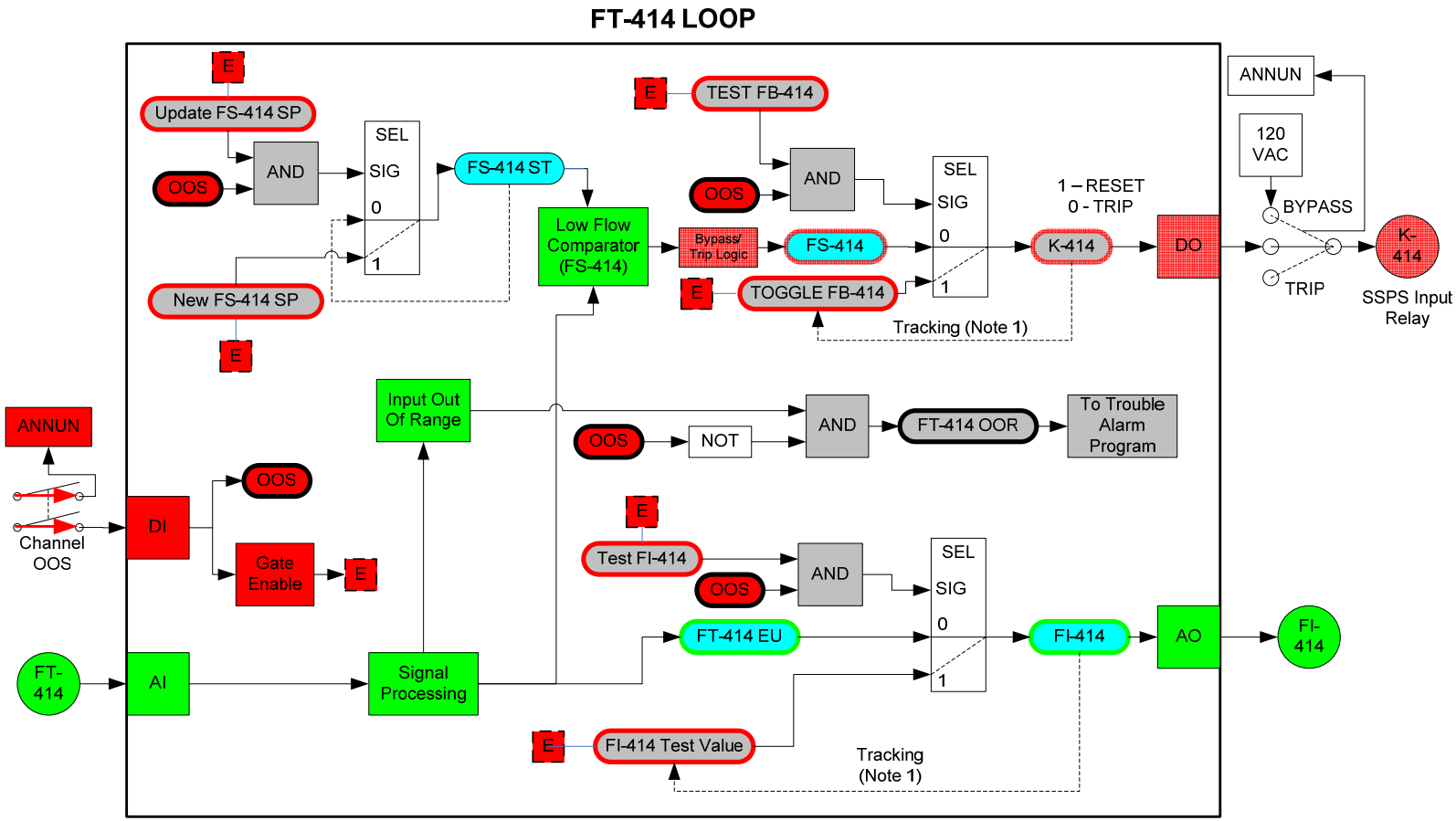


OOS – Out Of Service
OOR – Out Of Range

Note 1: Input 1 tracks Output when Input 0 is selected (bumpless transfer to test mode).

