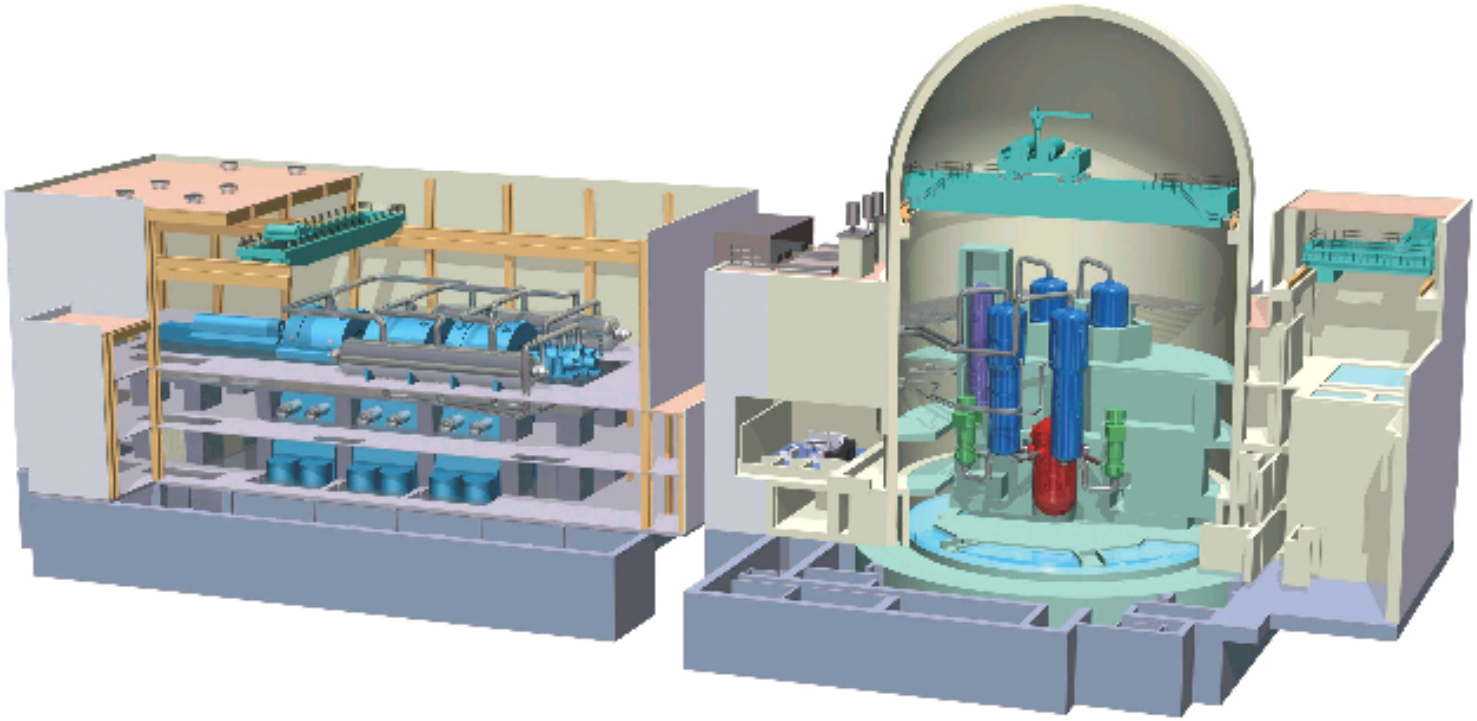
USAPWR

Defense-in-Depth and Diversity
Unique Prompting Alarms



