I&C for Plant Protection Systems (Systems Description)

2013 IAEA/ANSN ETTG Workshop on
Nuclear Safety Tailored for Regulators
(17~21 June, 2013)
Int. Nuclear Safety School, KINS, Korea

Name : Kim, Bok Ryul
E-mail : k060kbr@kins.re.kr

한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY

CONTENTS

1. Plant Protection System

Definition of Safety System

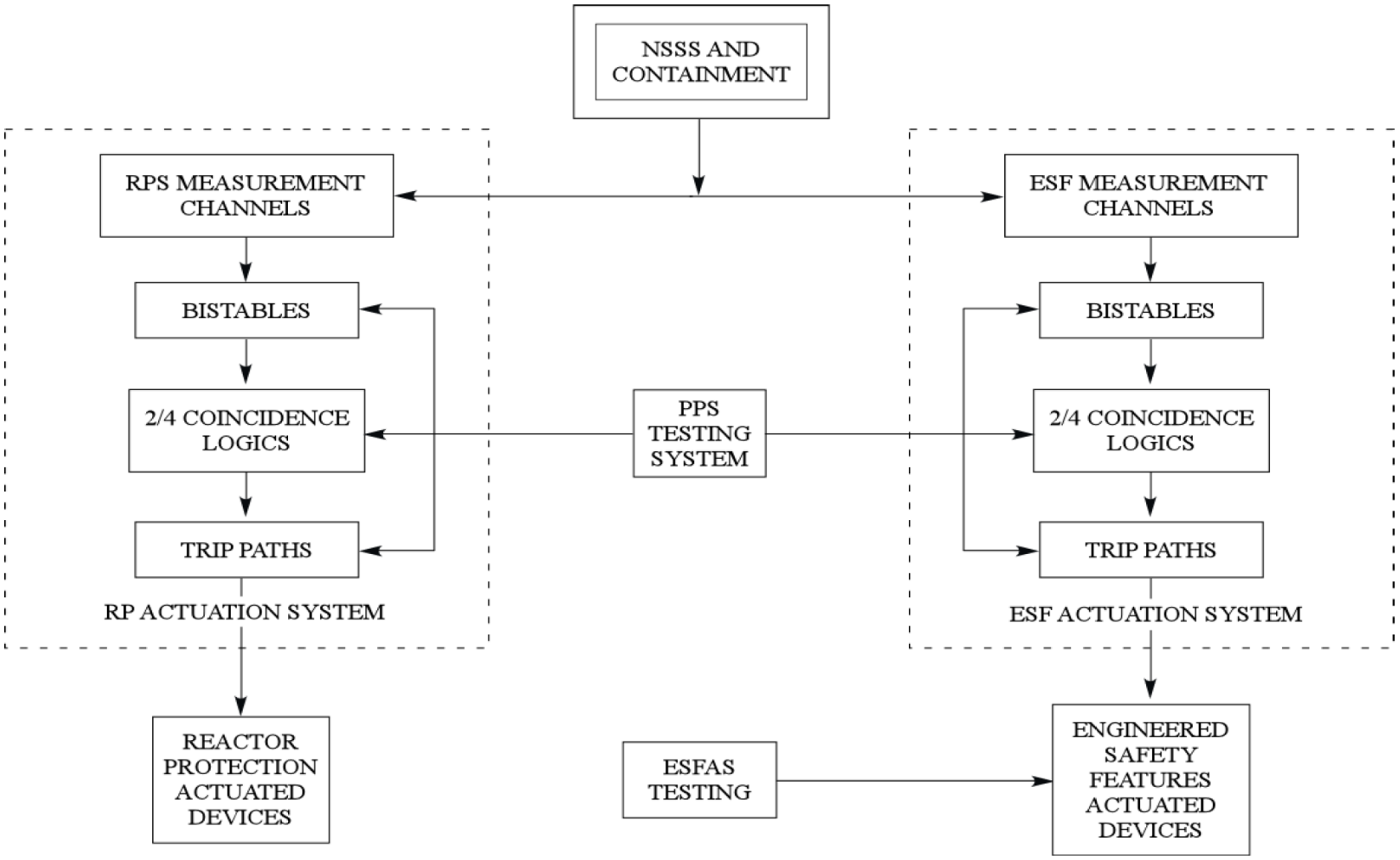
- IEEE Std. 603-1998 defines a "Safety System" as:
  - A system that is relied upon to remain functional during and following design basis events to ensure:
    - the integrity of the reactor coolant pressure boundary
    - the capability to shut down the reactor and maintain it in a safety condition
    - the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR 100 guidelines

Plant Protection System (1/4)

- **The Plant Protection System (PPS) is designed:**
  - to sense abnormal occurrences and/or accidents in the reactor plant
  - to initiate automatic actions to place the plant in a safe condition, and
  - to maintain the integrity of the three fission product barriers, e.g., fuel cladding, RCS system piping, and containment building

- **The Plant Protection System can be broken down into two subsystems.**
  - Reactor Protection System (RPS)
  - Engineered Safety Features Actuation Systems (ESFAS)

Plant Protection System (2/4)

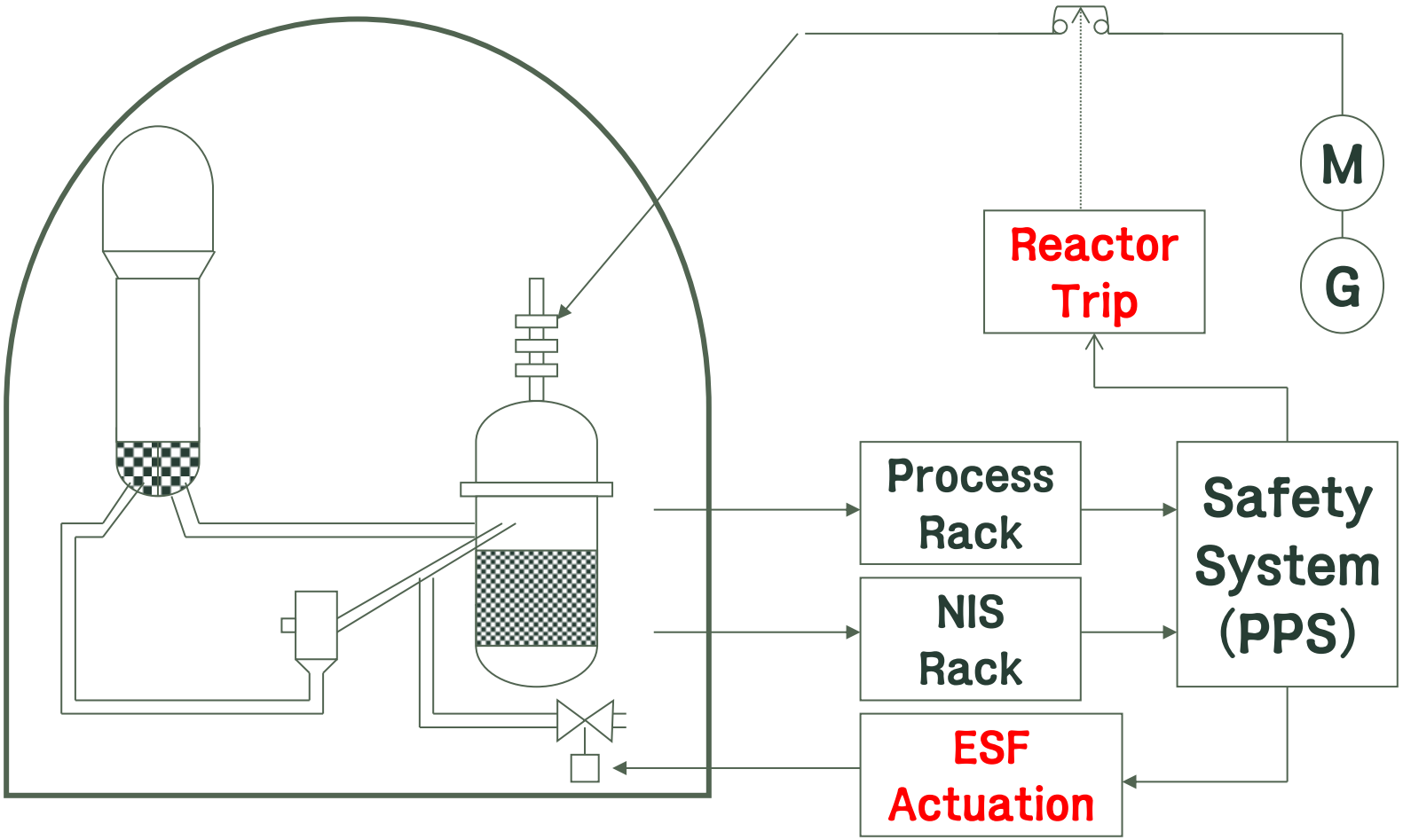


Plant Protection System Block Diagram

Plant Protection System (3/4)

- During an emergency,
  - The RPS rapidly inserts the Control Element Assemblies (CEAs) to shutdown the nuclear chain reaction to reduce the heat generation rate.
    - This action limits peak fuel centerline and cladding temperatures along with RCS temperatures and pressures.
  - The ESFAS actuates valves, pumps, fans, and other plant equipment to enhance the ability of the plant to protect the three fission product barriers(e.g., fuel cladding, RCS system piping, and containment building).

Plant Protection System (4/4)



[PROTECTION SCHEME]

2. Reactor Protection System

Reactor Protection System

Functions

- Monitors various plant parameters, such as reactor power, RCS temperature, pressurizer pressure, steam generator water levels and pressurizers, etc.
- Trips the reactor to maintain plant parameters within acceptable limits
  - To maintain the integrity of the fuel cladding and RCS boundaries during any Anticipated Operational Occurrences (AOO)
  - To limit offsite radiation doses to within the limits of 10 CFR 100 during design basis accident
- Initiate automatic protective action to aid the Engineered Safety Features (ESF) systems in limiting the consequences

Reactor Protection System

Design Bases (1/2)

- Prevent exceeding any Specific Acceptable Fuel Design Limits(SAFDLs) during any AOO.
  - SAFDLs are limits on monitored plant parameters which will assure the integrity of the fuel cladding.
    - Linear Heat Rate (LHR)
    - Departure from Nucleate Boling Ratio (DNBR)
- Comply with 10 CFR 50, Appendix A, GDC 21, which addresses protection system reliability, testability, redundancy, and independence.
  - No single failure will result in the loss of protective function
  - Removal of any channel or component from service will not result in loss of the required minimum redundancy
  - The PPS can be periodically tested at power without tripping the reactor or causing any protective actuation signals.

Reactor Protection System

Design Bases (2/2)

- Comply with the following provisions of IEEE 603 criteria for nuclear power plants
  - Four independent measurement channels are provided.
  - No single failure will prevent protective action.
  - System actuation of selected plant variables will be 2/4 coincidence.
  - When one channel is out of service, coincidence logic is reduced to 2/3.
  - Protective logic assumes the de-energized state to trip.
  - Manual reset is necessary once actuation is initiated.
  - System can be tested with the plant shutdown or operating.
  - Selected plant variables may be manually blocked or bypassed during plant startup and shutdown.

Reactor Protection System

Reactor Trip Variables (1/3)

- High Linear Power
  - Provides reactor core protection against rapid reactivity excursions which might result from an ejected CEA
- High Log Power
  - Assures the integrity of the fuel cladding and RCS boundary due to an unplanned criticality from a shutdown condition
- Local Power Density (LPD)
  - Prevents the linear heat rate (Kw/ft) in the limiting fuel rod in the core from exceeding the fuel design limit in the event of any AOO.
- Low Departure from Nucleate Boiling Ration (DNBR)
  - Prevents the DNBR in the limiting coolant channel in the core from exceeding the fuel design limit in the event of any AOO.
  - The LPD and DNBR trip setpoints are calculated in the Core Protection Calculators (CPCs).

Reactor Protection System

Reactor Trip Variables (2/3)

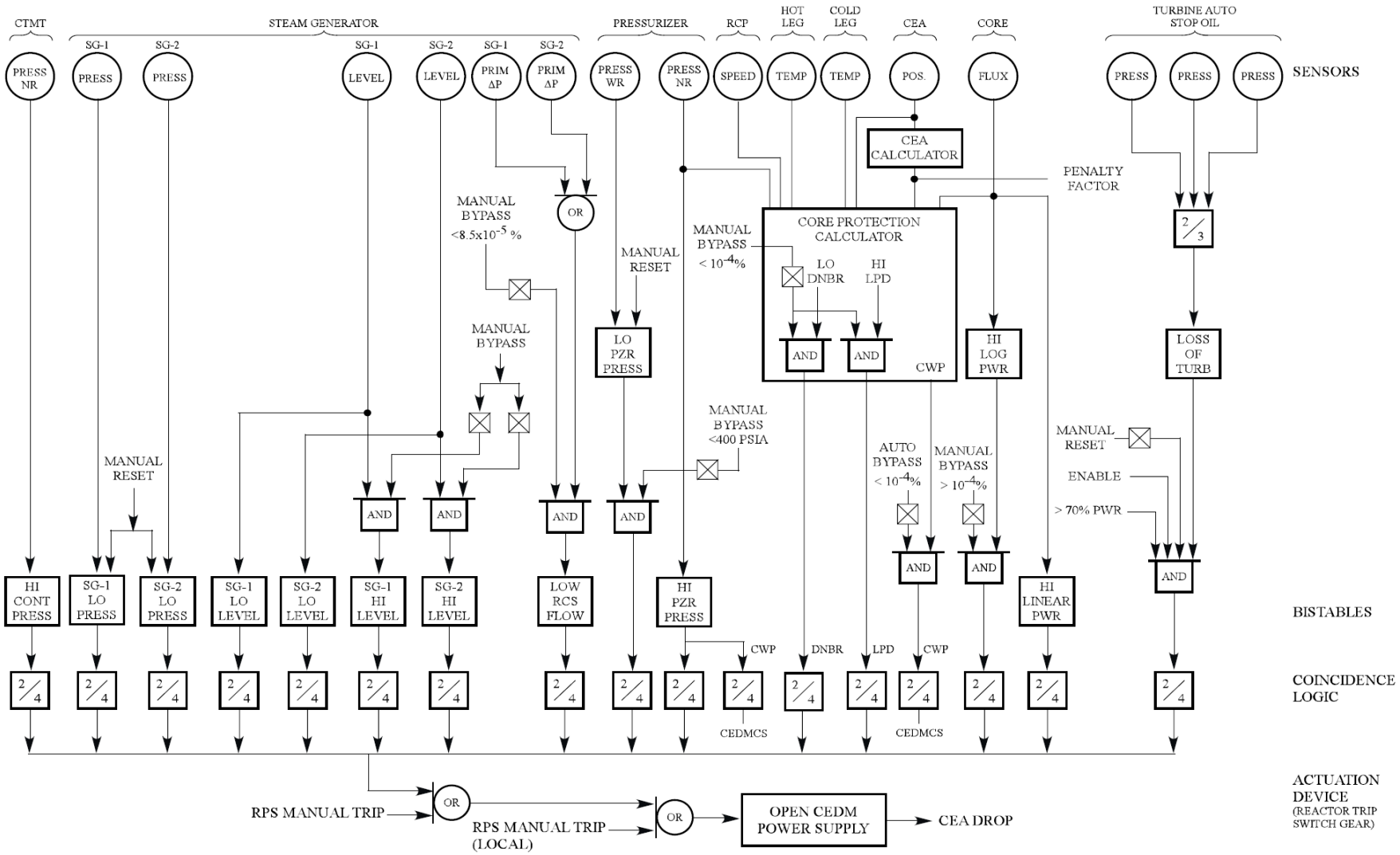
- High Pressurizer Pressure
  - Provides RVS over pressure protection during a loss of load
- Low Pressurizer Pressure
  - Assists the ESF systems in the event of a LOCA by tripping the reactor early in anticipation of reaching the ESF protective action setpoint
- Low Steam Generator Pressure
  - Provides protection against an excessive heat removal from the SGs and subsequent RCS cooldown
- Low Steam Generator Water Level
  - Provides protection against events involving a mismatch between steam and feedwater flow
- High Steam Generator Water Level
  - Protects the turbine from excessive moisture carryover

Reactor Protection System

Reactor Trip Variables (3/3)

- High Containment Pressure
  - Provides assurance that a reactor trip is initiated concurrent with safety injection, containment isolation, and main steam isolation signals.
- Steam Generator Low Flow
  - Provides protection against a Reactor Coolant Pump sheared shaft event and a steam line break event concurrent with a loss of offsite power
- Reactor Trip on Turbine Trip
  - Provides removal of the heat source from service by reactor trip when the turbine is tripped in anticipation of a possible loss of heat sink
- Manual Reactor Trip
  - Permits the operator to trip the reactor manually from the Main Control Room per the design bases requirements

Overall Reactor Trip Logic Diagram



Reactor Trip Methodology

Description (1/2)

