U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Instrumentation & Control Systems

AP1000 Technology Chapter 8.0

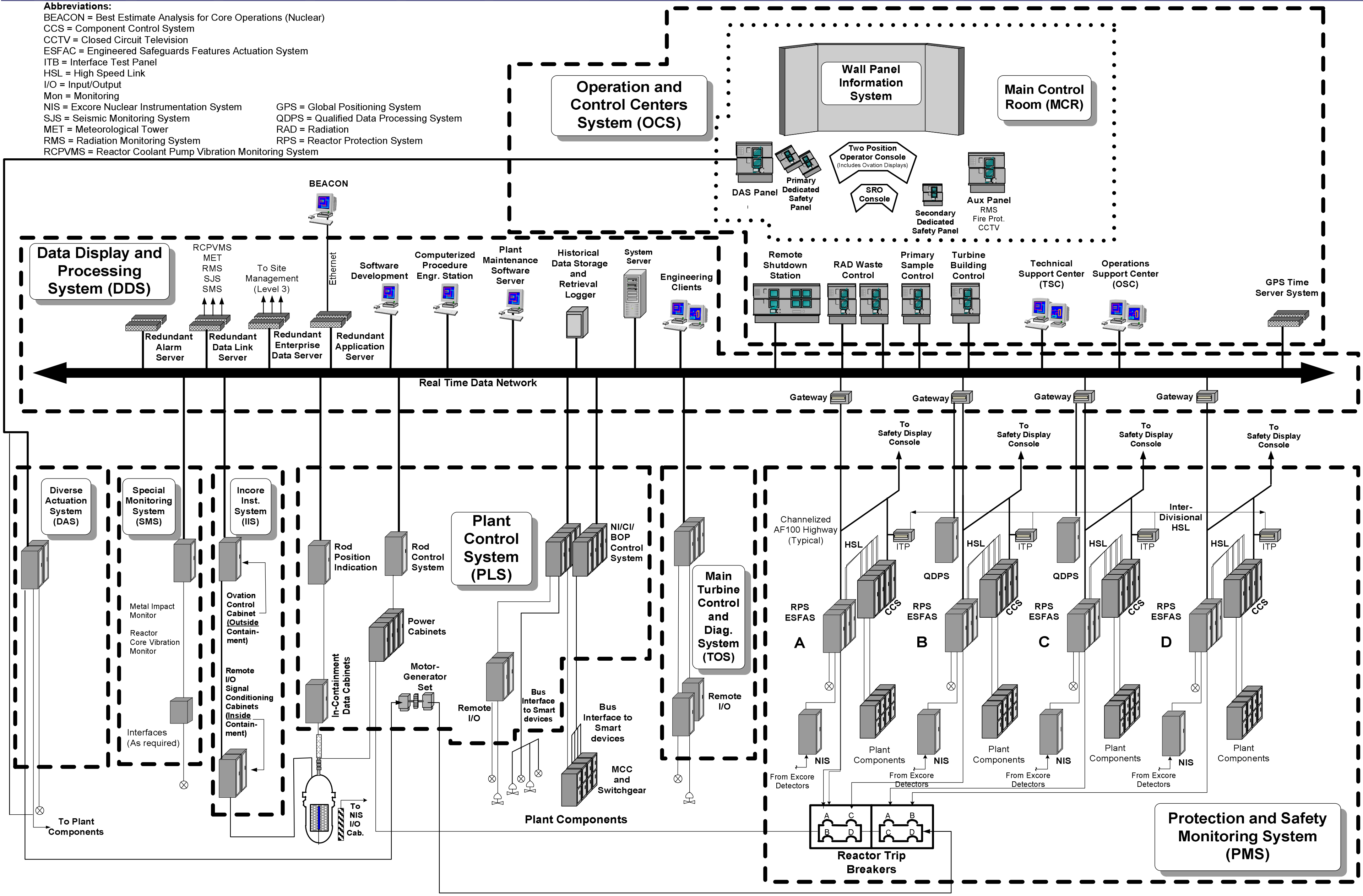
HRTD
Human Resources Training & Development

Learning Objectives:

1. State the purposes of the following:
   a. Protection and Safety Monitoring System
   b. Reactor Trip System
   c. Engineered Safety Features Actuation System
   d. Control Systems
   e. Diverse Actuation System
2. Describe the major differences between the AP1000 and current operating Westinghouse plants' control and instrumentation system designs.

Fig. 8-1 (Expanded) – I&C Architecture

Abbreviations:
BEACON = Best Estimate Analysis for Core Operations (Nuclear)
CCS = Component Control System
CCTV = Closed Circuit Television
ESFAC = Engineered Safeguards Features Actuation System
ITB = Interface Test Panel
HSL = High Speed Link
I/O = Input/Output
Mon = Monitoring
NIS = Excore Nuclear Instrumentation System
SJS = Seismic Monitoring System
MET = Meteorological Tower
RMS = Radiation Monitoring System
RCPVMS = Reactor Coolant Pump Vibration Monitoring System
GPS = Global Positioning System
QDPS = Qualified Data Processing System
RAD = Radiation
RPS = Reactor Protection System



Digital Platforms

- Protection (PMS): Common Q (ABB/CE)
  - Already used in existing nuclear plant applications
- Control (PLS): Ovation (Emerson)
  - Expert distributed control system
  - Already used in existing nuclear & fossil-fueled plants
- Diverse platforms should ensure common-mode failure cannot disable both protection & control.