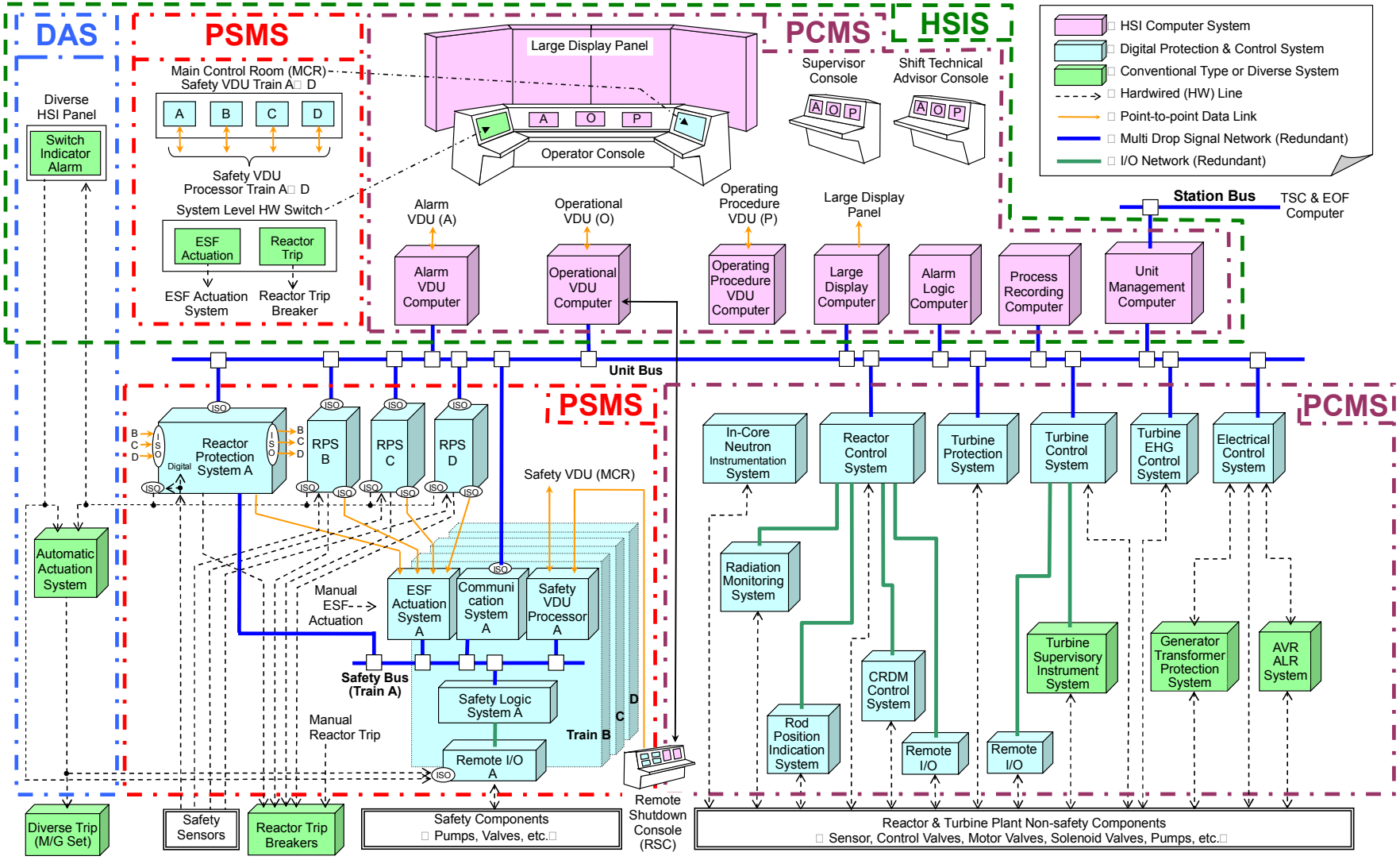
May 21, 2008

MITSUBISHI HEAVY INDUSTRIES, LTD.