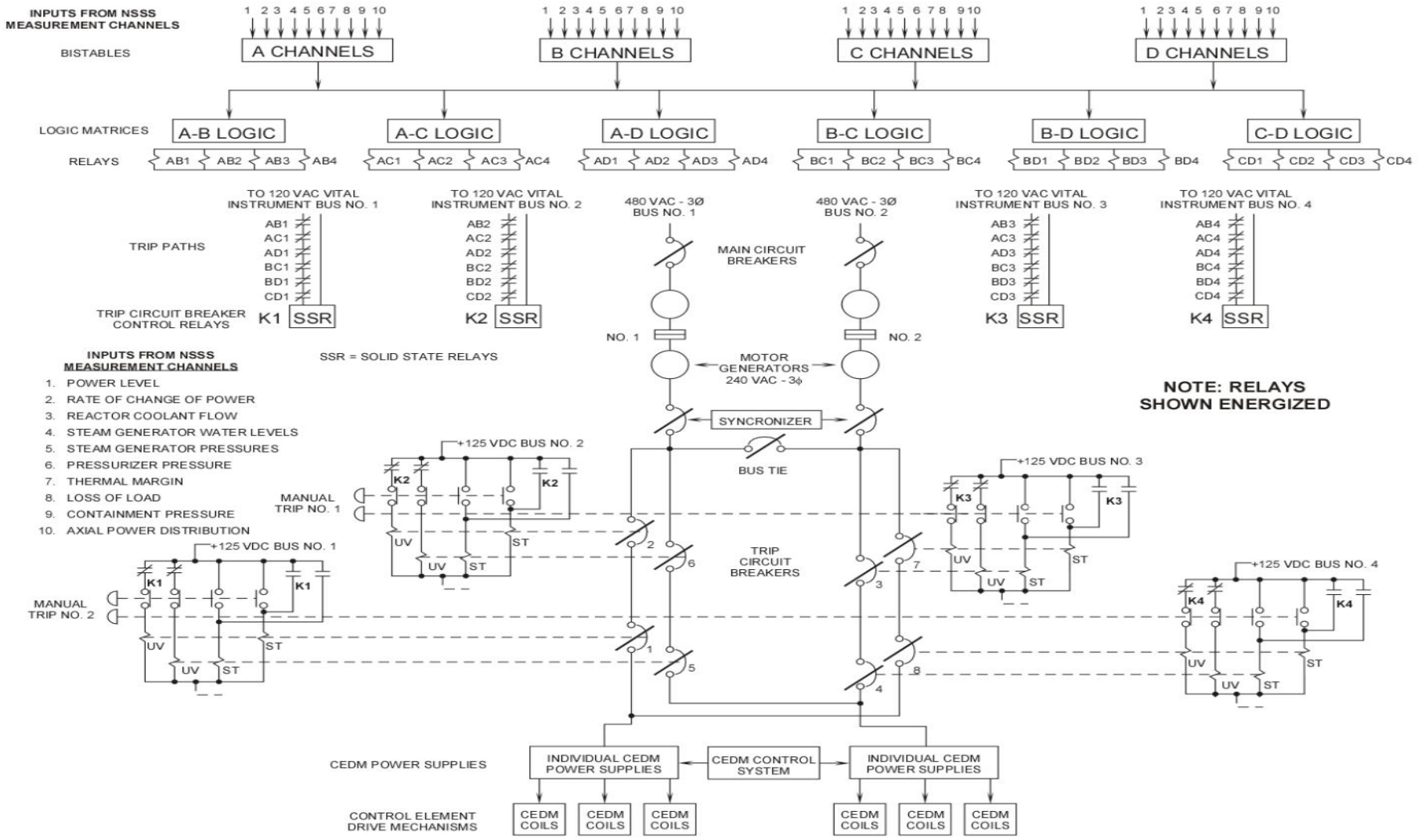
- Process sensors monitor selected plant parameters and send status to the RPS.
- This information is compared to bistable setpoints for each input parameter to determine if an unsafe plant condition is being approached.
- The bistables convert the analog inputs into digital outputs for use by the RPS coincidence logic circuits to determine if a trip is necessary.
  - Coincidence logics are used to prevent a single instrument failure from causing an unnecessary reactor trip.
  - A trip on one channel out of four will only cause an alarm, but two or more channels must trip to satisfy the 2/4 trip coincidence logic and establish a reactor trip path.

Reactor Trip Methodology

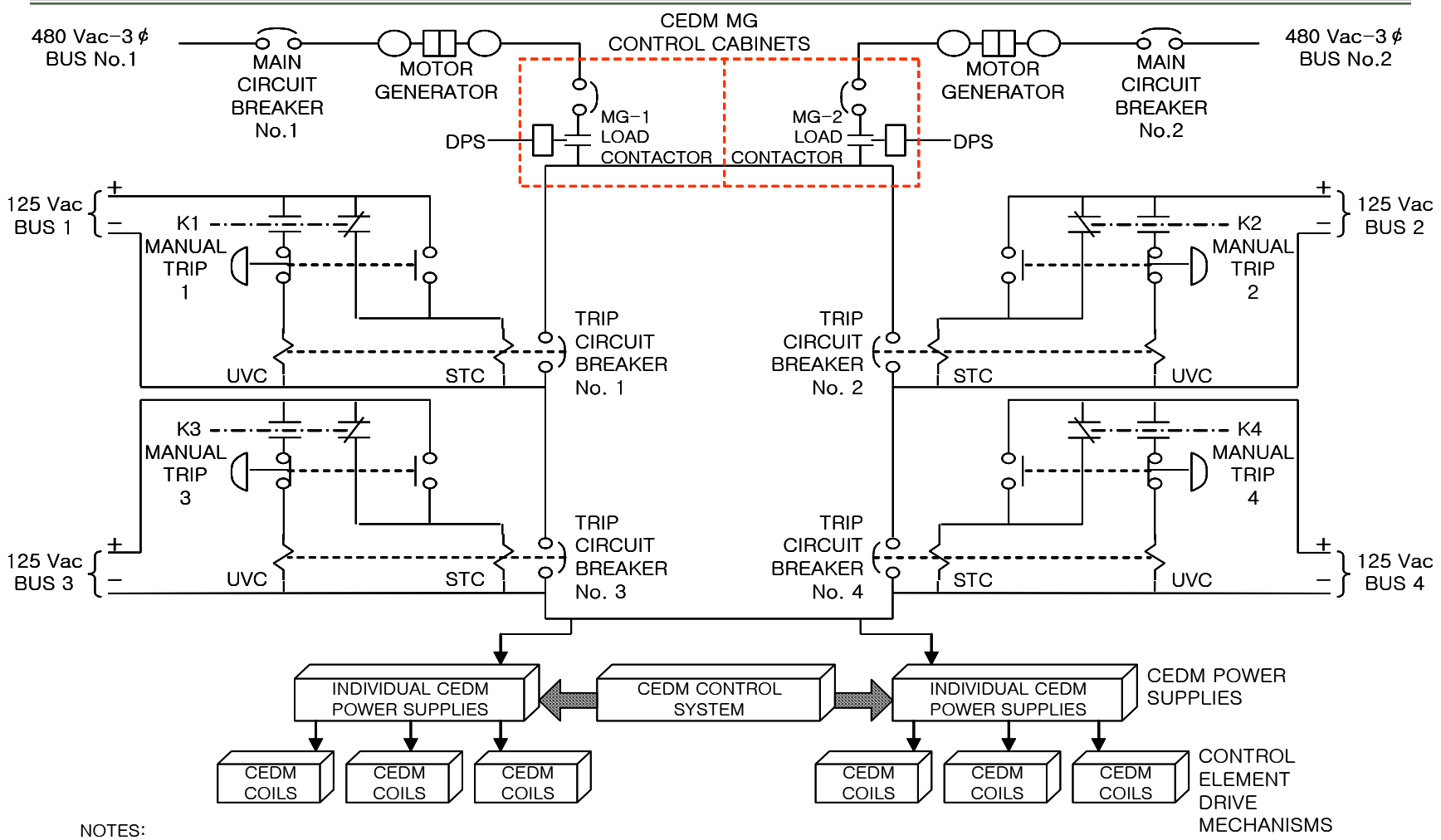
Description (2/2)

- Four input channels require six logic circuits to check for a two-out-of-four coincidence.
  - These six coincidence circuits are called matrices.
  - Each two-out-of-four coincidence matrix has four normally energized matrix output relays associated with it(AB1, AB2, AB3, AB4).
- When channels A and B exceed their trip setpoint, bistable A and B will trip, the ‘AB’ matrix will detect a 2/4 coincidence and de-energize its four matrix output relays (AB1, AB2, AB3, and AB4).
- Four matrix output relays will fail open in the four trip paths, which remove power to Initiation relays (K1, K2, K3, and K4).

Overall RPS Functional Logic Diagram



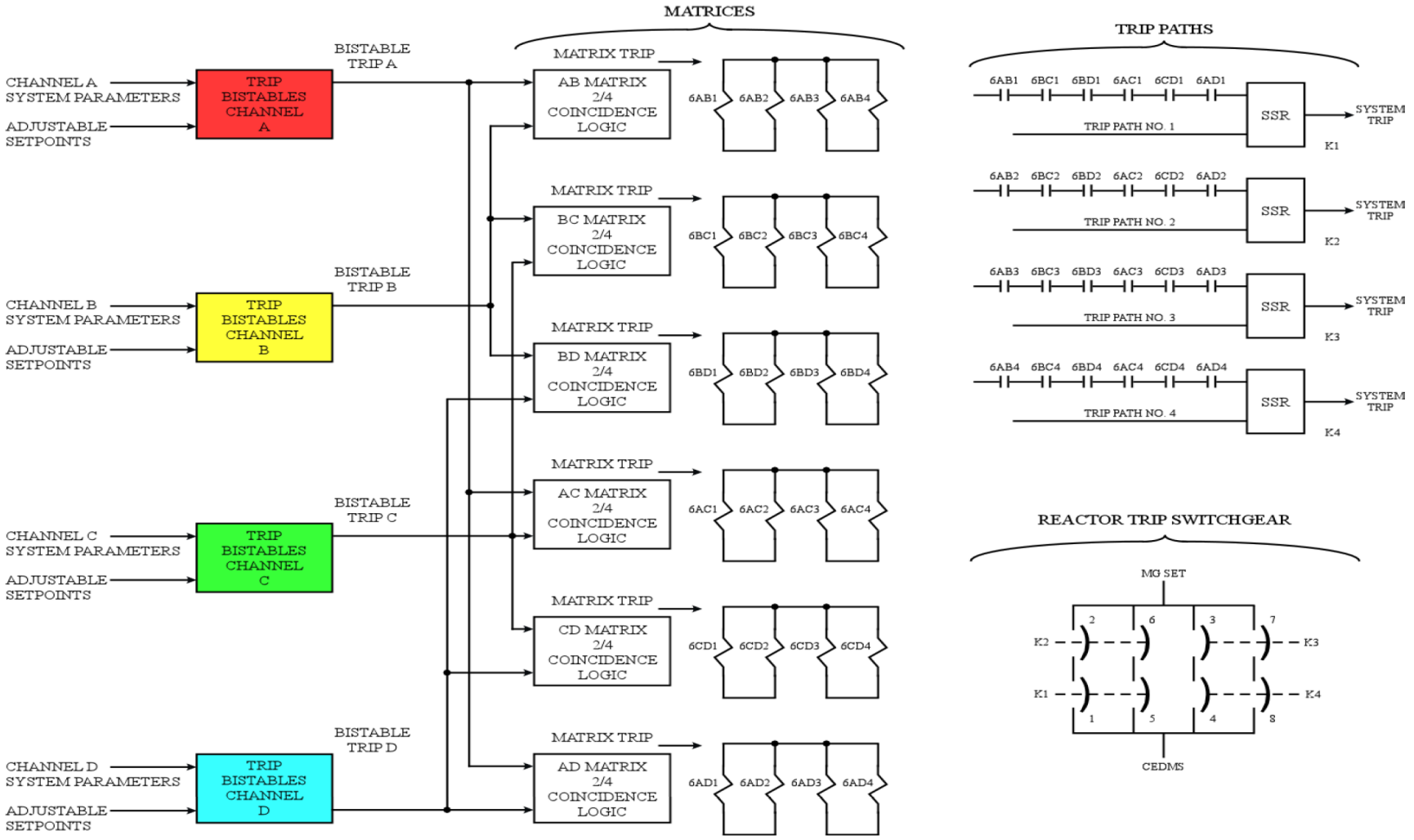
Reactor Trip Switch Gear System in OPR-1000



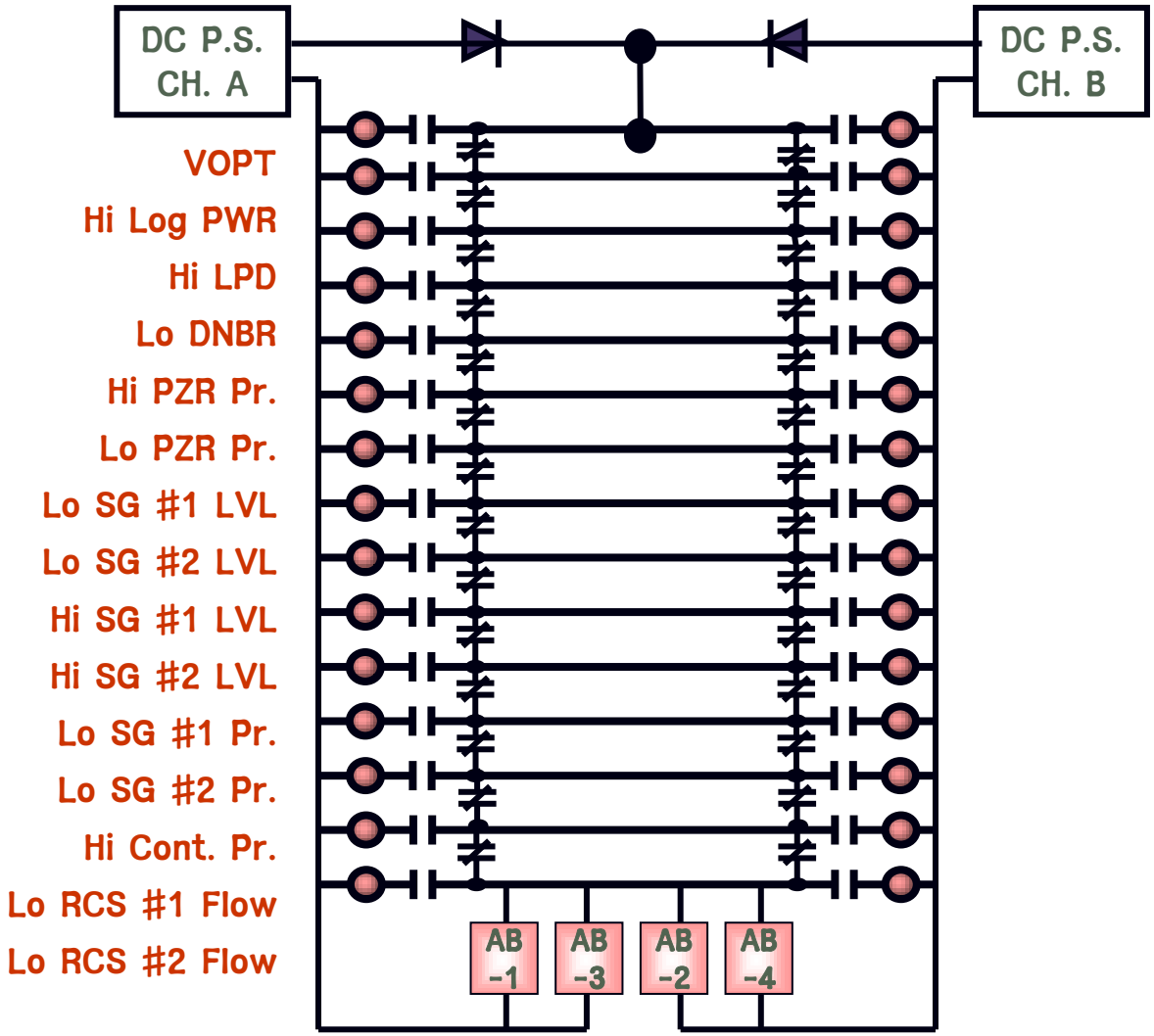
NOTES:

1. STC=SHUNT TRIP COIL
2. UVC=UNDER VOLTAGE COIL
3. DPS=DIVERSE PROTECTION SYSTEM

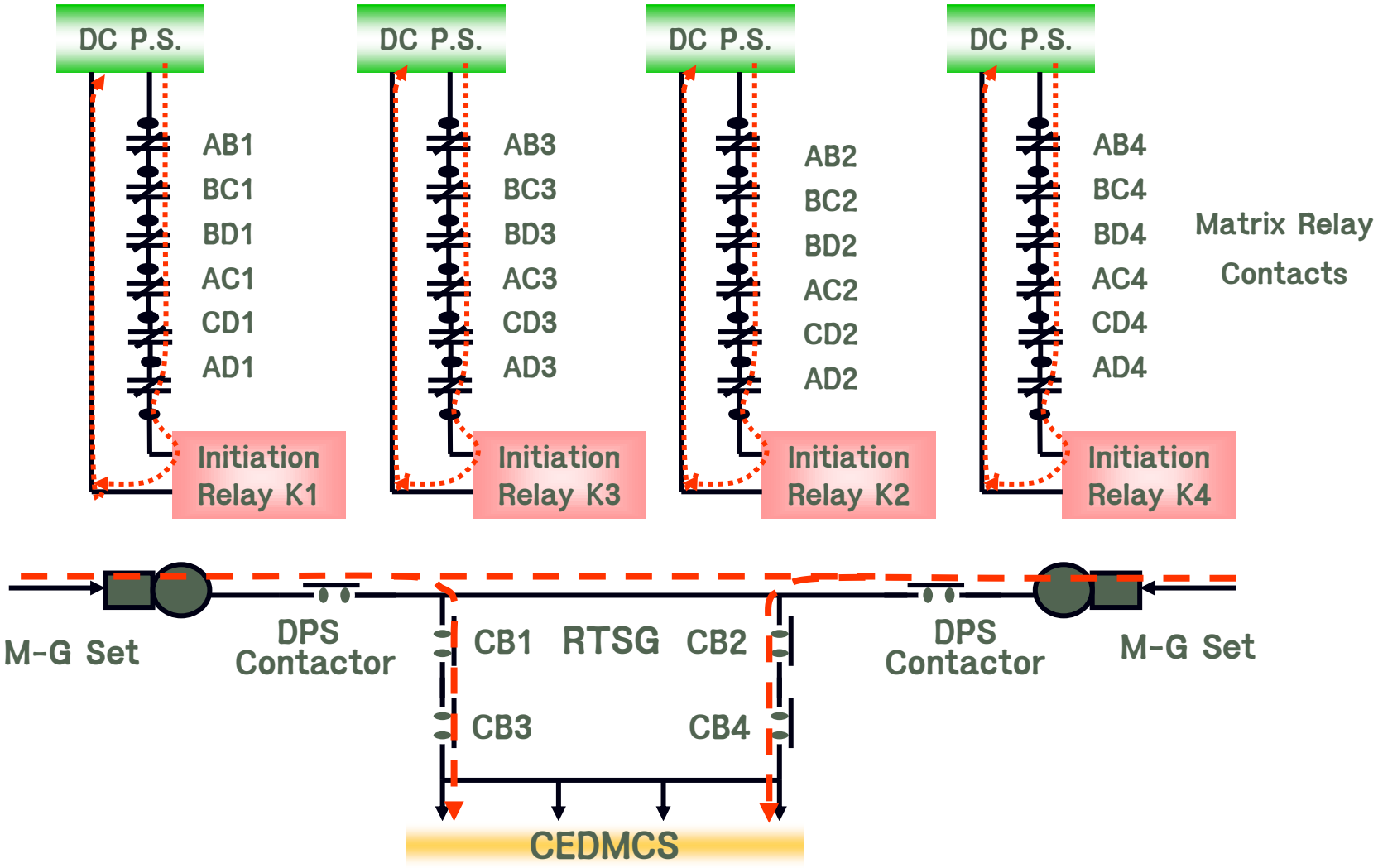
RPS Trip Signal Flow Paths



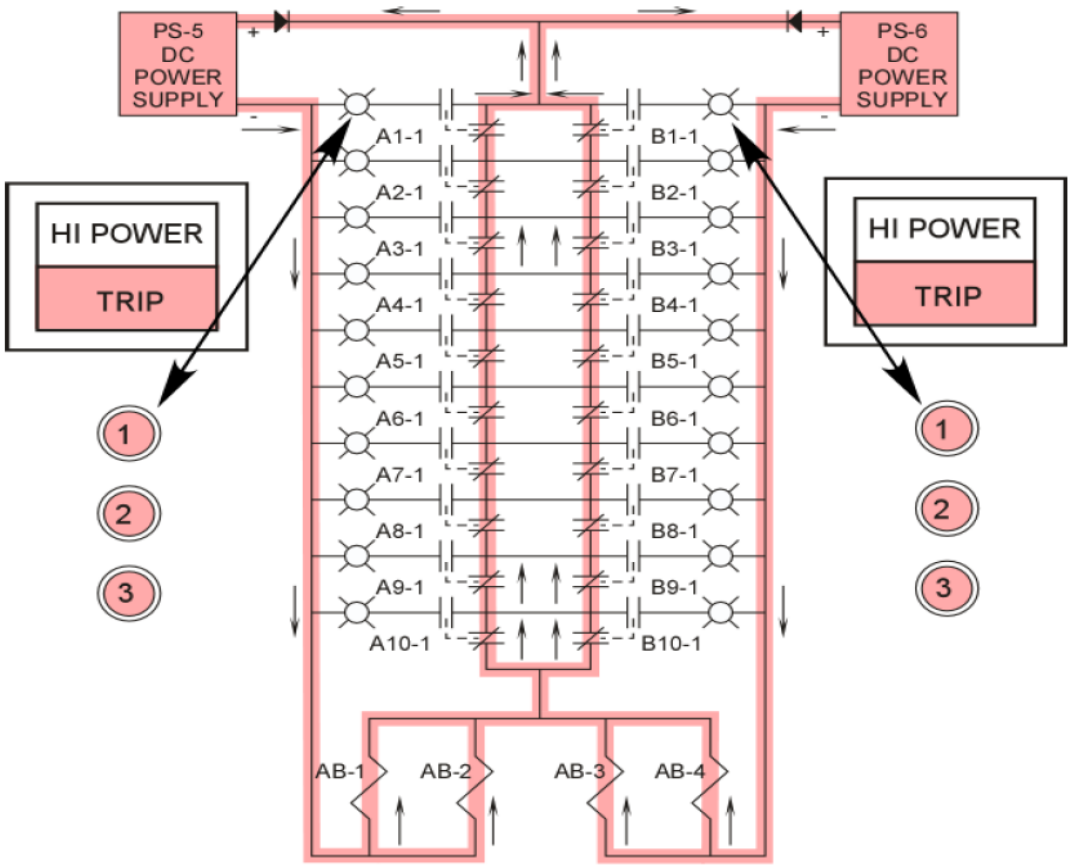
Configuration of AB Relay Matrices



Simplified Trip Logic Matrices



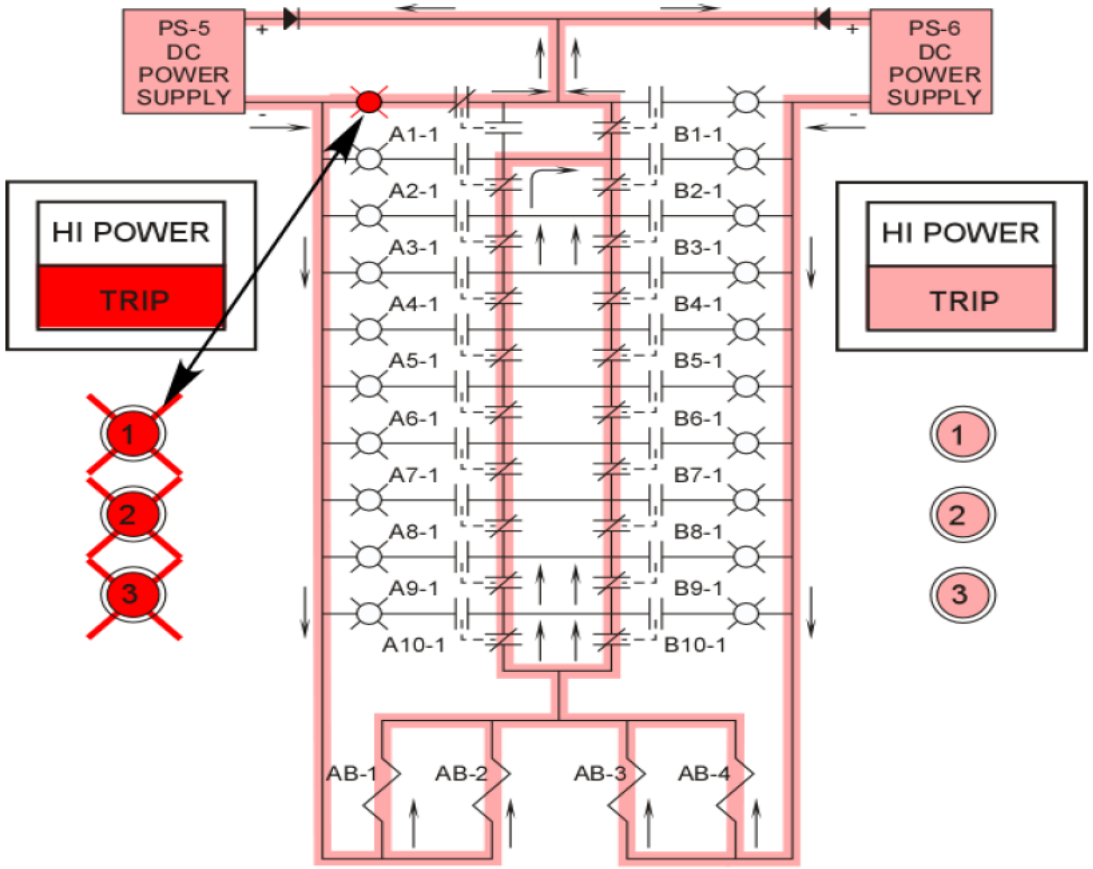
RPS AB Logic Matrix – Normal (untripped)



MATRIX SHOWN ENERGIZED
(NOT TRIPPED) CONDITION

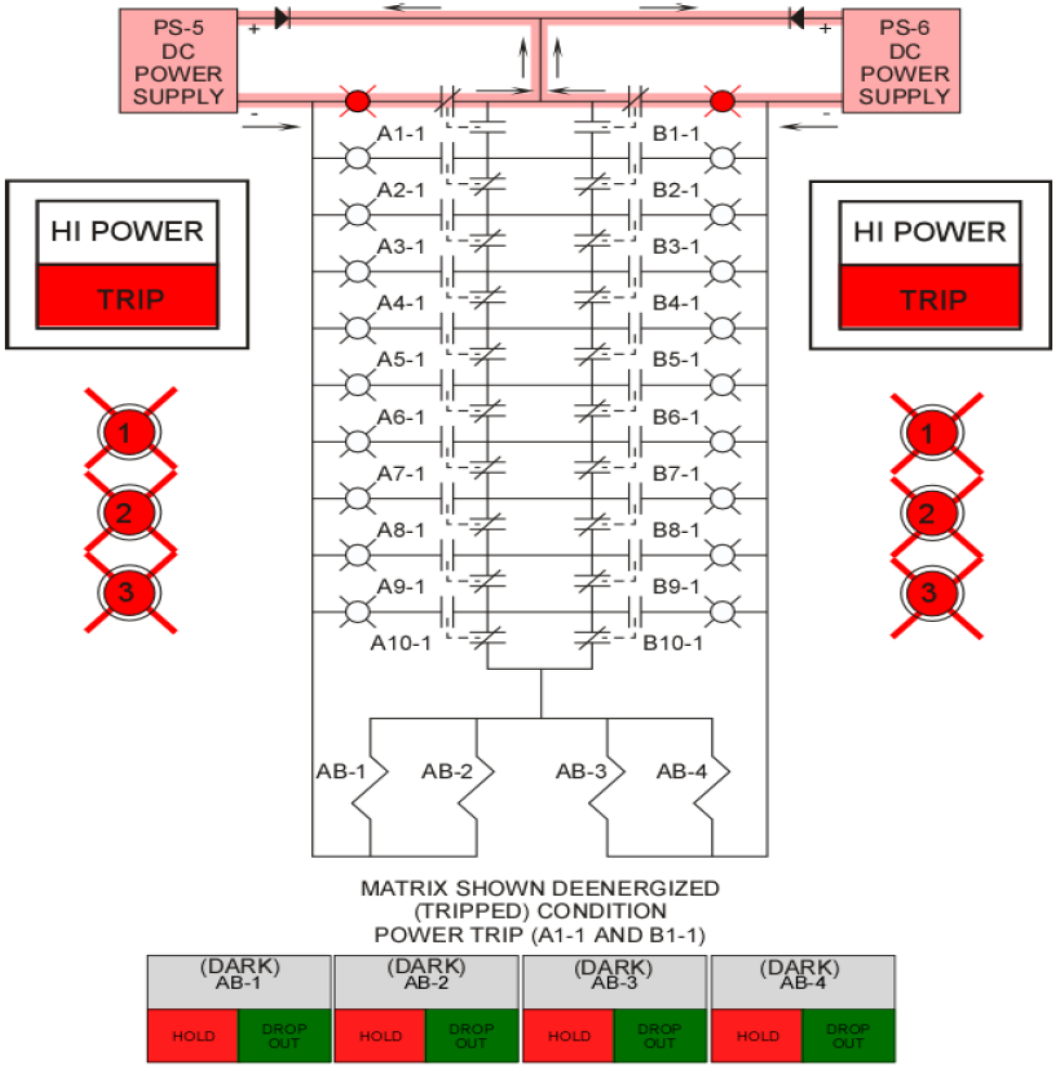
AB-1		AB-2		AB-3		AB-4	
HOLD	DROP OUT	HOLD	DROP OUT	HOLD	DROP OUT	HOLD	DROP OUT

RPS Logic Matrix – Channel A Tripped



MATRIX SHOWN WITH
POWER TRIP (A1-1) TRIPPED

RPS Logic Matrix – Channel A and B Tripped

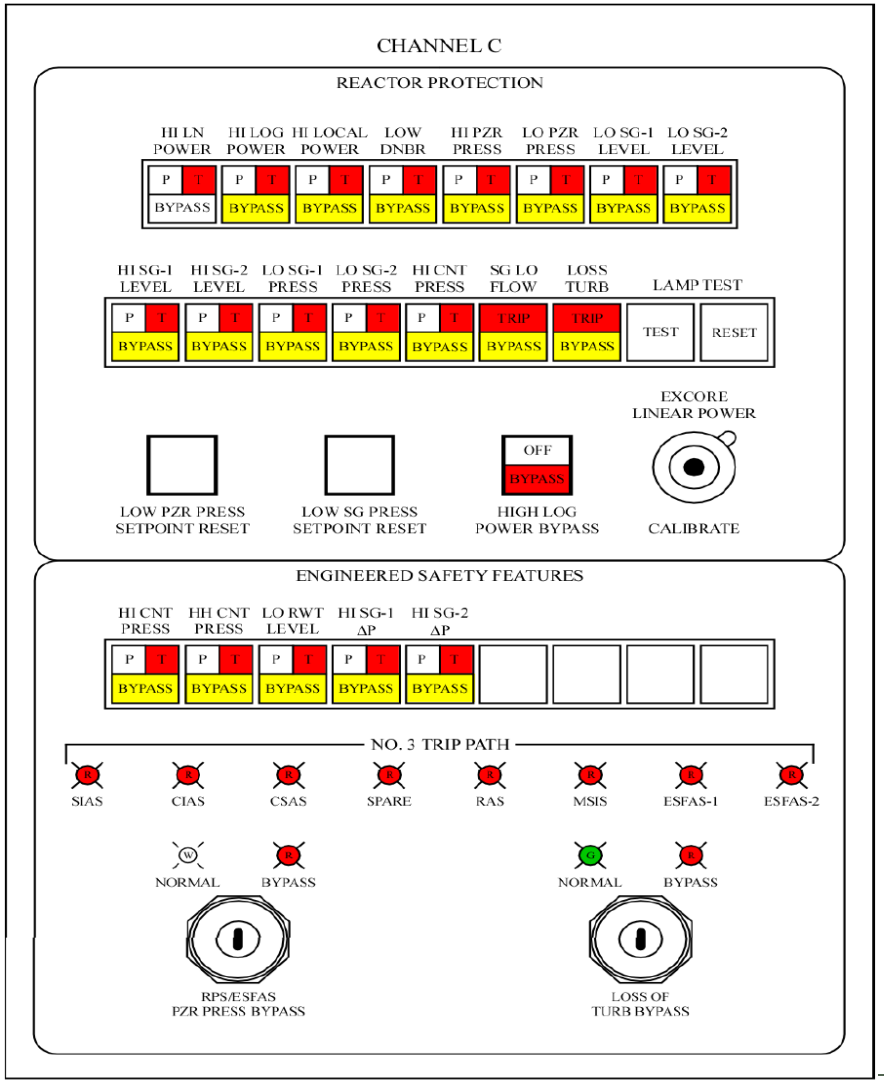


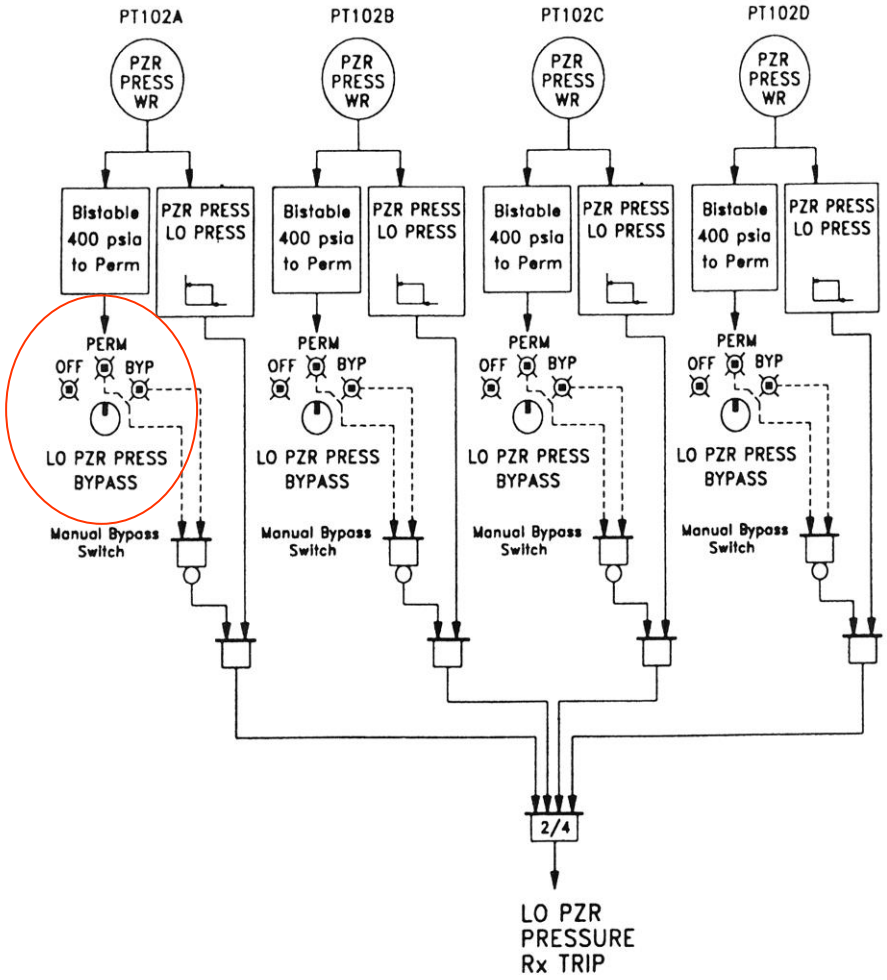
Operating Bypasses

Description

- Allows to bypass certain trips to permit plant operation during startup, shutdown, and low power testing conditions.
- Affects 4/4 protection channels for a particular trip function.
- Generally done via key switches in the Control Room. May also be done by pushbuttons or automatically.
- Generally have individual alarms associated with the bypass.