Loop Out of Service

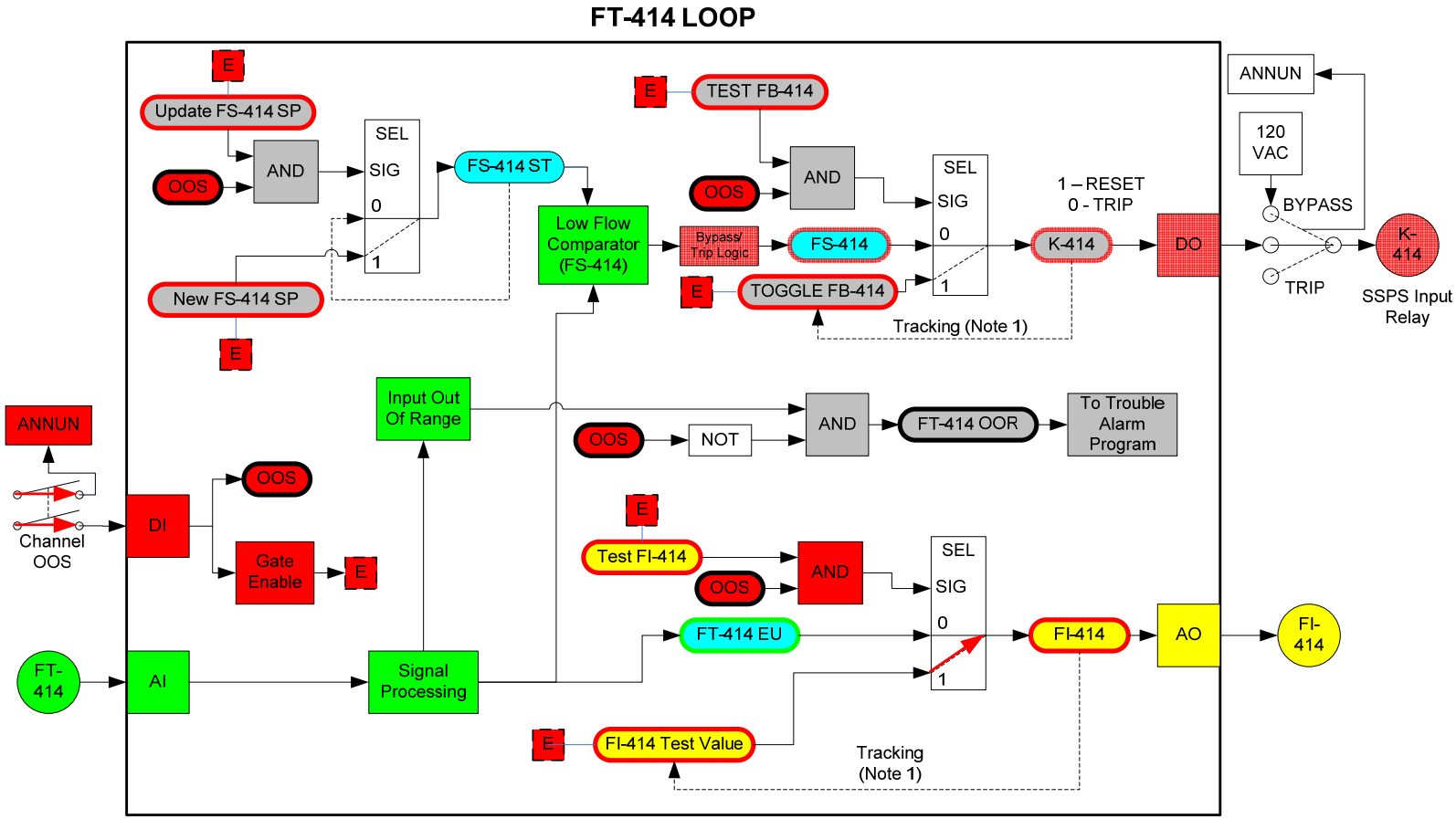
Gate Enable only enables a hard coded set of variables for that loop only



OOS – Out Of Service
OOR – Out Of Range

Note 1: Input 1 tracks Output when Input 0 is selected (bumpless transfer to test mode).