Purpose of Unique Prompting Alarms

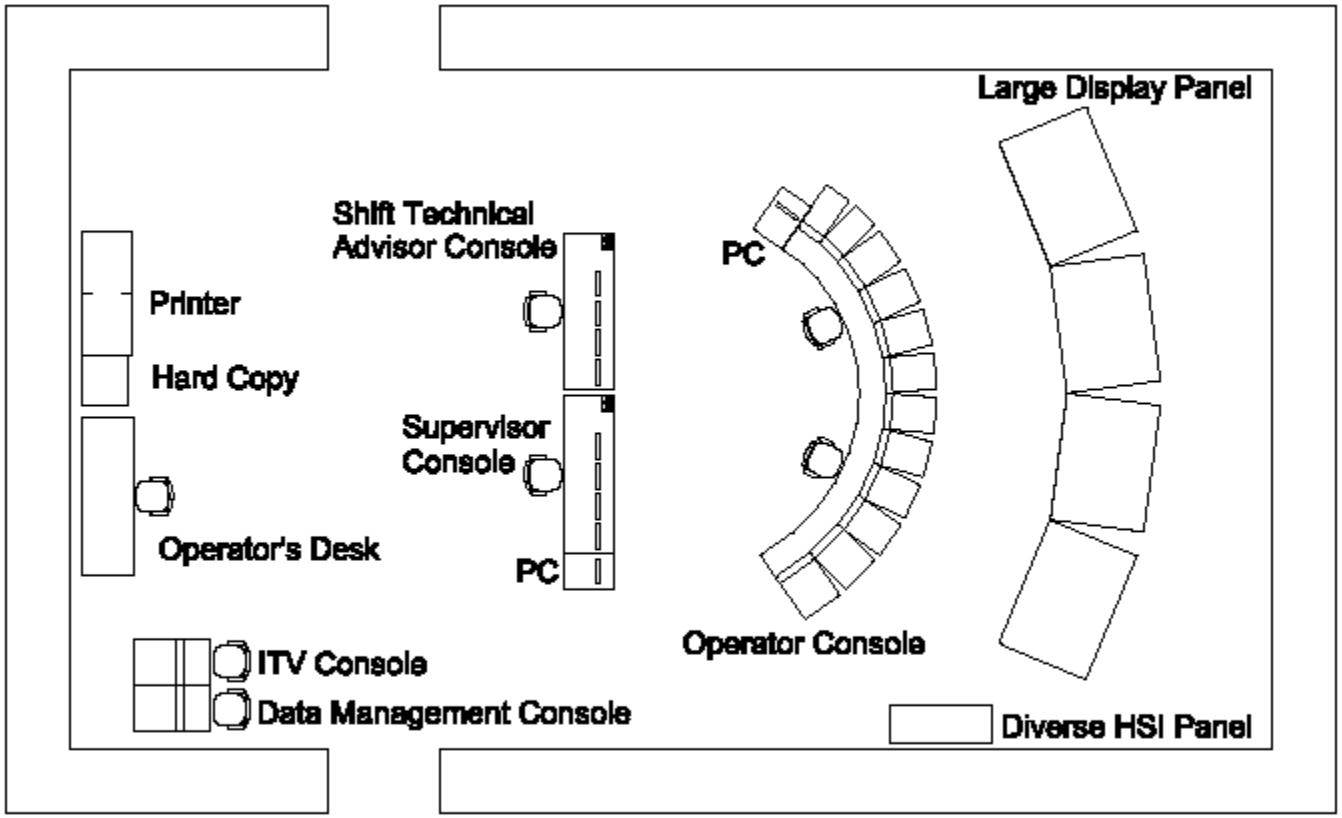
- The USAPWR credits unique alarms to prompt entry into Special Event EOPs for coping with AOOs or PAs, with concurrent CCF
- DAS design features ensure these alarms will not be spuriously generated
  - ✓ If there is no I&C CCF
  - ✓ Due to credible single failures
- DAS operability, including alarms, is ensured through
  - ✓ Periodic testing
  - ✓ Limiting conditions of operation
- Operators will be trained to provide an immediate response to the unique prompting alarm
  - ✓ **Without additional equipment failure diagnosis or plant event diagnosis**
  - ✓ **Because normal automation and HSI is now suspect**

The Overall Architecture of the I&C System



DAS : Diverse Actuation System PSMS : Protection and Safety Monitoring System HSIS : Human System Interface System PCMS : Plant Control and Monitoring System

US-APWR MCR


Large Display Panel
Shift Technical
Advisor Console
PC
Printer
Hard Copy
Supervisor
Console
Operator's Desk
PC
Operator Console
ITV Console
Data Management Console
Diverse HSI Panel