PPS Remote Operator Module



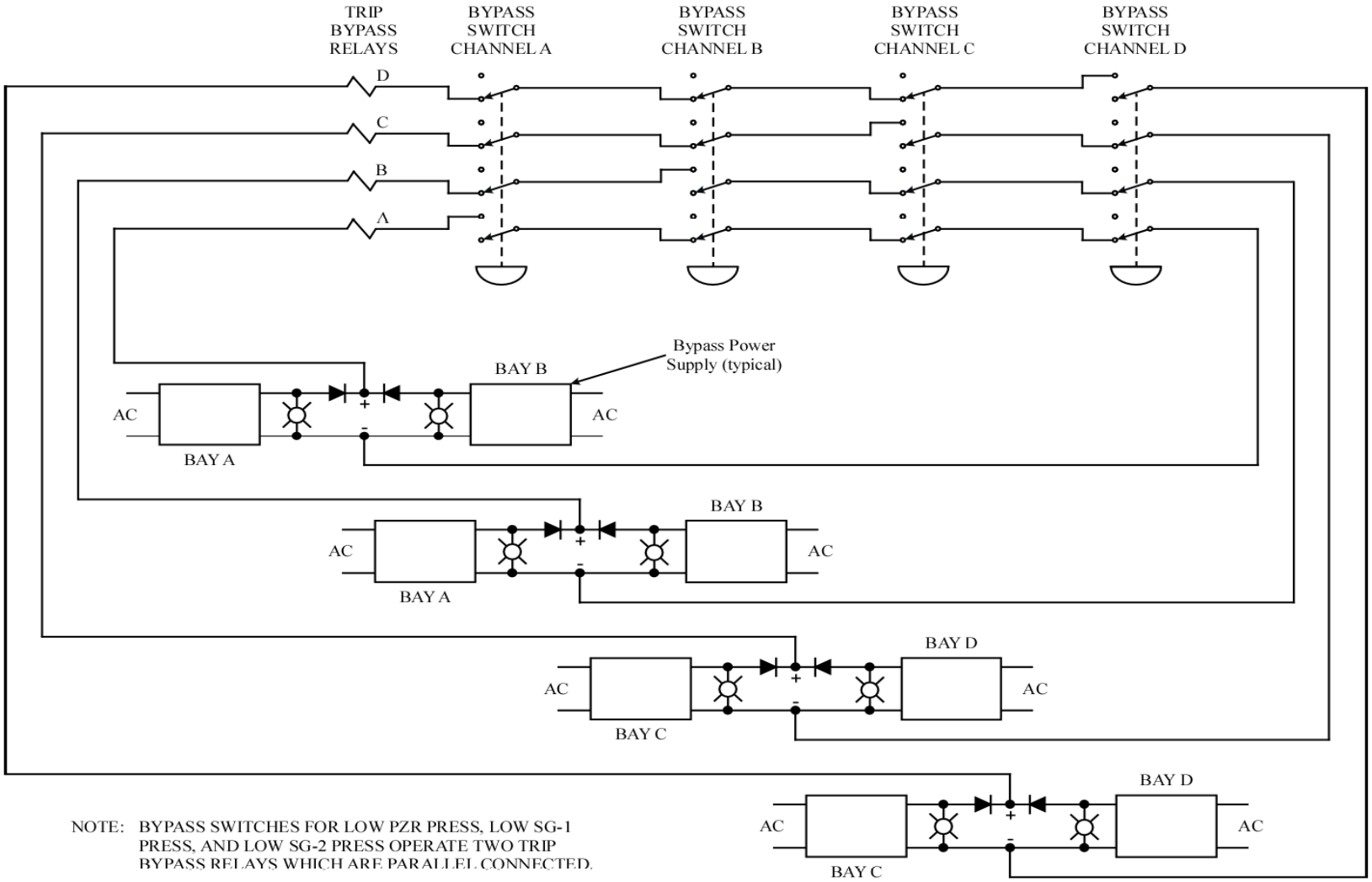


Trip Channel Bypass

Description

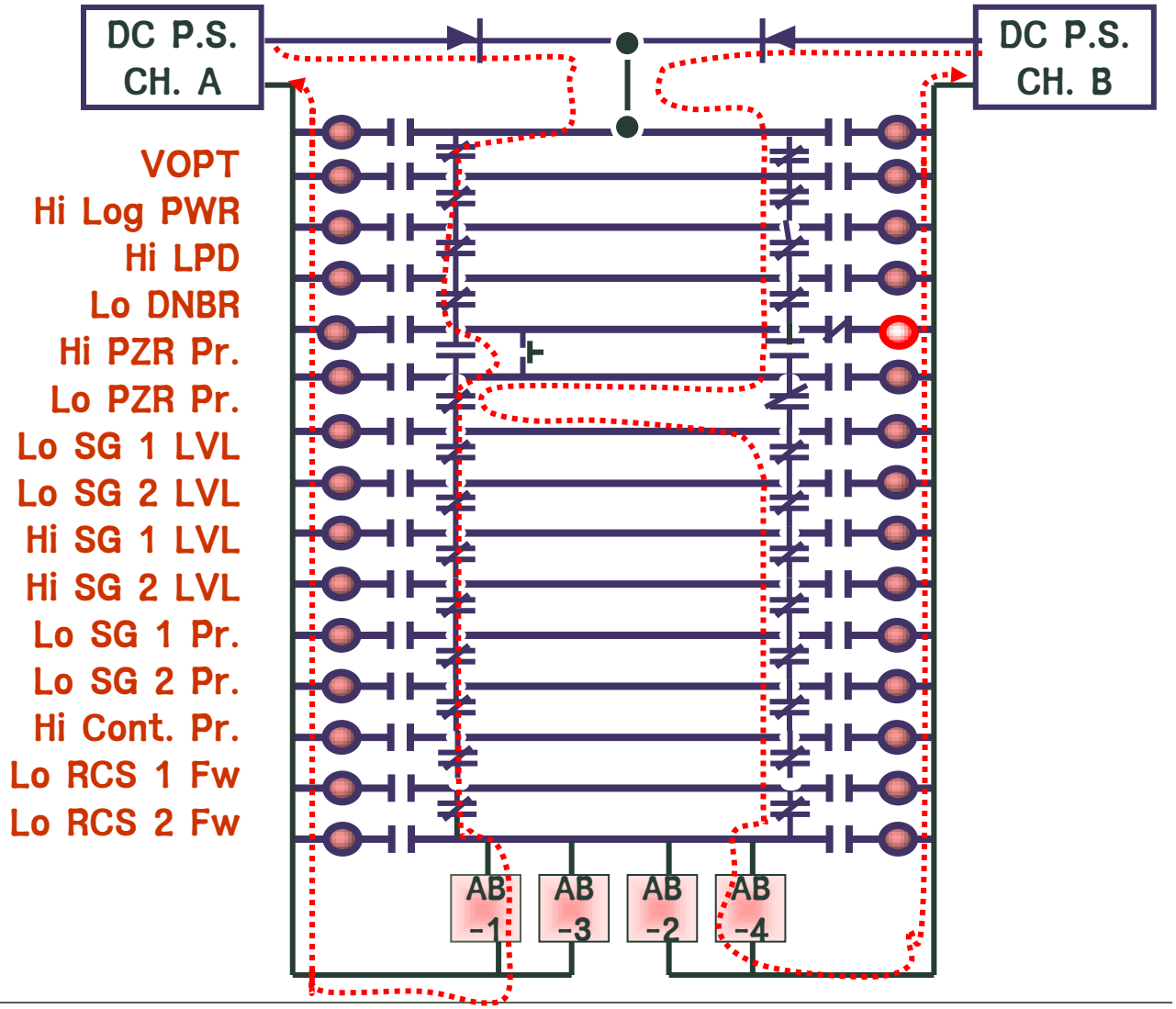
- All trip bistables have Trip Channel Bypass capability to remove them from service for testing or maintenance.
- When one channel bistable is in Trip Channel Bypass, the trip logic is converted to 2/3 by relying on the three remaining channels.
- There is an electrical interlock which allows only one channel for a given trip function to be bypassed at a time.
  - Attempting to bypass two channels at the same time unbypasses both channels.
- All trip channel bypasses annunciate a common alarm in the control room.

Trip Channel Bypass Electrical Interlock



Example of Channel A Bypassed

- Channel A & B trip, but Ch. A is bypassed.
- 2/4 logic is changed to 2/3 logic.
- In case of failure of a process variable, relevant channel shall be bypassed.
- When an excore channel fails, DNBR, LPD, VOPT variables are bypassed.



3. Engineered Safety Features Actuation System

Engineered Safety Features Actuation Systems

Functions

- Ensures that accident consequences are kept within acceptable limits
- Generates actuation signals for the ESF and ESF support systems
- Like the RPS, the ESFAS receives sensor inputs to feed bistables, 2/4 coincidence logic matrices, and trip paths to actuate devices
  - The RPS trip signals actuate the RTSG Trip CBs, but the ESFAS trip signals actuate various ESF system components, such as valves, pumps, and fans.

Engineered Safety Features Actuation Systems

ESFAS Trip Paths

- Sensor inputs are sent to trip normally energized bistables.
- These bistable use the same type of bistable comparator cards and bistable relay cards that the RPS bistables use.
- However, while RPS bistables use two bistable relay cards, ESF bistables use three bistable relay cards due to the additional outputs required for the two selective 2/4 logic schemes.
- Each trip path consists of six contacts in series, with each contact being fed from a 2/4 coincidence matrix.
- An open trip path actuates redundant SSRs which then send two independent trains of ESFAS signals to relays in each of the two Auxiliary Relay Cabinets.

Engineered Safety Features Actuation Systems

Design Bases

- Since both the RPS and the ESFAS are part of the PPS, they have the same design bases.

ESFAS Signals

- Safety Injection Actuation (SIAS)
  - The SIAS is generated by high containment pressure or by low pressurizer pressure.
    - Low pressurizer pressure is interpreted as either an RCS Loss of Coolant Accident(LOCA) or a Main Steam Line Break(MSLB) induced RCS cooldown.
    - High containment pressure is interpreted as either an RCS LOCA or a MSLB.

Engineered Safety Features Actuation Systems

ESFAS Signals

- Containment Isolation Actuation Signal (CIAS)
  - The CIAS is generated by high containment pressure or by low pressurizer pressure.
    - The CIAS interprets the low pressurizer pressure event as either an RCS LOCA or a MSLB.
    - High containment pressure is also interpreted as either an RCS LOCA or a MSLB.
- Containment Spray Actuation Signal (CSAS)
  - The CSAS is generated by high-high containment pressure coincident with an automatic SIAS.
    - This ensures that failure of both CSAS high-high containment pressure transmitters would not, by itself, cause a CSAS.

Engineered Safety Features Actuation Systems

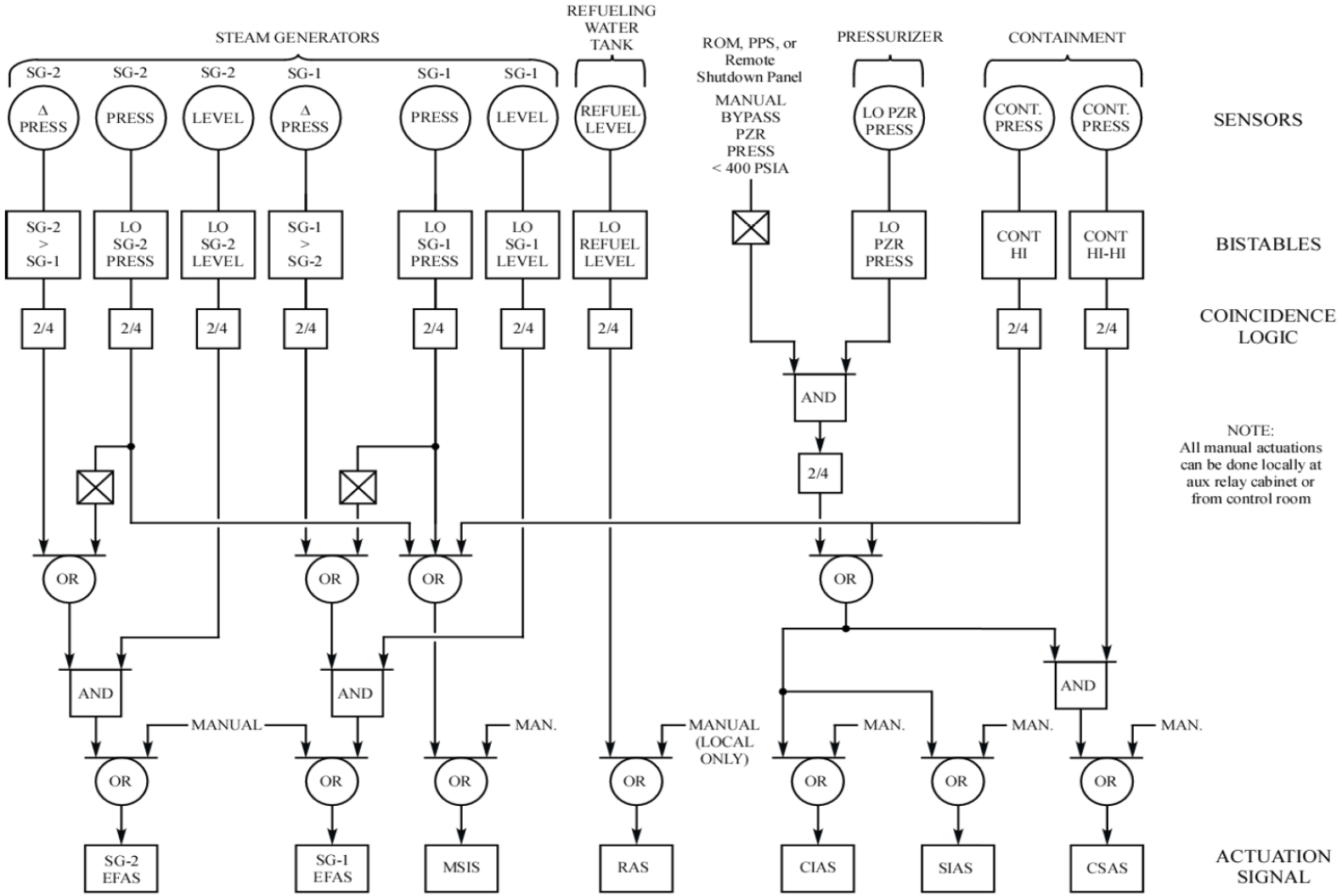
ESFAS Signals

- Main Steam Isolation Signal (MSIS)
  - The MSIS is generated by either high containment pressure or low steam pressure on either steam generator.
    - Both of these conditions are interpreted as MSLBs.
    - MSIS will close the main steamline isolation valves and the main feedwater isolation valves to isolate the steam release to the maximum extenet possible.
- Emergency Feedwater Actuation Signal (EFAS-1, EFAS-2)
  - The EFAS is generated by a low steam generator level coincident with that steam generator pressure being above the MSIS setpoint.

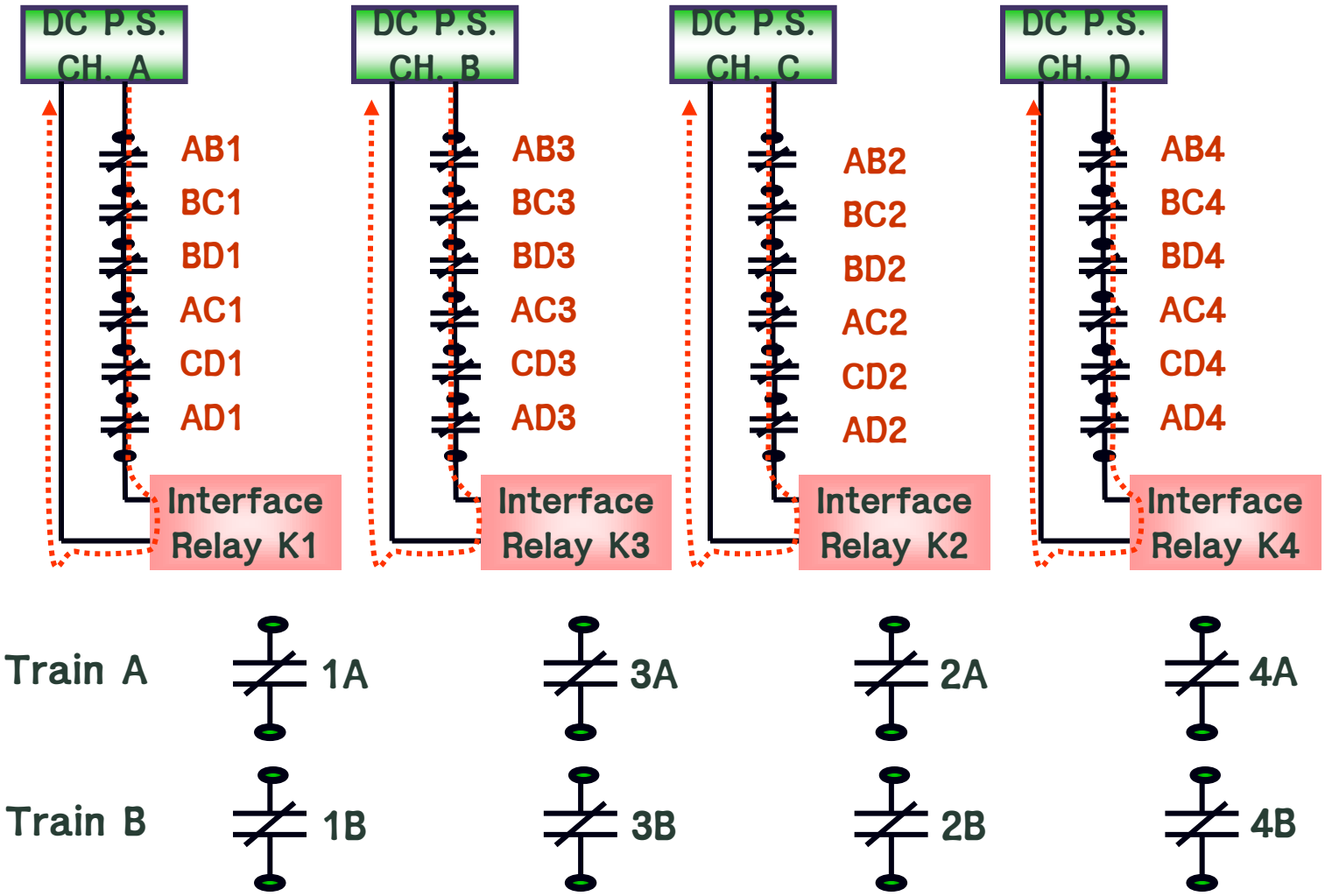
Engineered Safety Features Actuation Systems

- **ESFAS Signals**
  - Recirculation Actuation Signal (RAS)
    - The RAS is generated by RWT low water level.
      - This is interpreted to mean that a large LOCA is in progress since that is the most likely cause for a large drop in the RWT level.
- **Operating and Trip Channel Bypasses**
  - There are only two bypasses associated with the ESFAS; an operating bypass on SIAS(low pressurizer pressure) and a trip channel bypass
  - It is the same as the RPS bypasses in operating logic.
- **ESFAS Testing**
  - ESFAS testing is identical to RPS testing.
  - Like RPS testing, ESFAS testing is performed in an over-lapping manner such that the overall protection circuit is functionally tested.