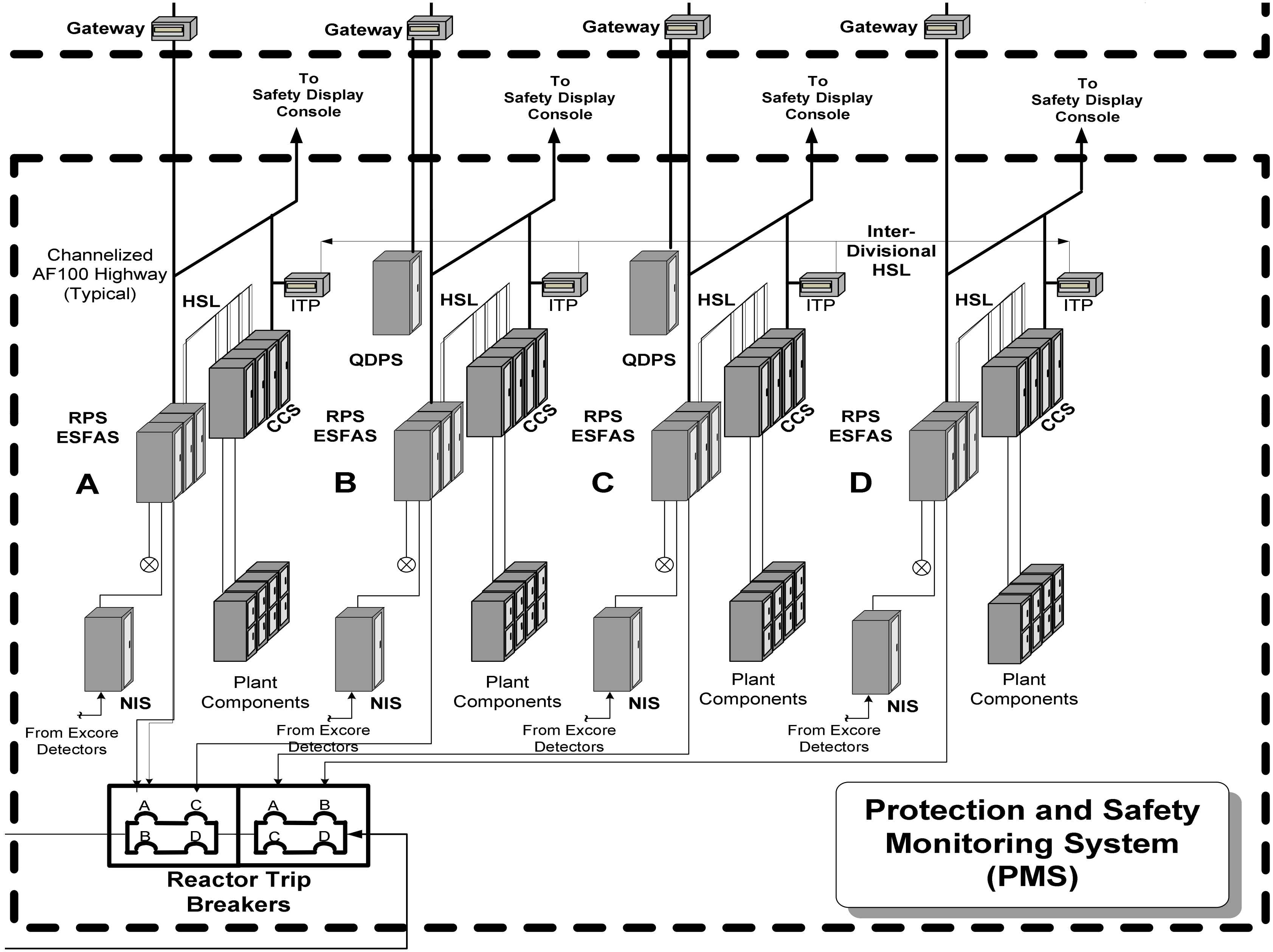
PMS Overview

PMS subsystems include:

- Nuclear Instrumentation System (NIS)
- Reactor Trip System (RTS)
- Engineered Safety Features Actuation System (ESFAS)
- Qualified Data Processing System (QDPS)

Fig. 8-1 (expanded)

Overview of PMS



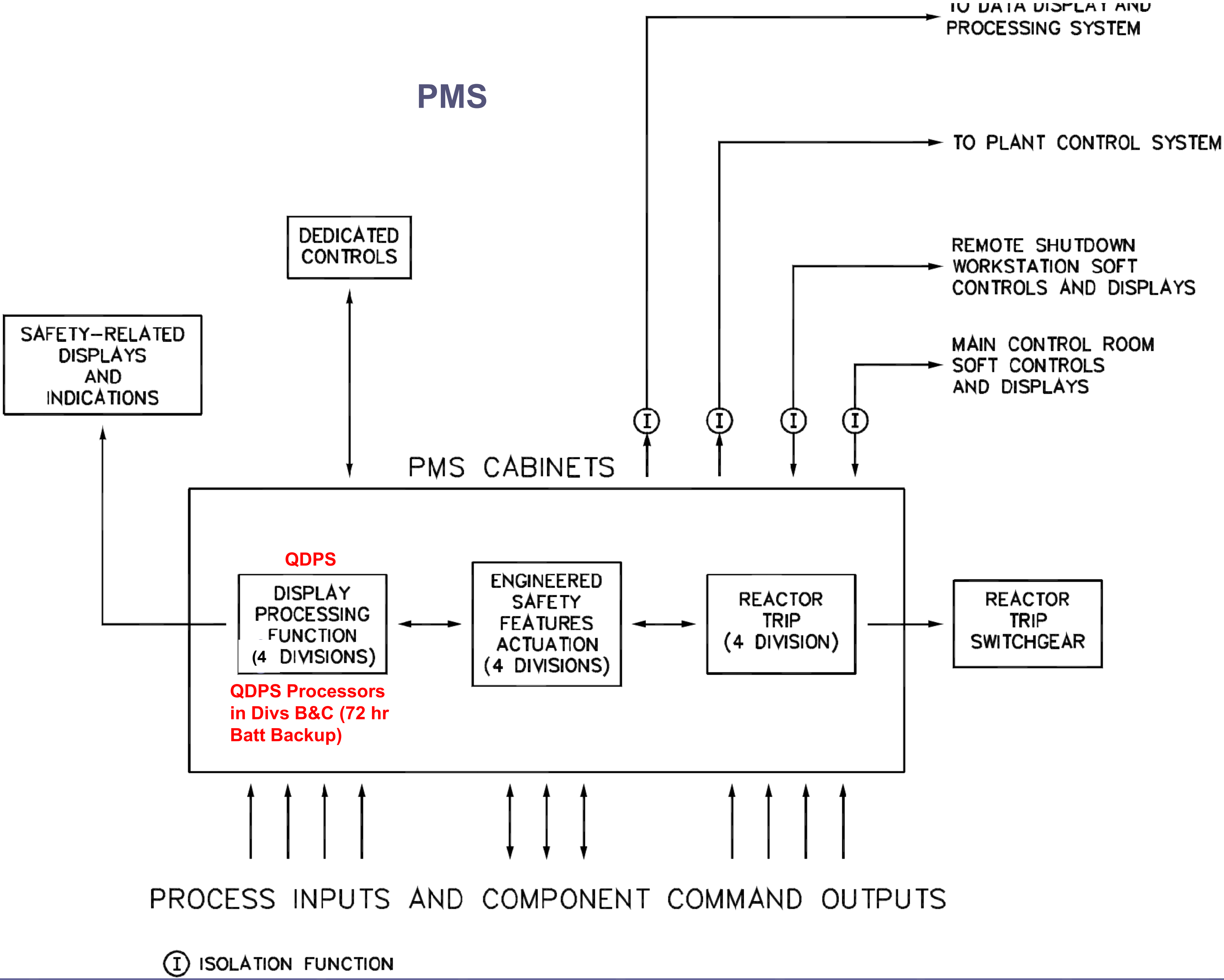
PMS Design Criteria

- Single failure does not prevent trip/ actuation, even with a channel bypassed
- Diversity of reactor trip functions
- Protection and control interaction
  - Setpoints take no credit for control actions
  - Analysis assumes worst case control action/ inaction
  - Control system failures isolated from PMS

PMS Design Criteria (cont.)