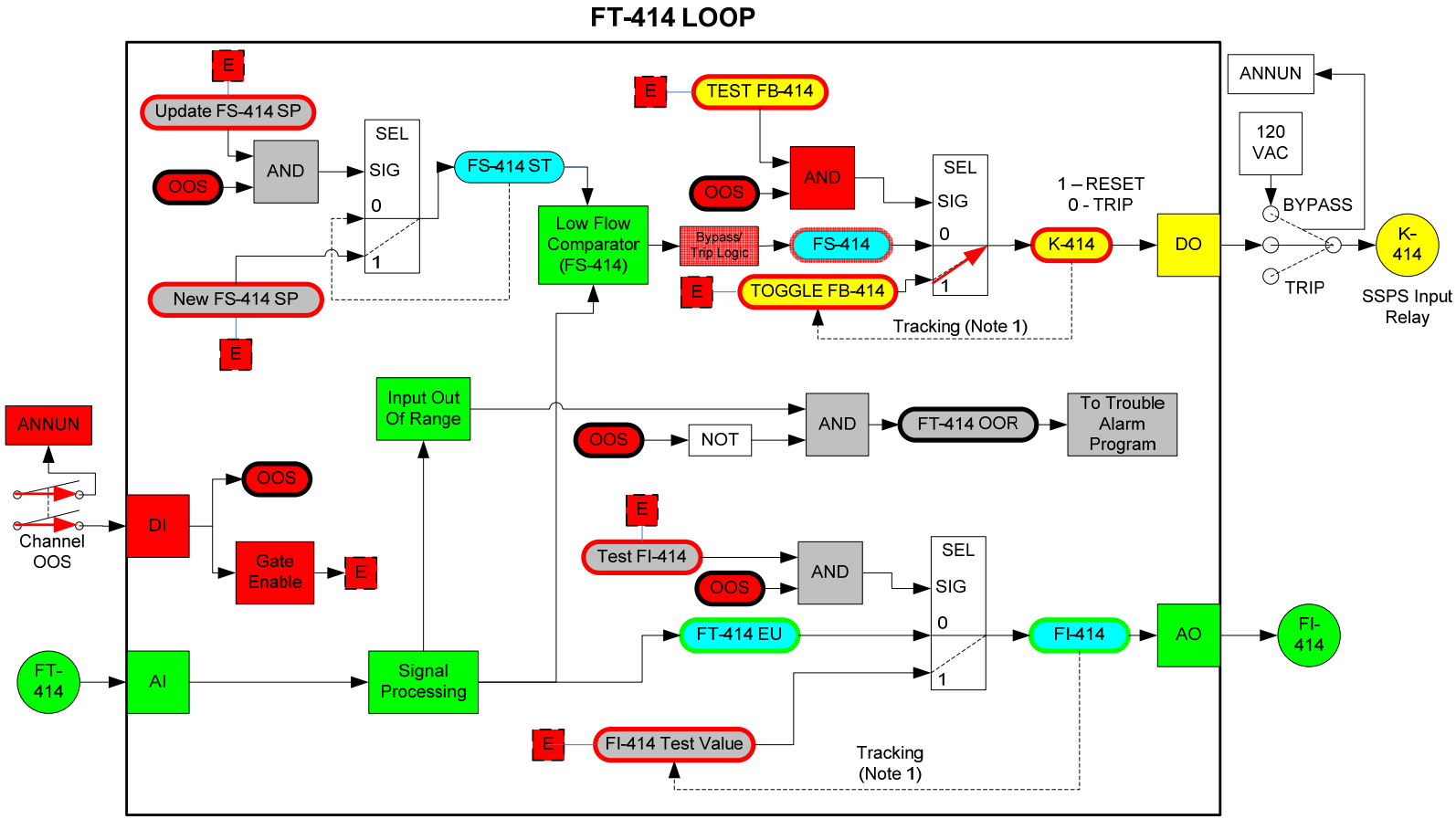
Analog Output in Test from HMI



OOS – Out Of Service
OOR – Out Of Range

Note 1: Input 1 tracks Output when Input 0 is selected (bumpless transfer to test mode).