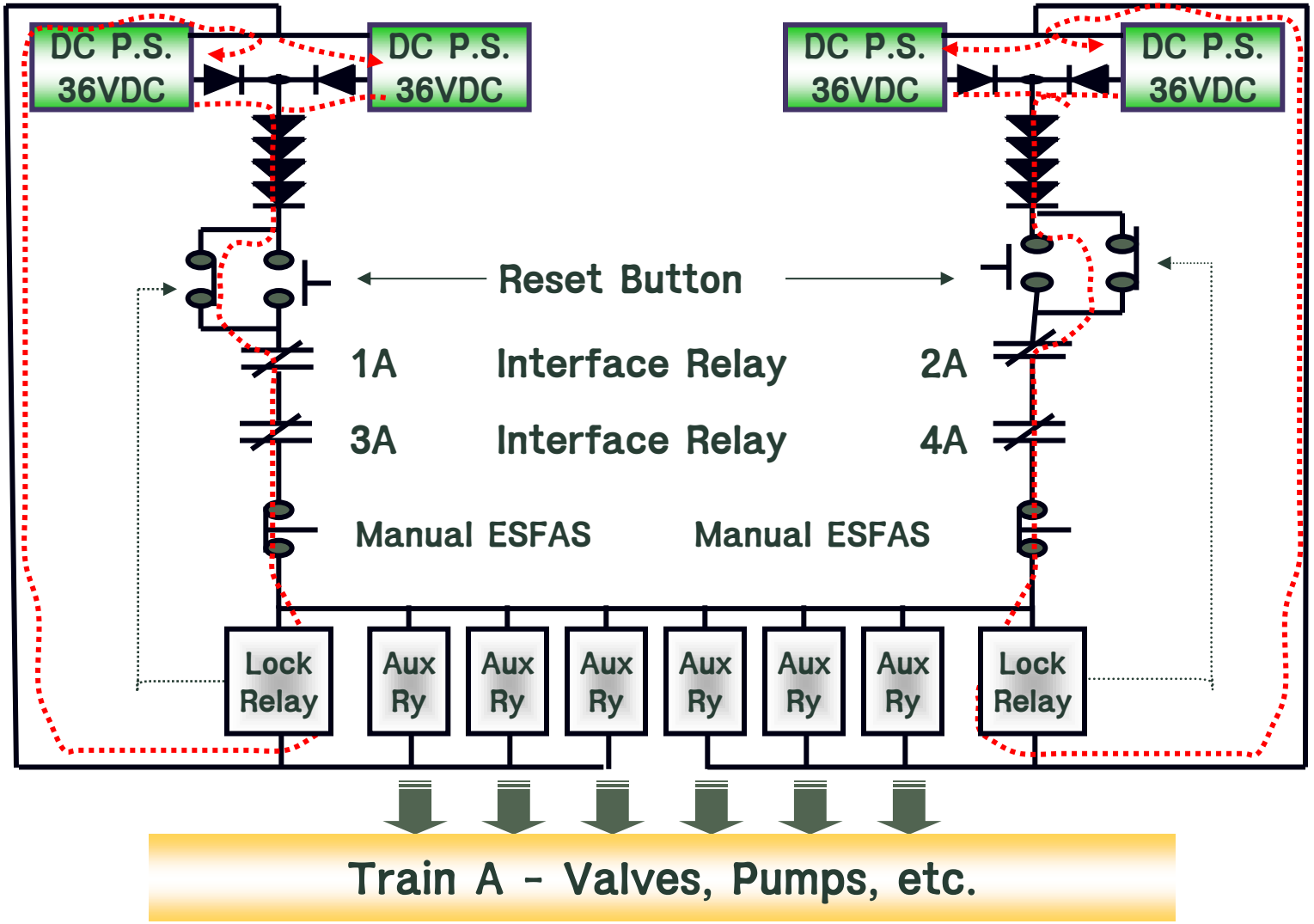
Overall ESFAS Logic Diagram



Simplified Initiation Logic Diagram



Simplified Selective 2/4 Initiation Logic Diagram

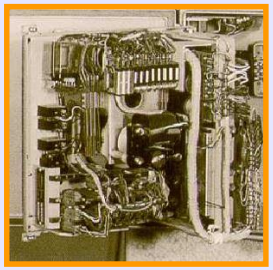


4. Digital Plant Protection System

Evolution of NPP I&C Systems in Korea

1st Generation

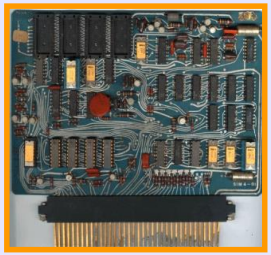
Relay Tech.



- Kori Unit 1

2nd Generation

Solid-state Tech.



- Kori 2,3,4
- Yonggwang 1,2
- Ulchin 1,2

3rd Generation

Hybrid Tech.

- Wolsong 1,2,3,4
- Yonggwang 3,4,5,6
- Ulchin 3,4

4th Generation

PLC-based Computer

- Ulchin 5,6
- Shin-Kori 1,2
- Shin-Wolsong 1,2

5th Generation

Advanced HMI Tech.

- Shin-Kori 3,4
- Shin-Ulchin 1,2

1970 1980 1990 2000 2010

Digital Plant Protection System

Functions

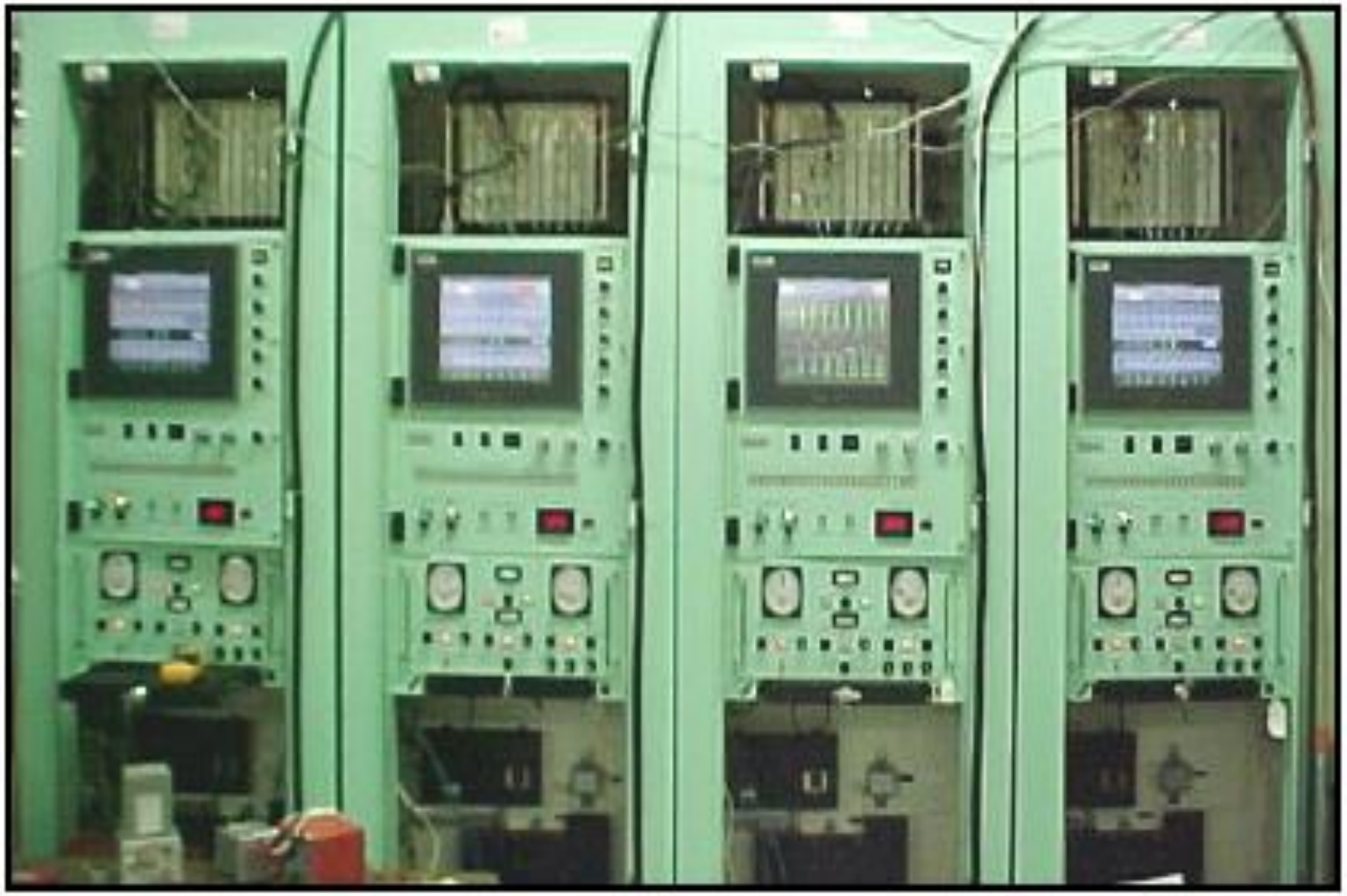
- Maintains plant safety by monitoring selected plant parameters, and initiating appropriate protective action when any parameter reaches a limiting setpoint.
- Generates signals to actuate Reactor Trip and Engineered Safety Features automatically whenever monitored processes exceed predefined limits.
  - The Reactor Trip provides an emergency shutdown of the reactor to protect the core and the RCS pressure boundary.
  - The Engineered Safety Features prevent the release of significant amounts of radioactive material to the environment.
- Selected plant parameters are monitored by four independent and redundant measurement channels that provide signals to separate DPPS channels.

Digital Plant Protection System

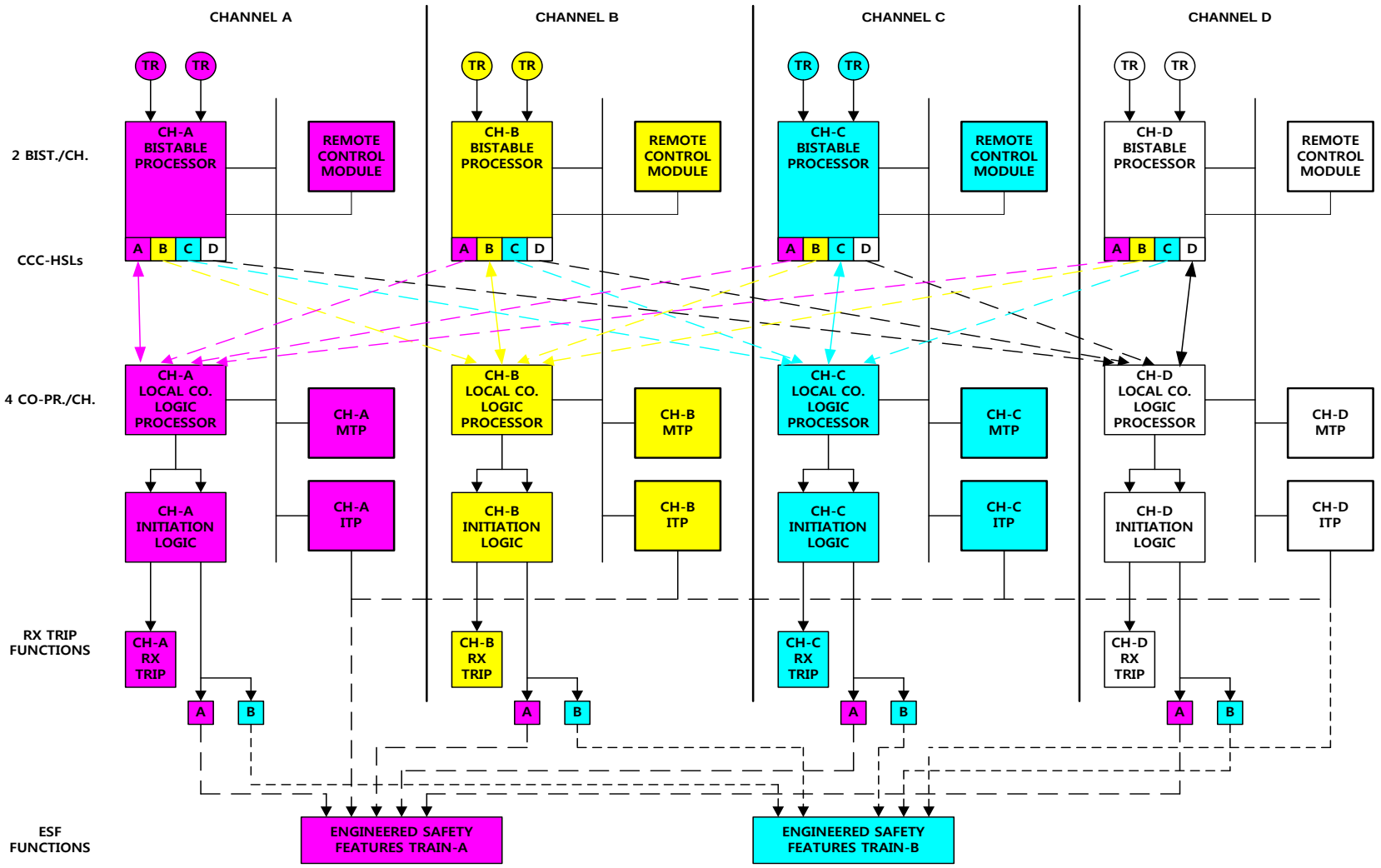
Configuration

- The DPPS is implemented via four identical equipment cabinets.
- Each cabinet contains modular equipment for a single DPPS Channel (Channel A, B, C, and D).
- Within each channel;
  - A set of two Bistable Processors (BP) perform the bistable function.
  - A set of four Local Coincidence Logic (LCL) Processors perform the coincidence logic function.
  - An Interface and Test Processor (ITP) provides for system testing and data reporting
  - A Maintenance and Test Panel (MTP) provides an operator interface to the DPPS from which system information can be displayed.