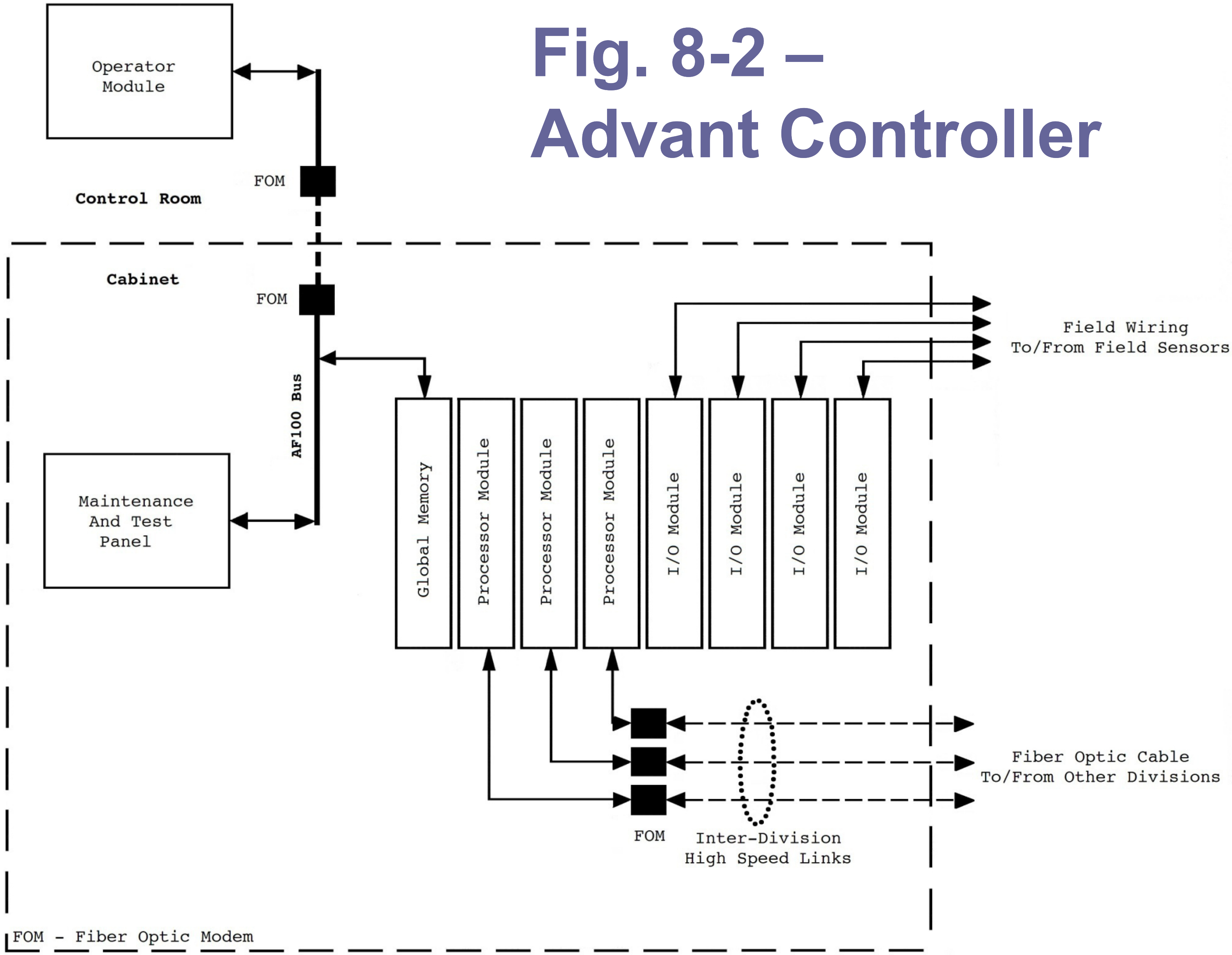
- Failure in protection channel monitoring a variable also used for control
  - Does not result in control system actions requiring protection by the redundant channels monitoring that variable
- Functional diversity used in determining ESF actuation signals

PMS



TO DATA DISPLAY AND PROCESSING SYSTEM
TO PLANT CONTROL SYSTEM
REMOTE SHUTDOWN WORKSTATION SOFT CONTROLS AND DISPLAYS
MAIN CONTROL ROOM SOFT CONTROLS AND DISPLAYS
DEDICATED CONTROLS
SAFETY-RELATED DISPLAYS AND INDICATIONS
PMS CABINETS
QDPS
DISPLAY PROCESSING FUNCTION (4 DIVISIONS)
QDPS Processors in Divs B&C (72 hr Batt Backup)
ENGINEERED SAFETY FEATURES ACTUATION (4 DIVISIONS)
REACTOR TRIP (4 DIVISION)
REACTOR TRIP SWITCHGEAR
PROCESS INPUTS AND COMPONENT COMMAND OUTPUTS
I ISOLATION FUNCTION

Fig. 8-2 – Advant Controller



Reactor Trip

- Plant control systems attempt to keep the reactor operating away from safety limits.
- Safety systems shut down the reactor when safety limits are approached.
- Reactor trip is a protective function performed by PMS when it anticipates an approach of a parameter to its safety limit.