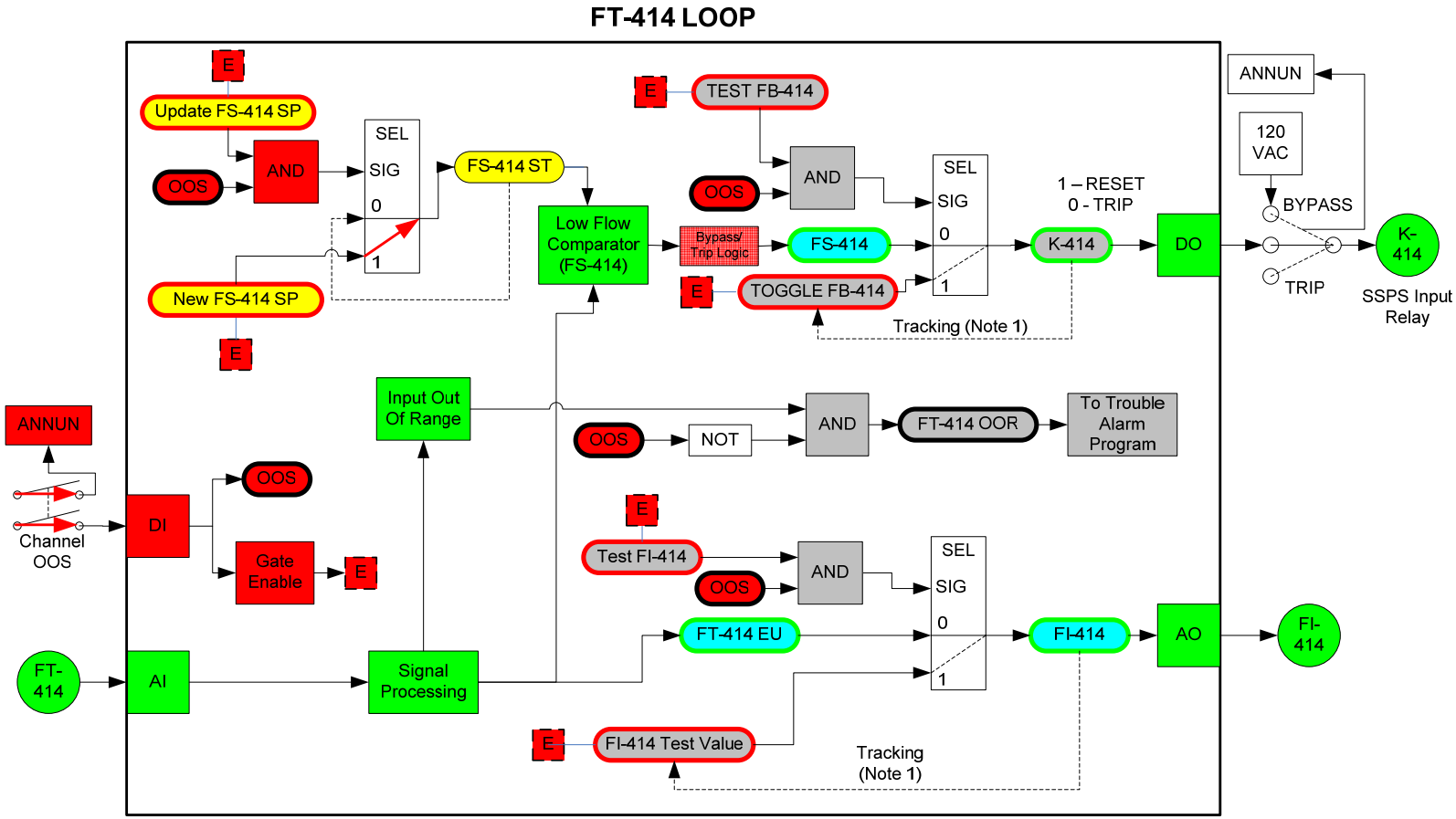
Digital Output in Test from HMI



OOS – Out Of Service
OOR – Out Of Range

Note 1: Input 1 tracks Output when Input 0 is selected (bumpless transfer to test mode).

Parameter Update from HMI



OOS – Out Of Service
OOR – Out Of Range

Note 1: Input 1 tracks Output when Input 0 is selected (bumpless transfer to test mode).

Safety-to-non-Safety Digital Communication Interfaces

- MVDU Controls to prevent inadvertent changes:

OOS switch	HMI	Failure[a]
0	0	0
0	1[b]	0
1[c]	0	0
1[c]	1[b]	1

a: Failure is defined as hardware failure, software failure, human error

b: HMI failures - log-on false positive (s/w error); weak password; maintenance error (procedural or human, e.g. maintenance technician types in AND accepts incorrect parameter value); communication error causes corrupt value (also entails multiple faults)

c: OOS switch failures - hardware failure; maintenance error (procedural or human); weak physical access controls

- Write/Test error requires both OOS switch failure and HMI failure

Software Development

- Triconex and CS Innovations will develop and test the initial application software for their portion of the project with oversight of the V&V process by PG&E
- PG&E intends to submit the Software Operation and Maintenance Plan to allow software changes by the vendor or PG&E after initial installation
- The ALS platform will require the vendor to make changes due to its technology
- Firmware updates will be handled by the vendors under their programs

Questions