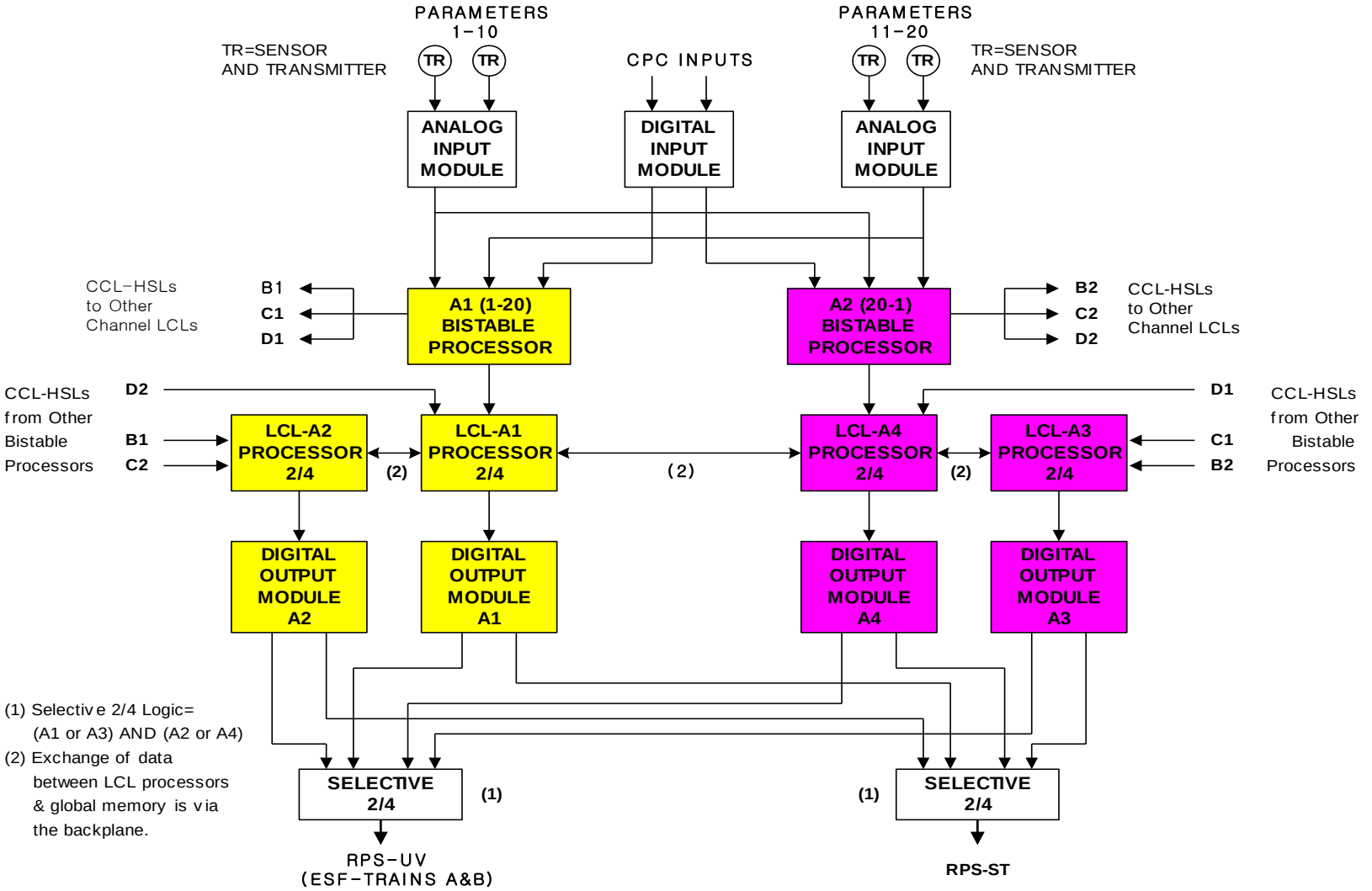
Four Channel DPPS Cabinets



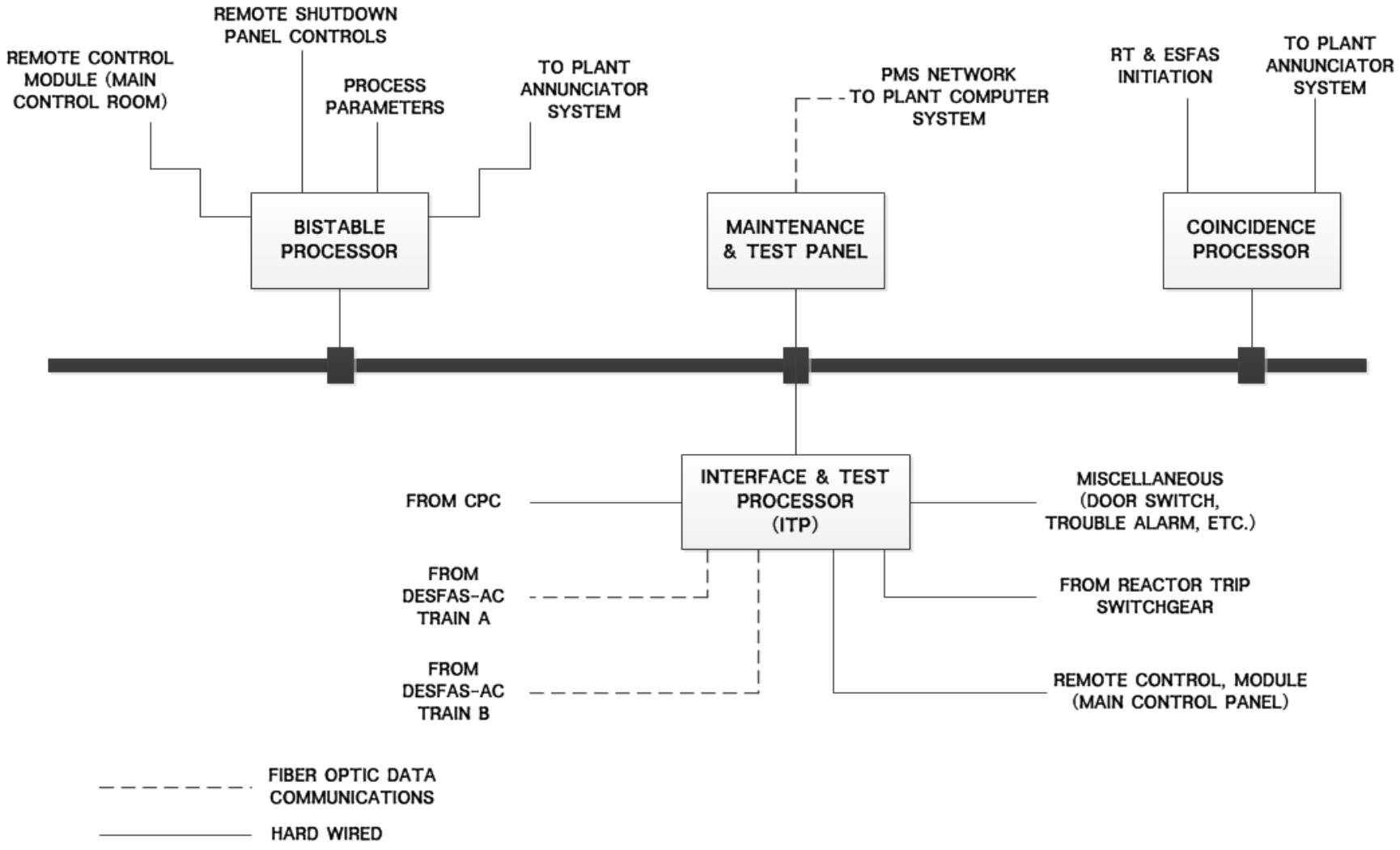
DPPS Basic Block Diagram



DPPS Channel A Trip Path Block Diagram

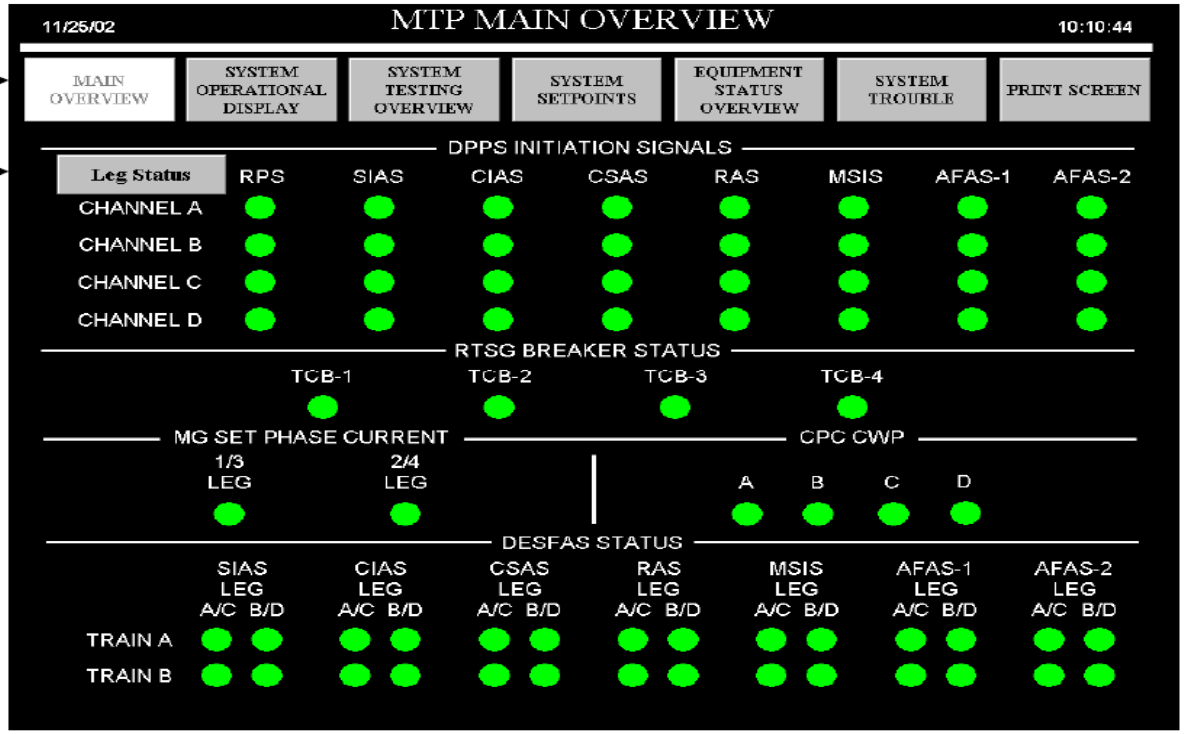


DPPS PLC Internal Network Diagram



MTP Main Overview Display Screen

Navigation Menu Bar

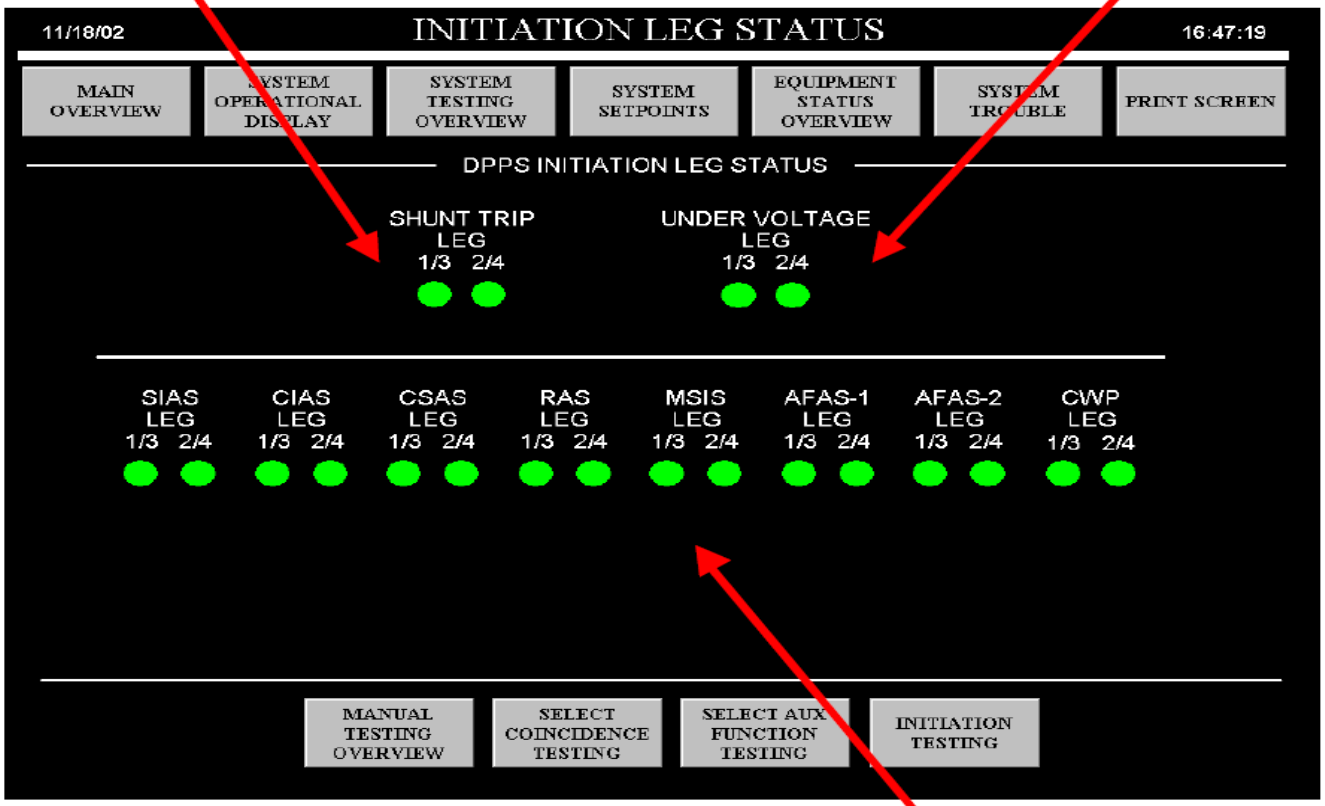


Switch allows access to the LEG STATUS display page

Initiation Leg Status Display

Status of DPPS Initiation Signals for a Shunt Trip (Reactor Trip)

Status of DPPS Initiation Signals for an Undervoltage Trip (Rector Trip)



Status of DPPS Initiation Signals for ESFAS Activations

Digital Engineered Safety Features Actuation System

Functions

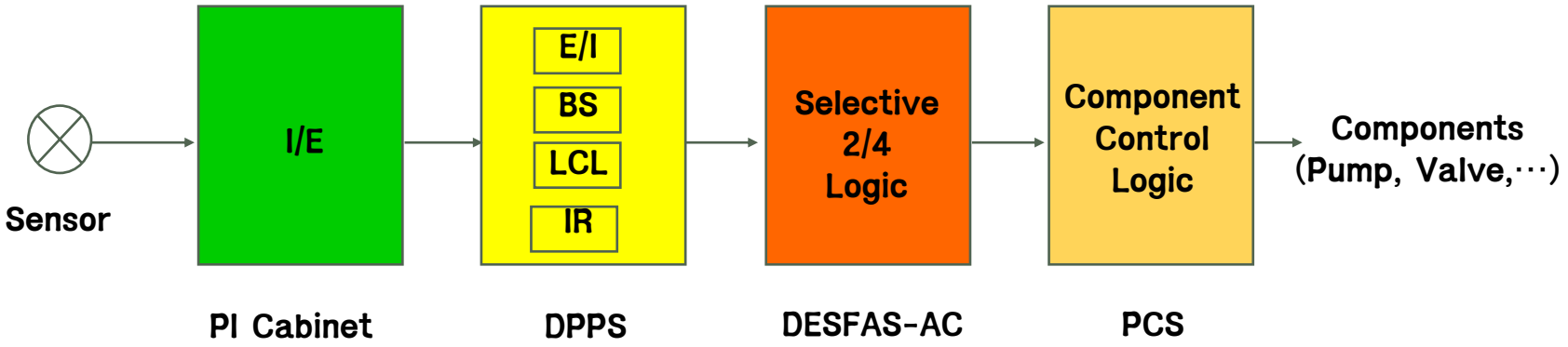
- The Digital ESFAS cabinets are an extension of the DPPS, and is used for interfacing between the DPPS cabinet and various plant equipment and components such as pumps and valves which comprising the ESF systems
- The DESFAS provides actuation of the following independent ESF systems
  - Safety Injection Actuation Signal
  - Containment Isolation Actuation Signal
  - Containment Spray Actuation Signal
  - Main Steam Isolation Signal
  - Recirculation Actuation Signal
  - Auxiliary Feedwater Actuation Signal-1 and -2

Digital Engineered Safety Features Actuation System

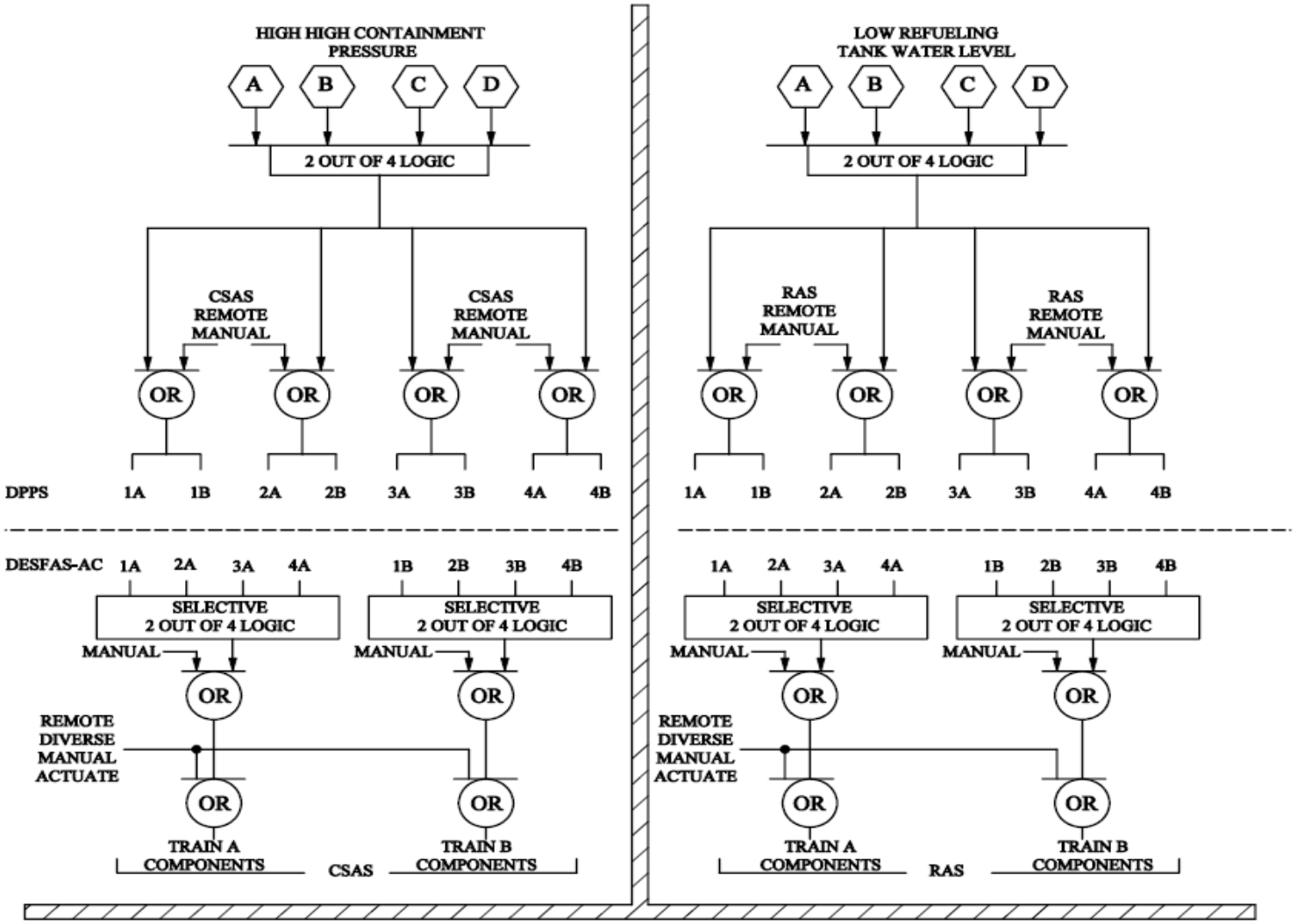
DESFAS Signal Flow Paths

- The DPPS cabinet provides four signals for each DESFAS function for each of the two DESFAS cabinets.
- Initiation output signals from the DPPS are transmitted to DESFAS via Fiber Optic Transmitters(FOT) as follows;
  - ESFAS initiation signals for ESF Train A
  - ESFAS initiation signals for ESF Train B
- Each DESFAS train performs a selective 2/4 actuation logic for each ESF function, as transmitted by the four channel DPPS
- When a valid initiation condition exists, the appropriate valves and pumps for the initiated ESF functions are activated.