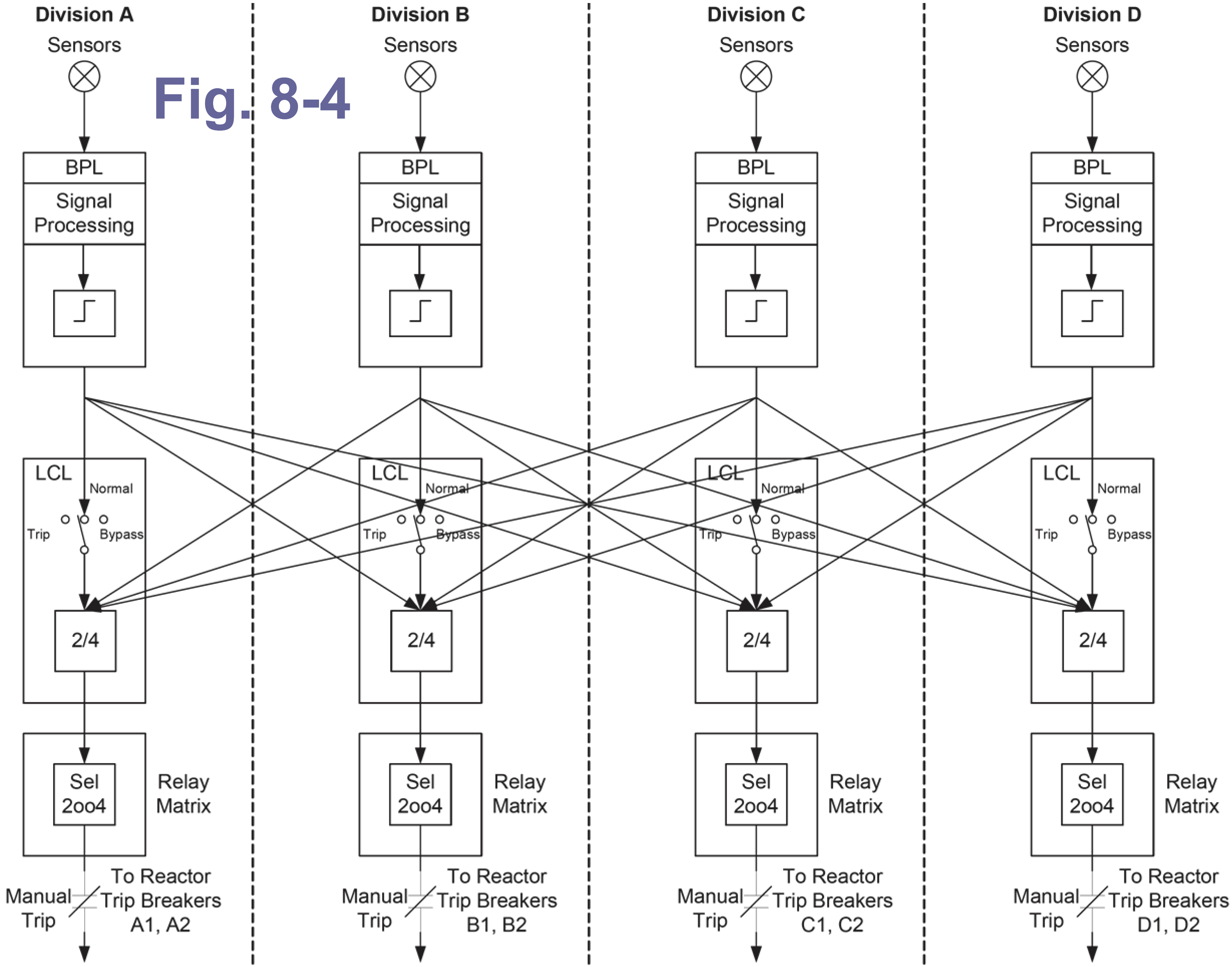
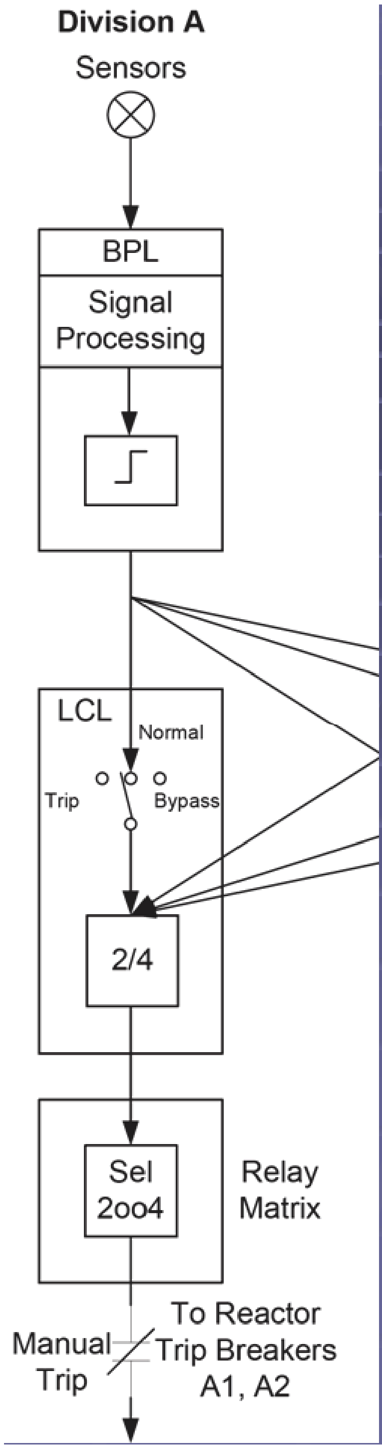


Fig. 8-4
Division A
Sensors
BPL
Signal Processing
LCL
Normal
Trip
Bypass
2/4
Sel 2oo4
Relay Matrix
Manual Trip
To Reactor Trip Breakers A1, A2
Division B
Sensors
BPL
Signal Processing
LCL
Normal
Trip
Bypass
2/4
Sel 2oo4
Relay Matrix
Manual Trip
To Reactor Trip Breakers B1, B2
Division C
Sensors
BPL
Signal Processing
LCL
Normal
Trip
Bypass
2/4
Sel 2oo4
Relay Matrix
Manual Trip
To Reactor Trip Breakers C1, C2
Division D
Sensors
BPL
Signal Processing
LCL
Normal
Trip
Bypass
2/4
Sel 2oo4
Relay Matrix
Manual Trip
To Reactor Trip Breakers D1, D2



BPL – Bistable Processor Logic

- Compares signals from sensors
- Generates partial trip/actuation signal

LCL – Local Coincidence Logic

- LCL receives partial trips from all divisions via one-way HSL connections (fiber optics for division separation). 4 redundant reactor trip processors perform 2/4 votes in each division.

- Selective 2/4 (1/2 taken twice) contact matrix for undervoltage, shunt trip attachments. Sufficient coincidence generates trip of division-controlled trip breakers (2).