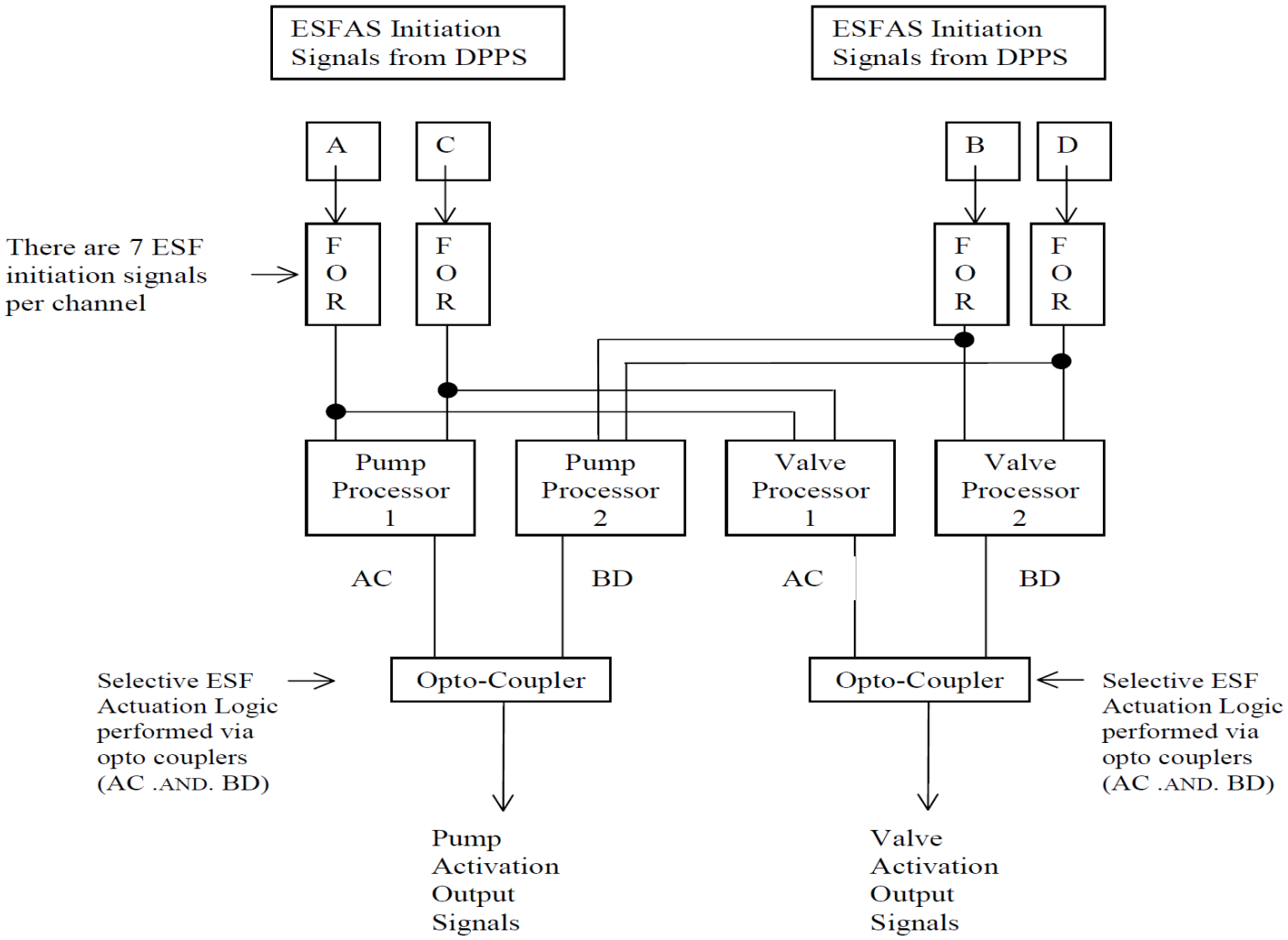
Simplified DESFAS Signal Flow Path



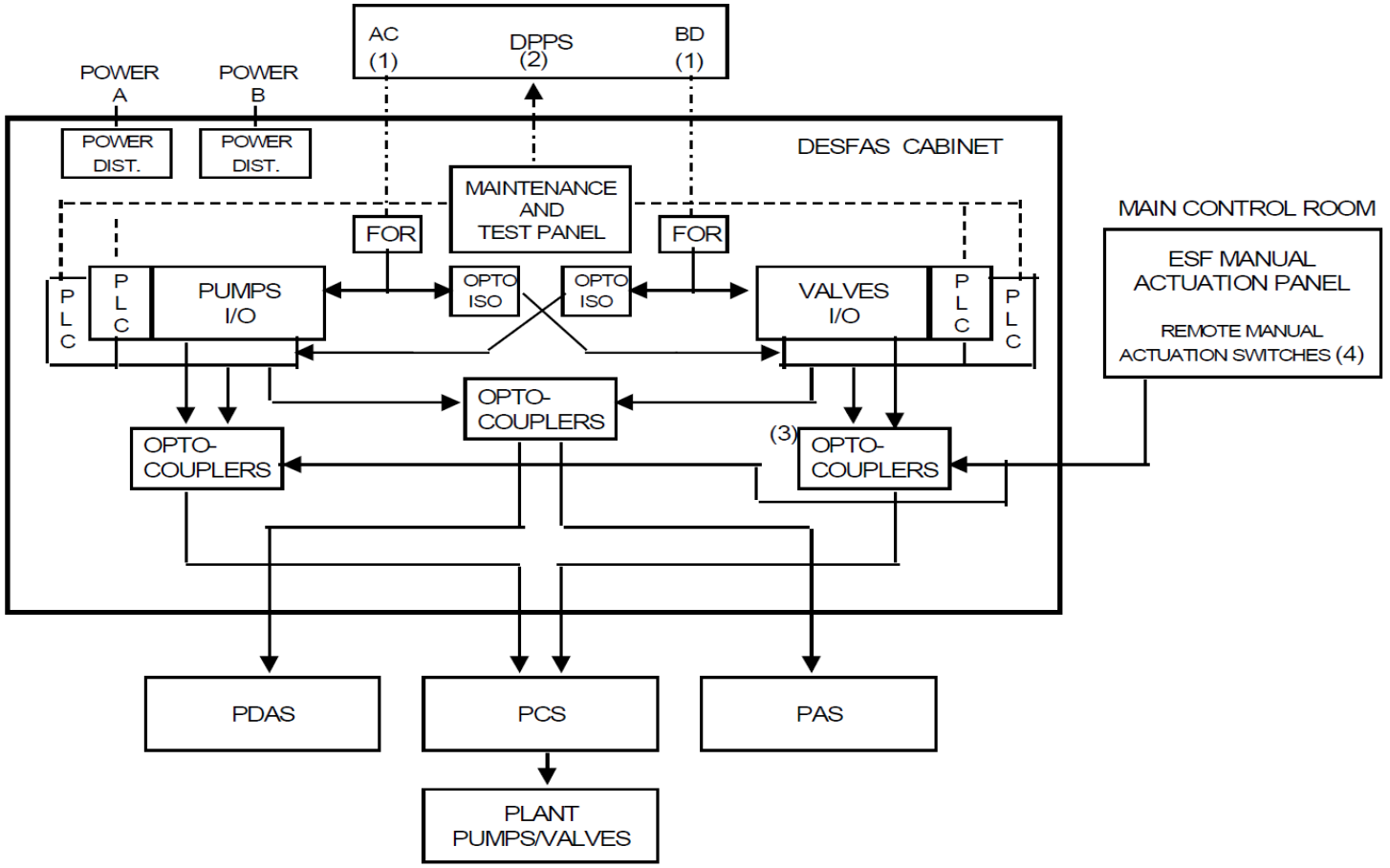
Typical DESFAS Actuation Logic Diagram



Simplified DESFAS Function Actuation Path



DESFAS-AC Basic Block Diagram

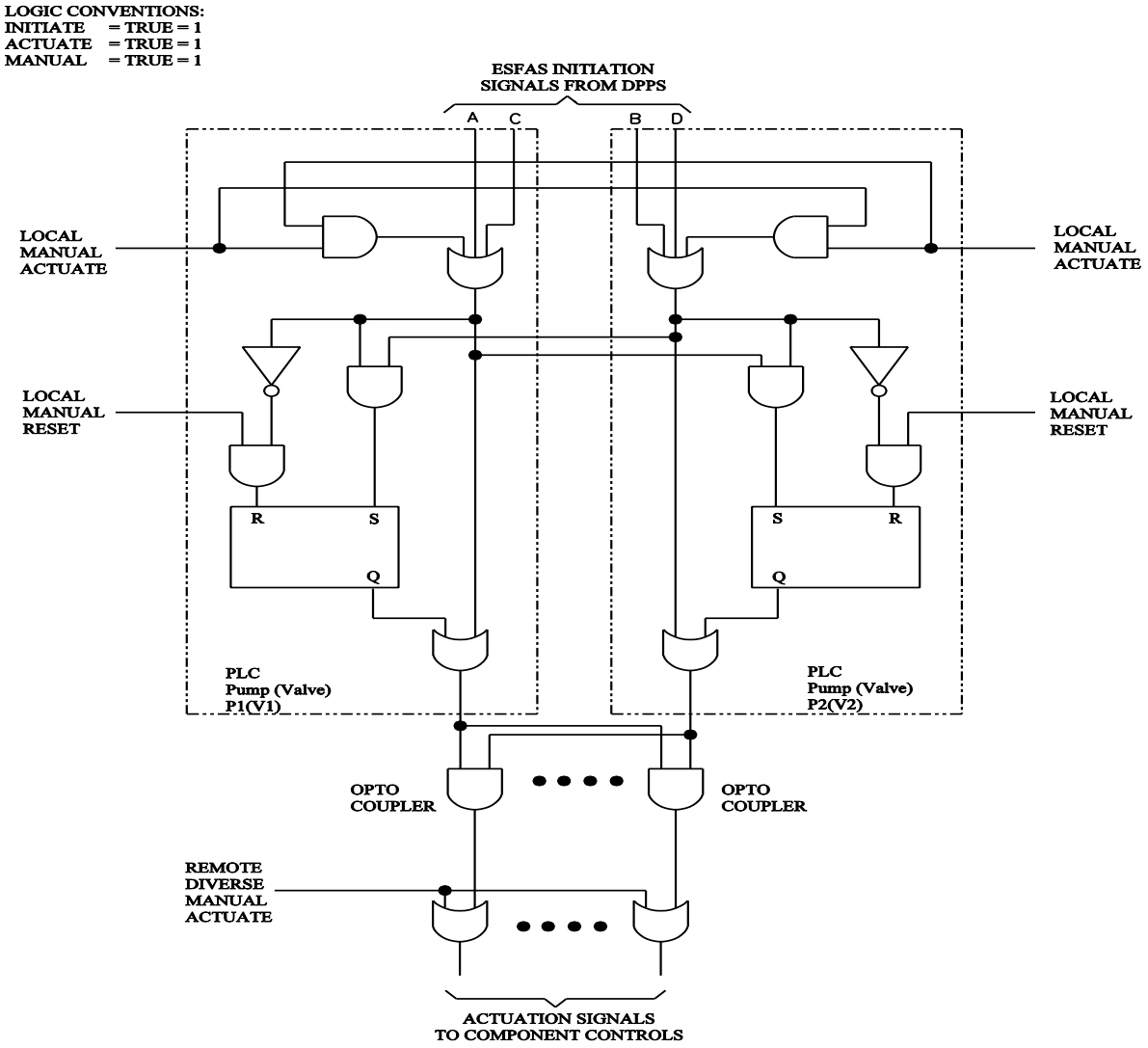


NOTES:
(1) ESFAS fiber optic initiation signals (A,B,C&D)
(2) ESFAS fiber optic status/test feedback signals
(3) Includes isolated redundant channel outputs
(4) Two manual switches for each ESF function
(5) FOR = Fiber Optic Receiver, ISO = Isolation device.

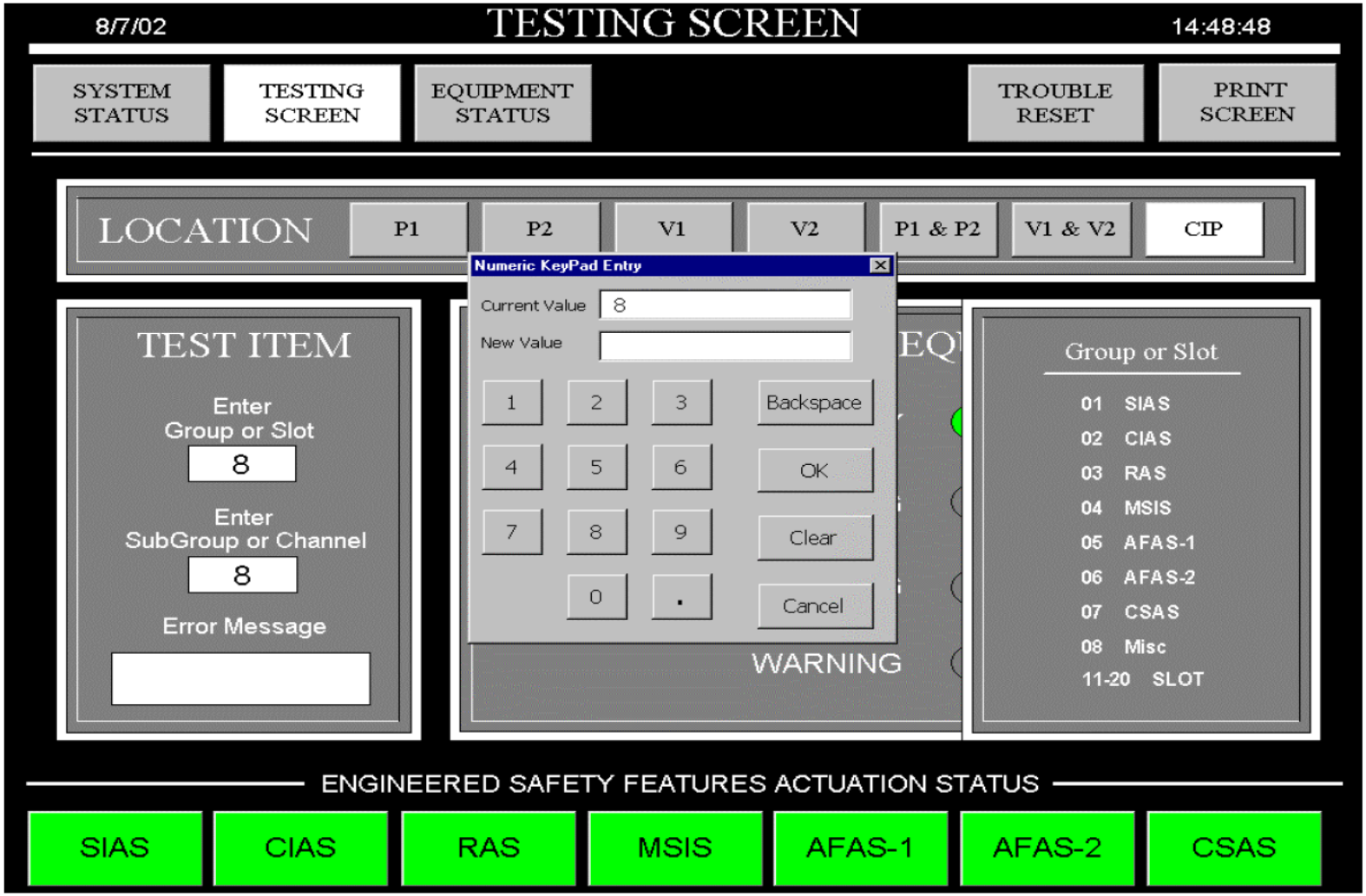
DATA LINK
HARDWIRED INTERFACE
FIBER OPTIC

File:FIG721d.PPT CFR 03 / 30 / 99

DESFAS Selective 2/4 Logic Diagram



DESFAS MTP Testing Screen Display



5. Diverse Protection System

Diverse Protection Systems

Functions

- The DPS augments the PPS to address 10 CFR 50.62 requirements for reduction of risk from ATWS events.
- The DPS assists the mitigation of the effects of a postulated CCF of the digital computer logic within the DPPS.
- The DPS can be broken down into a reactor trip and an auxiliary feedwater actuation.
  - A reactor trip signal causes CEDM motor-generator set output breaker to open and drop the CEA into the reactor core.
  - The DPS automatically initiates the auxiliary feedwater actuation system when either steam generator water level falls below a predetermined setting.

Diverse Protection Systems

Design Bases

- The DPS is designed to comply with the requirements 10 CFR 50.62.
  - The DPS is designed to provide adequate protection during an AOO followed by failure of the reactor trip of the plant protection system.
- The DPS is designed to comply with the USNRC staff requirements memorandum regarding SECY 93-087, II.Q (Defense-in-Depth and Diversity), as referenced by NUREG-0800, BTP 7-19 (4-point positions).
  - On high containment pressure, the DPS automatically initiates reactor trip against a postulated CCF of the digital computer logic within the DPPS.
- The diverse manual ESF system actuations are provided to allow manual control capability in the event of a postulated CCF of the DPPS and DESFAS.

Diverse Protection Systems

- **Four-Point Positions Regarding Diversity**
  - Applicant shall do a D-in-D&D assessment
  - Common mode failure vulnerabilities shall be adequately addressed.
  - In the assessment, possible common mode failures shall be postulated for each Chapter 15 event.
  - Effects of the combined failure plus event sequence shall be calculated using "best estimate" methods.
  - The analysis shall demonstrate "adequate diversity."