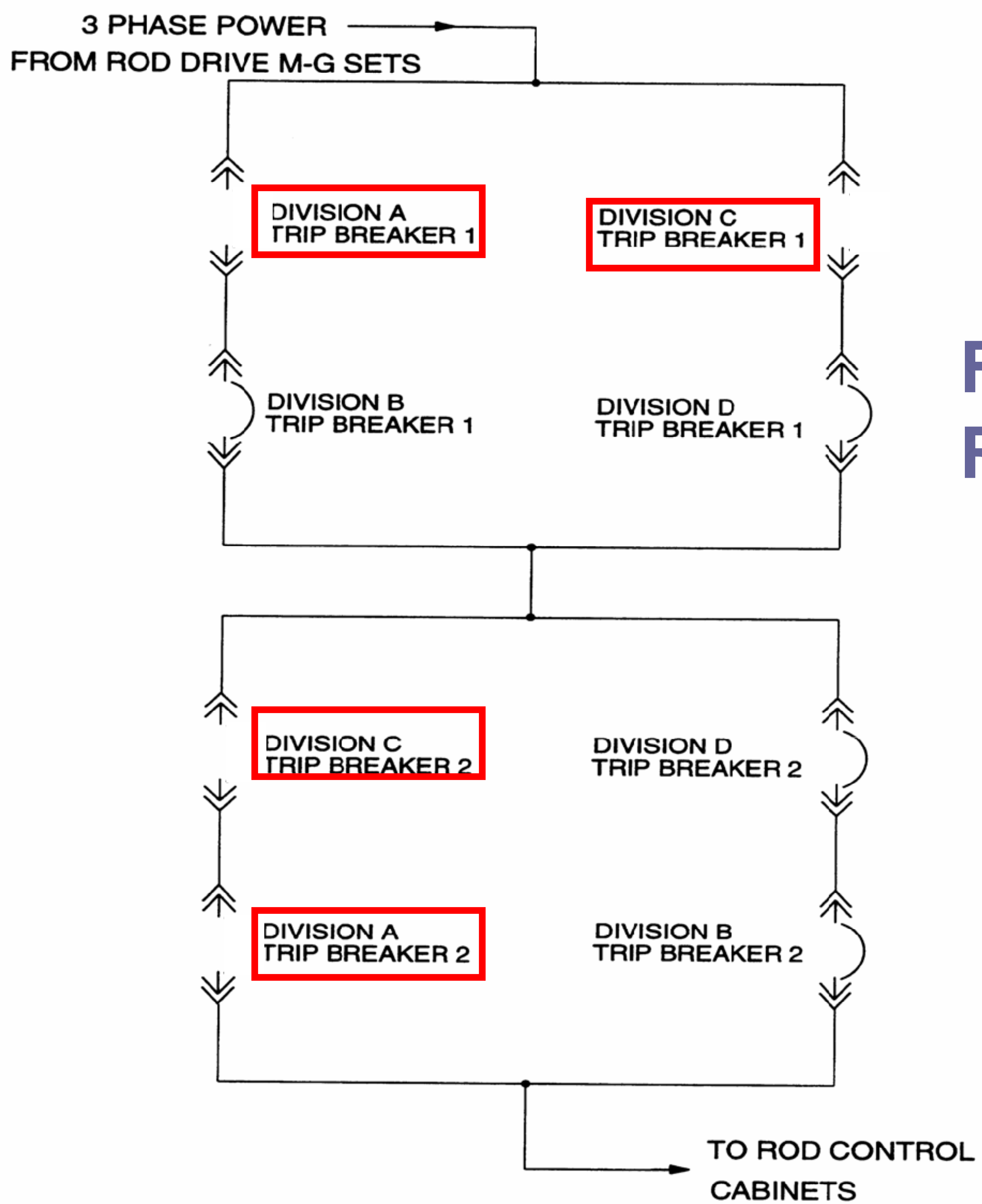
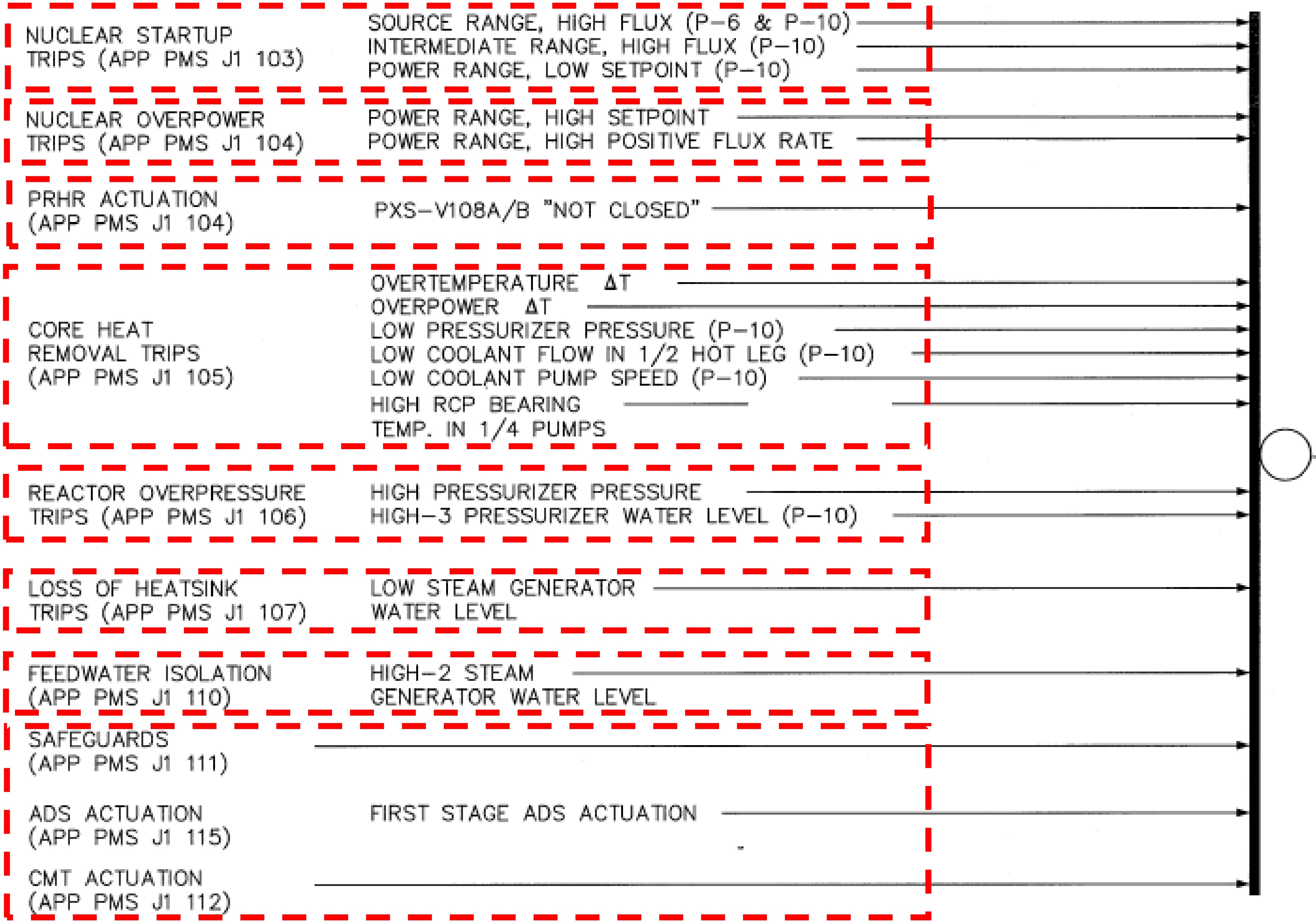


Fig. 8-5 – Rx Trip Breakers

Reactor Trip Signals (Fig. 8-7)



Reactor Trip System Interlocks

- (P-#) Provided to ensure reactor trips are in the correct configuration for the current plant status.

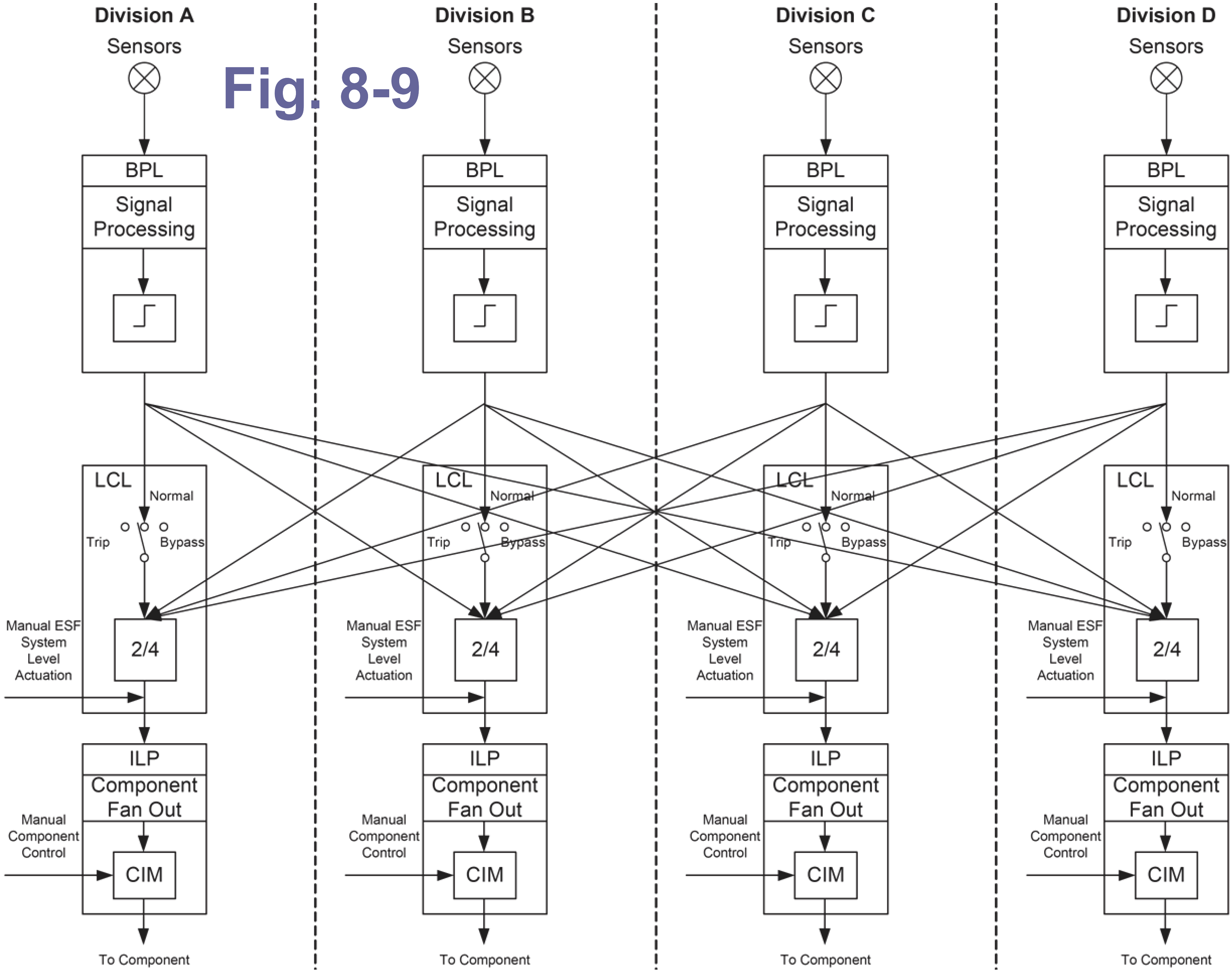
- Back up operator actions to ensure protection system functions are not blocked during plant conditions for which the safety analysis assumes they are OPERABLE.

Engineered Safety Features Actuation Signals

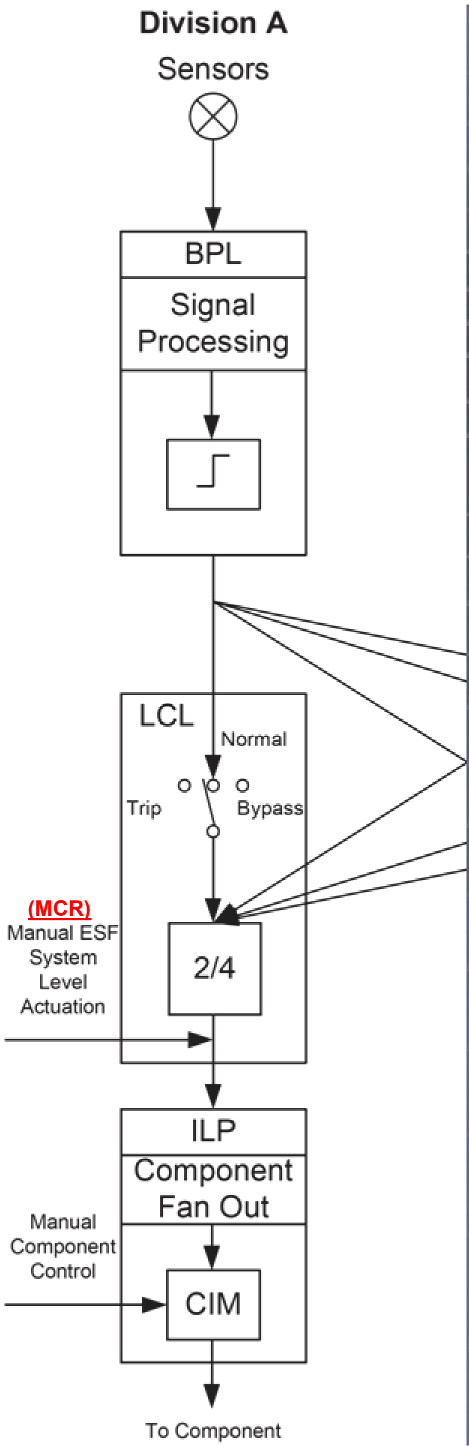
- The occurrence of a limiting fault (i.e., LOCA or MSLB) requires a reactor trip plus actuation of one or more engineered safety features (ESFs).

- Prevents or mitigates damage to the core and RCS components, and provides containment integrity.