Diverse Protection Systems

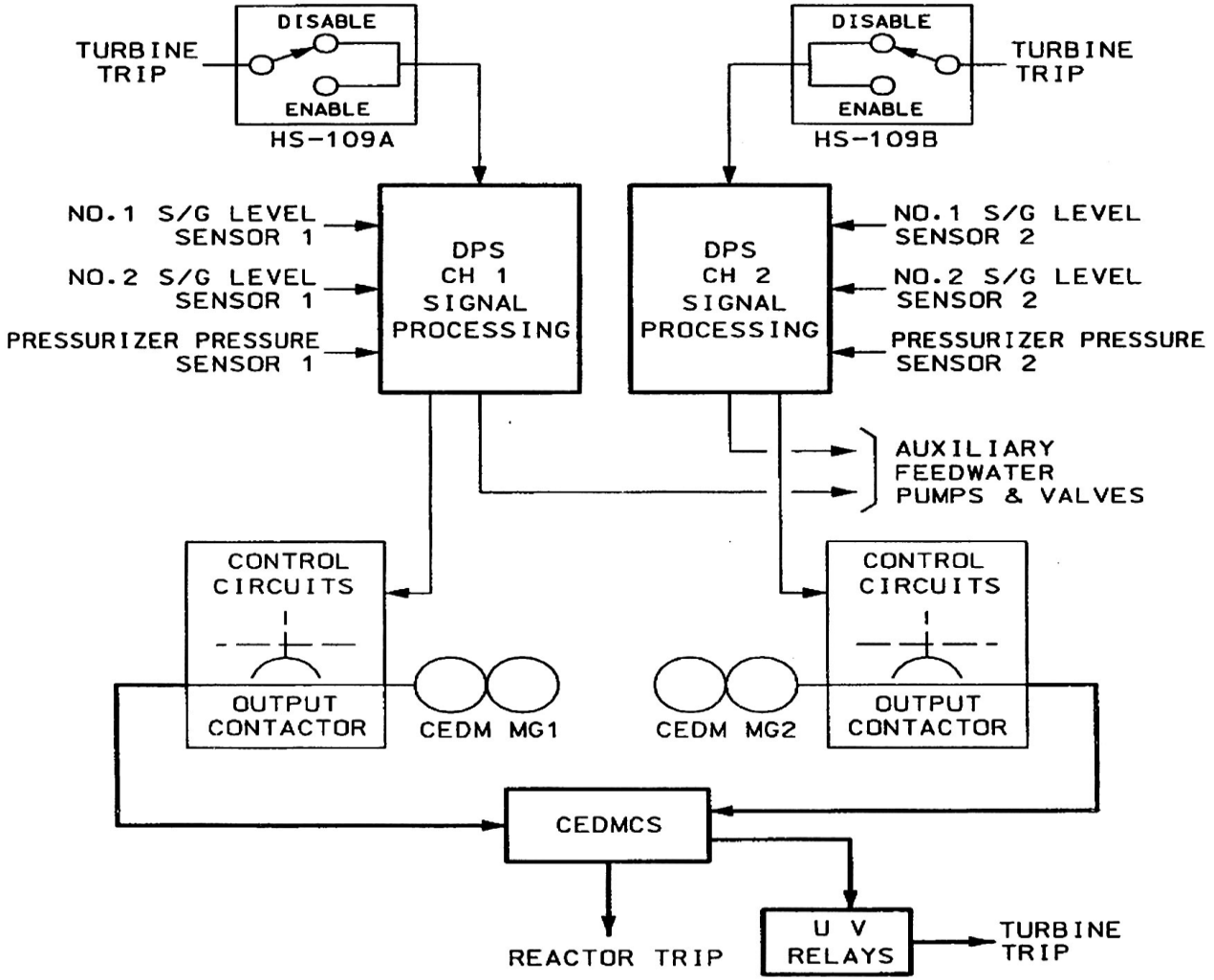
Four-Point Positions Regarding Diversity

- The diverse response shall be unlikely to be subject to the same common mode failures.
- The diverse response shall perform "either the same function or a different function."
- High quality, non-safety equipment may provide the diverse response to common mode failures (only).
- A set of manual controls and displays (not subject to the same common mode failures) shall be provided in the main control room to perform system-level actuation of critical safety functions.

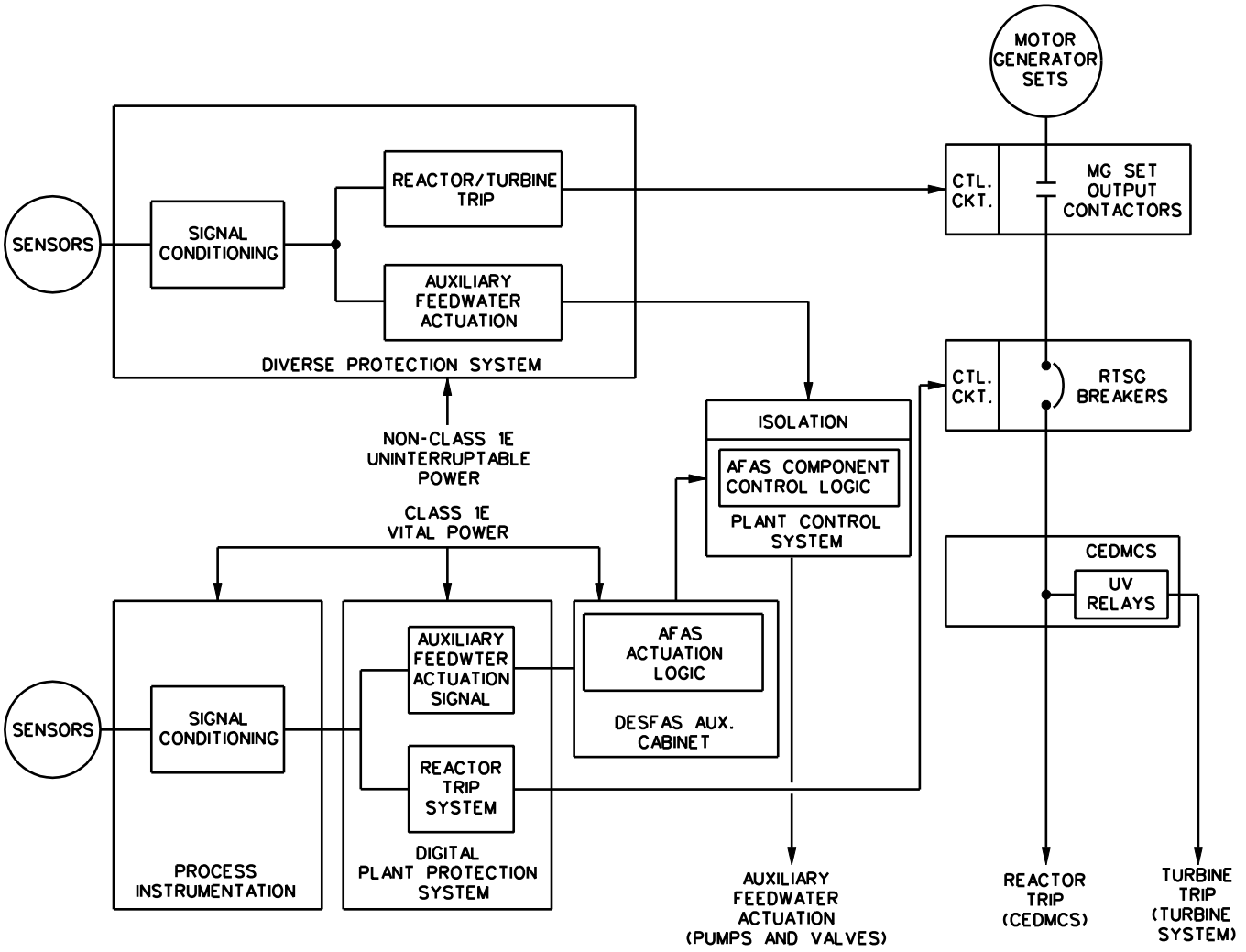
Diverse Protection Systems

- **Diverse Reactor Trip Signals**
  - High Pressurizer Pressure
  - High Containment Pressure
  - Reactor Trip by Turbine Trip
  - Manual Reactor Trip
- **Diverse Auxiliary Feedwater Actuation Signals**
  - Steam Generator No. 1 – Low Level
  - Steam Generator No. 2 – Low Level
- **Diverse Manual ESF System Actuation Signal**

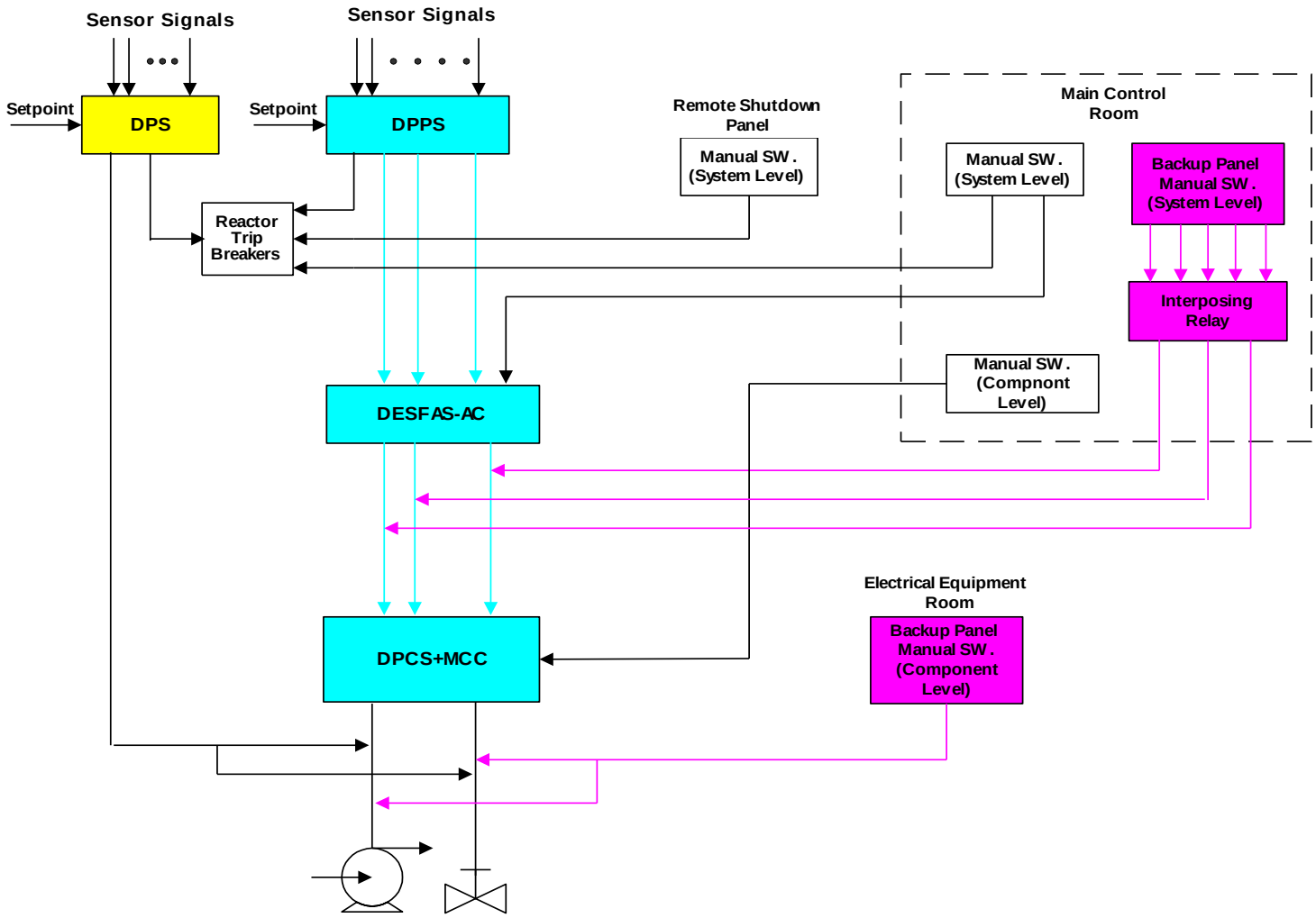
Diverse Protection System Functional Diagram



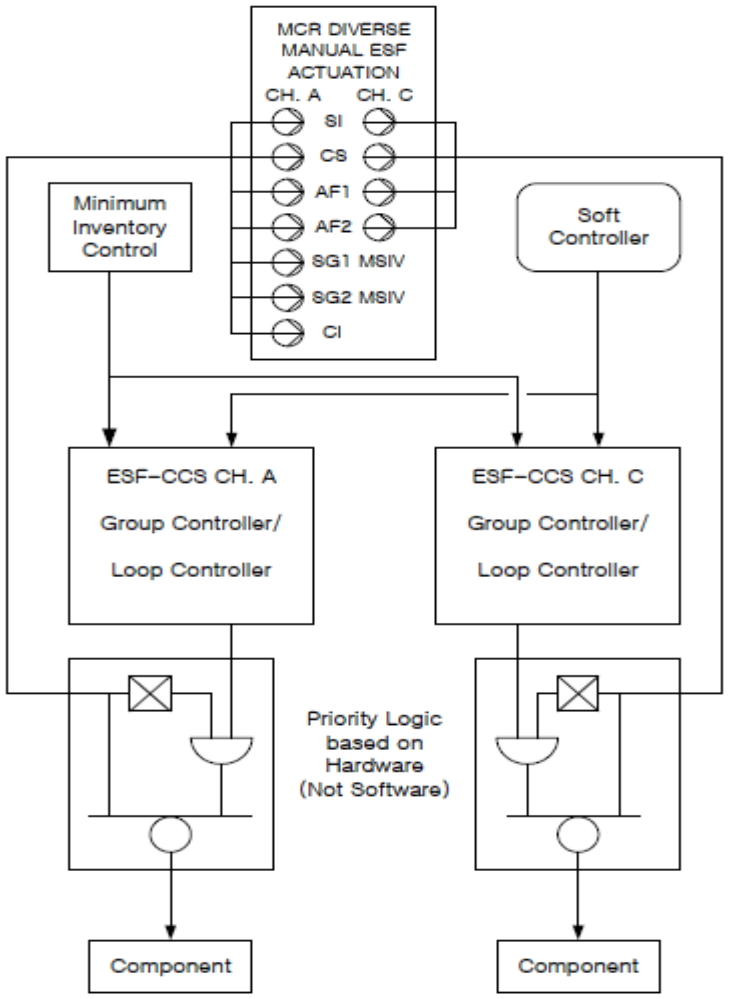
DPS and Auxiliary Feedwater Actuation Diagram

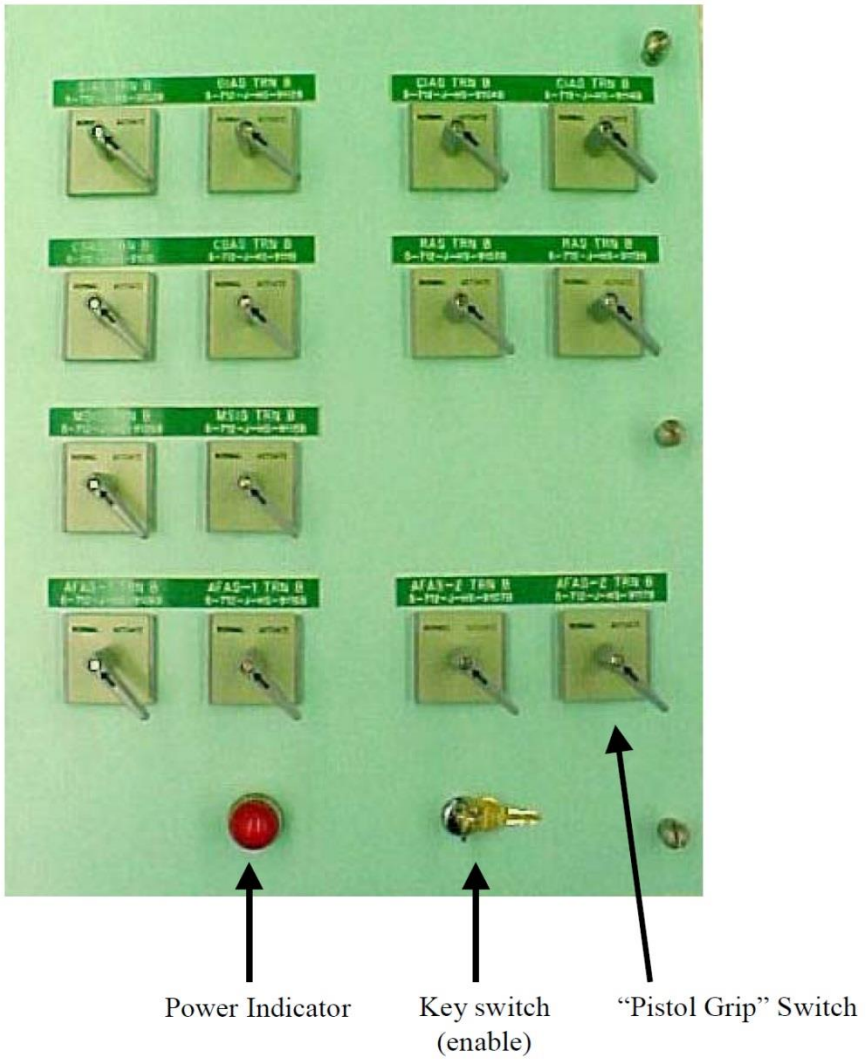


Diverse Manual ESF System Actuation



Diverse Manual ESF Actuation in MCR





Always we keep watching our Atomic Power

Name : Kim, Bok Ryul
E-mail : k060kbr@kins.re.kr

Thank You

한국원자력안전기술원
KOREA INSTITUTE OF NUCLEAR SAFETY