Fig. 8-9



Division A
Sensors
Division B
Sensors
Division C
Sensors
Division D
Sensors
BPL
Signal Processing
LCL
Normal
Trip
Bypass
2/4
Manual ESF System Level Actuation
ILP
Component Fan Out
CIM
Manual Component Control
To Component



ILP – Integrated Logic Processor

➢Receives system-level actuation signal when both of its division's ESF processors call for actuation.

➢Generates component-level actuations.

CIM – Component Interface Module

➢Actuates specific, individual components when 2/2 ILP modules call for actuation.

Safeguards (S) Signal

Conditions:

- Low PZR pressure (2/4 divisions)
- Low steam line pressure (2/4 divisions on 1/2 main steam lines)
- Low cold leg temperature (2/4 divisions)
- High-2 containment pressure (2/4)
- Manual

Protection:

- LOCA, SLB, FLB, SGTR
- Inadvertent opening of PZR or SG safety valve or inadvertent actuation of ADS
- Inadvertent PRHR actuation

Safeguards (S) Signal -- Actuations

- Reactor trip
- Time-delayed trip of all RCPs
- Turbine trip
- CMT actuation
- Containment isolation, including air filtration and RNS
- Feedwater isolation

CMT Injection

Conditions:

- Safeguards actuation
- First-stage ADS actuation
- PZR level below Low-2
  - Manual block when PZR level is below P-12
  - Automatically unblocked above P-12
- Low WR SG level coincident with High HL temperature
- Manual

Protection:

- LOCA, inadvertent opening of PZR safety or ADS
- Inadvertent opening of SG safety.
- Inadvertent PRHR actuation

CMT Injection -- Actuations

- Reactor trips
- RCPs trip
- CMT isolation valves align for injection
- PZR heaters blocked
- Confirmatory open signal to cold leg balance line isolation valves

RCP Trip

Conditions:

- Safeguards actuation
- First-stage ADS actuation
- PZR level below Low-2
- Low WR SG level coincident with High hot leg temperature
- Manual CMT actuation
- RCP bearing water High temp.

Protection:

- Assurance of RCP trip when CMT injection needed
- RCP protection

PRHR Actuation

- CMT actuation
- First-stage ADS actuation
- WR SG level Low in either SG
- SG NR level Low longer than time delay, coincident with low startup feedwater flow, in a particular SG
- PZR water level above High-3
- Manual

PRHR Actuation (cont'd)

Components actuated:

- Opens PRHR HX discharge isolation valves
- Closes IRWST gutter isolation valves (gutter overflows to IRWST)
- Confirmatory open signal to PRHR HX inlet isolation valve

Protection:

Safety-related decay heat removal when:

- Pri-to-sec heat transfer degraded or unavailable
- Accident potentially in progress

1^{st}-Stage ADS Actuation

Conditions:

- CMT level below Low-1 in either CMT coincident with CMT injection signal
- Extended loss of ac power sources
- Manual (simultaneous actions required)

Protection:

- LOCA
- Inadvertent opening of PZR safety valve or ADS path

4^{th}-Stage ADS Actuation

Conditions:

- CMT level < low-2 in either CMT coincident w/:
  - RCS pressure < 1200 psig
  - Time delay elapsed since 3^{rd}-stage actuation
- Level in both HLs < low-2 for longer than time delay
  - Shutdown protection (Modes 4, 5, 6)
  - Automatically blocked w/ PZR level > P-12
  - Block removed when CMT actuation on low PZR level is manually blocked

4th-Stage ADS Actuation (cont.)

Actuation:

- ADS 4th-stage valves
- IRWST injection

Protection:

- LOCA
- Inadvertent opening of PZR safety valve or ADS path

IRWST Injection

Conditions:

- Fourth-stage ADS actuation
- Level in both HLs < low-2 for longer than time delay
  - Shutdown protection (Modes 4, 5, 6)
  - Automatically blocked w/ PZR level > P-12
  - Block removed when CMT actuation on low PZR level is manually blocked
- Manual (simultaneous actions required)

Protection:

- LOCA
- Inadvertent opening of PZR safety valve or ADS path

Containment Recirculation

Conditions:

- IRWST level below Low-3 coincident with fourth-stage ADS actuation – opens all recirc. isolation valves
- Manual (simultaneous actions required) – opens all recirc. isolation valves
- Loss of AC power sources longer than time delay – opens recirc. isolation valves in series w/ check valves

Protection: LOCA

Passive Containment Cooling

Conditions:

- Containment pressure above High-2
- Manual (also actuates containment isolation)

Protection: LOCA, SLB, FLB (high energy line break inside containment)

Opens: PCCWST isolation valves

Startup Feedwater Isolation

Conditions:

- RCS T_{cold} Low in any loop
- High-2 SG NR level in either SG
- Manual actuation of main feedwater isolation
- High SG NR level in either SG + P-4

Protection:

Assurance of SUFW isolation when:

- RCS is overcooling due to secondary break or excessive FW addition
- SG is approaching overfill due to SGTR

Components actuated:

- Trip startup feedwater pump
- Close SU feedwater isolation & control valves

ESFAS Interlocks (P- #)

- Allows some flexibility in unit operations.
- Permits the blocking of some signals.
- Permits auto enabling of other signals.
- Prevents some actions from occurring, and causes other actions to occur.
- Backs up manual actions to ensure required functions are operable under the conditions assumed in the safety analyses.

Control Systems

- Establish and maintain the plant operating conditions within prescribed limits.
- Improve plant safety by minimizing the number of situations for which some protective response is initiated.
- Regulate the operating conditions in the plant automatically in response to changing plant conditions and changes in plant load demand.

Design Capability

- ±10% step load change without reactor trip or steam dump actuation.
- ± 5% ramp load change without reactor trip or steam dump system actuation.
- 100% load rejection without reactor trip.
- Turbine trip from full-power operation without reactor trip.

Reactor Power Control System

Enables response to the following:

- Step load changes of ± 10%
- Ramp load changes of ± 5%/min
- Daily load follow operations with following profile:
  - Power ramps from 100% to 50% in 2 hours
  - Power remains at 50% for 2 to 10 hours
  - Power ramps back up to 100% in 2 hours
  - Power remains at 100% for the remainder of the 24-hour cycle
- Grid frequency response resulting in a maximum of 10% power change at 2%/min

Reactor Power Control System

- Uses different control strategies for rods used to regulate core power (M banks) and rods used to regulate axial offset (AO bank).

- During load follow or load regulation response transients, the **Power Control** and the **Axial Offset Control** subsystems jointly function to control both core power and axial offset.

Power Control

- Similar to current operating plant's rod control system (temperature & power mismatch).
- Maintains T_{avg} on program (T_{ref}) using "M" control bank rods.
- Uses a control input signal derived from the reactor power versus turbine load mismatch circuit.

Axial Offset Control

- Controls the core AO to a value that is within the desired control range.

- Measured AO is input into the AO control subsystem and then compared to an AO control "window."

- When the AO error is outside the “window,” the AO rods are adjusted until the error is back inside the “window.”

Rod Control System

- Receives rod speed and direction signals from the power and AO control subsystems.
  - Power control operates the MA, MB, MC, MD, M1 and M2 control rod banks.
  - AO control operates the AO control rod bank.

- Power control rod speed varies 8 to 72 spm.

- AO control rod speed is fixed at 8 spm.

Additional Control Systems

- Pressurizer Pressure Control
- Pressurizer Water Level Control
- Feedwater Control System
  - Feedwater Control
  - Startup Feedwater Control
- Steam Dump Control
  - Load Rejection Steam Dump Controller
  - Plant Trip Steam Dump Controller
  - Steam Header Pressure Controller

Rapid Power Reduction System

- Reduces nuclear power to a level within the capabilities of the steam dump system for a large load rejection.
- Upon detection of a large/rapid turbine load reduction generates a signal demanding the release of a preselected number of control rods.
- The dropping of these preselected rods causes the reactor power to rapidly reduce to $\leq$50%.

Signal Selector Algorithm

- Prevents a failed input signal from initiating an undesirable control action.
- Selects the signals that represent the actual status of the plant and rejects erroneous signals.
- Prevents an unsafe control action from occurring if one of four redundant protection channels experiences a random failure.

Diverse Actuation System

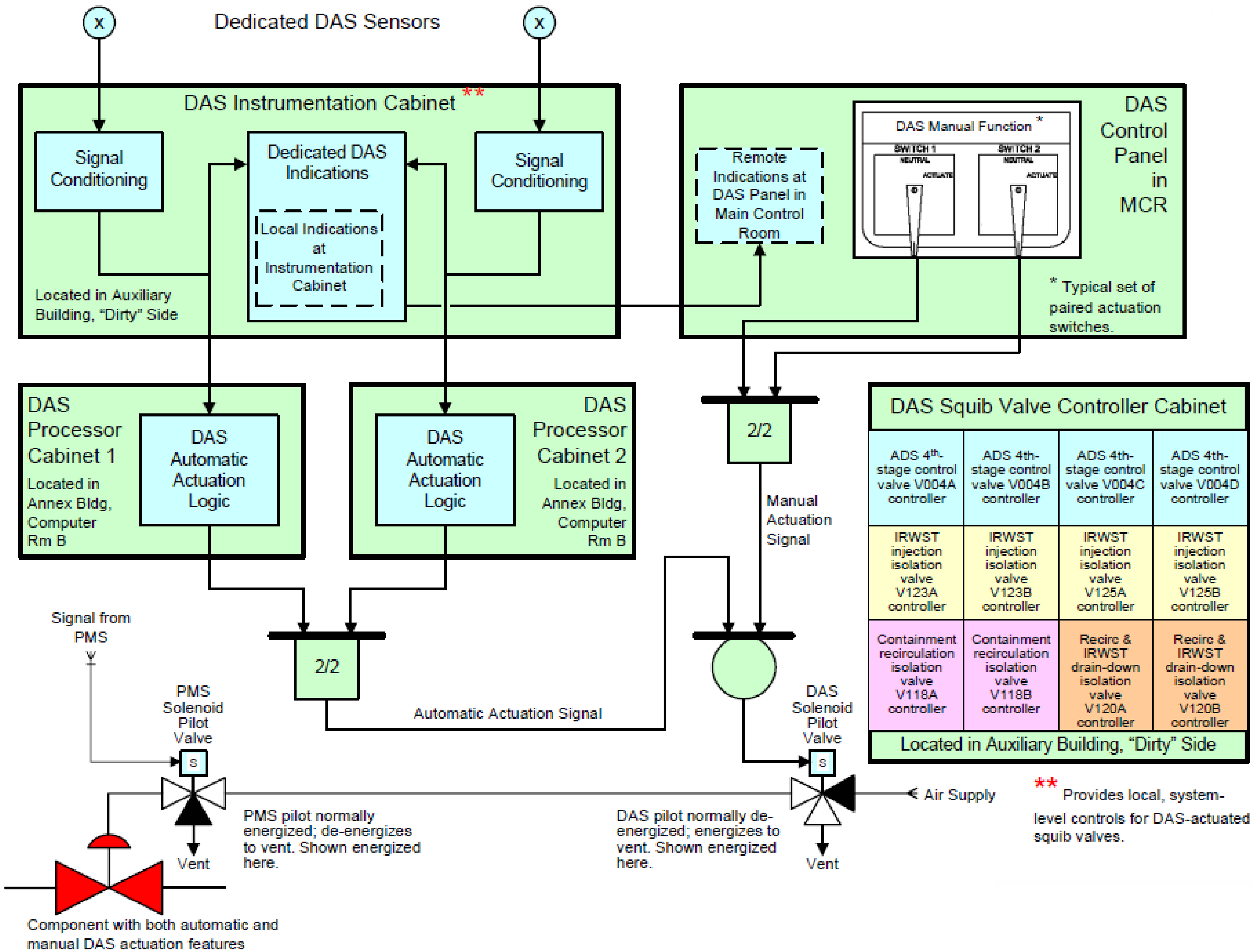
- Nonsafety-related system that provides a diverse backup to the protection system.
- In the low probability case where a common-mode failure occurs within PMS, the DAS provides diverse protection.
- Auto actuation signals provided by the DAS are generated in a functionally diverse manner from the PMS actuation signals.

Diverse Actuation System

The DAS automatic actuations are:

- **Low WR SG Water Level:** Trips rods via MG set bkrs, trips turbine, initiates passive RHR, actuates core MU tanks, and trips the RCPs.
- **High Hot Leg Temperature:** Trips rods via MG set bkrs, trips turbine, opens the passive RHR discharge isolation valves, and closes the IRWST gutter isolation valves.
- **Low Pressurizer Water Level:** Trips rods via MG set bkrs, trips turbine, actuates the core MU tanks, and trips the RCPs.
- **High Containment Temperature:** Isolates selected containment penetrations and starts passive containment cooling water flow.

DAS Simplified Block Diagram



Questions?

The Reactor Coolant Pump Bearing Water Temperature Trip is an anticipatory trip based on the expectation of………..

a. A complete loss of the RCP seals.

b. A partial loss of RCS flow.

c. A failure of the RCP casing.

d. A complete loss of RCS flow.

The RCS Cold Leg Temperature (T_{cold}) – Low signal provides protection against……..

a. Loss of RCS flow accidents.

b. RCS dilution accidents.

c. Main steam or feedline break accidents.

d. SG tube rupture accidents.