Full Scope Simulator - Pittsburgh

Full Scope Simulator - Pittsburgh

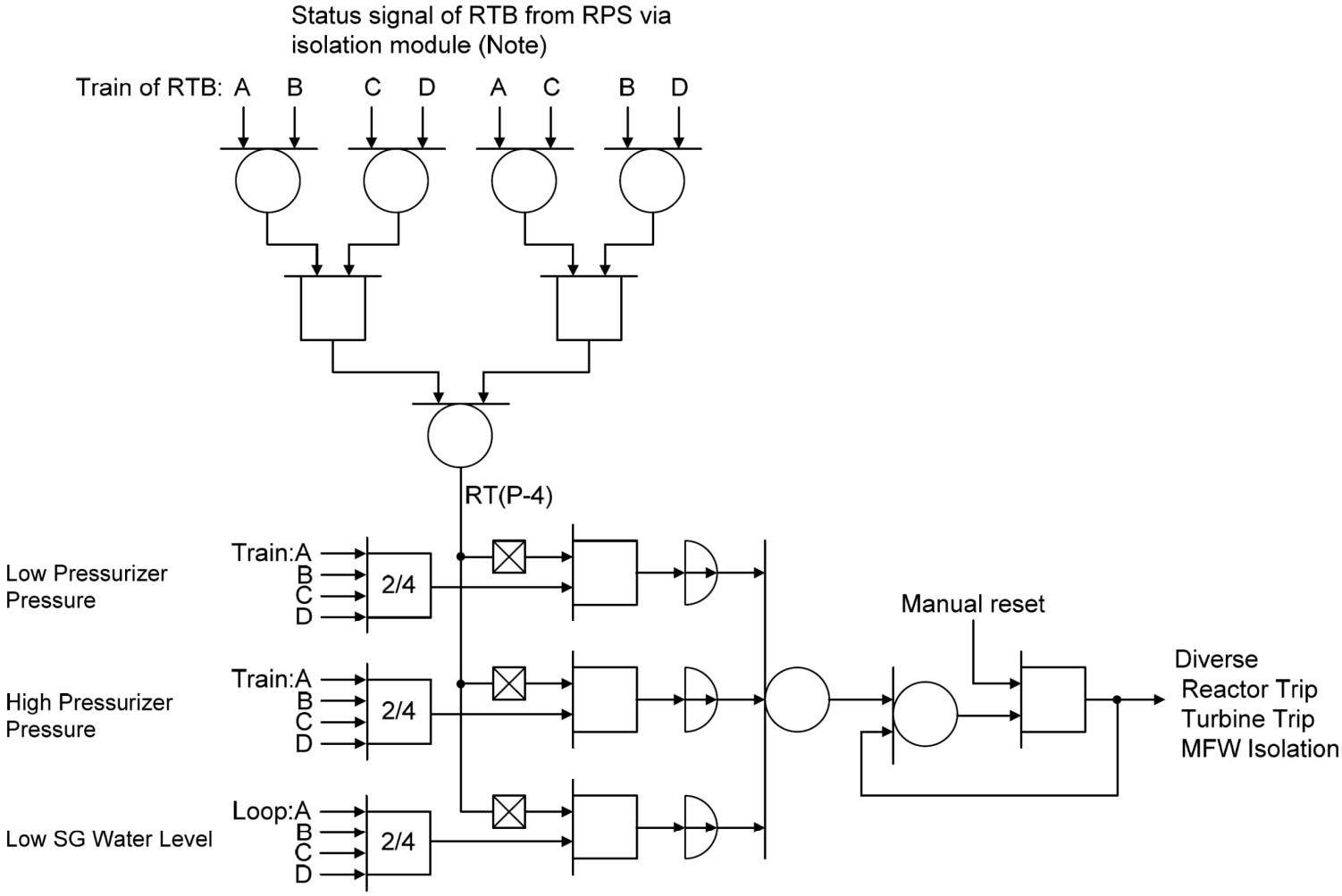
DAS Actuation and Alarms

- The DAS system level actuation signals are generated for
  - ✓ Reactor trip, turbine trip, and MFW isolation
    - Low Pressurizer Pressure
    - High Pressurizer Pressure
    - Low SG Water Level
  - ✓ EFW actuation
    - Low SG Water Level
- A summary alarm for actuation of any of these functions is actuated <u>on the DHP</u>
  - ✓ This includes a diverse audible alarm
- The first-out alarm panel, on the DHP, indicates the specific parameter that has caused the system level actuation
- Operators are prompted by the alarm
  - ✓ Then directed to the specific EOP by the first-out indication

Spurious Actuation/Alarm Prevention

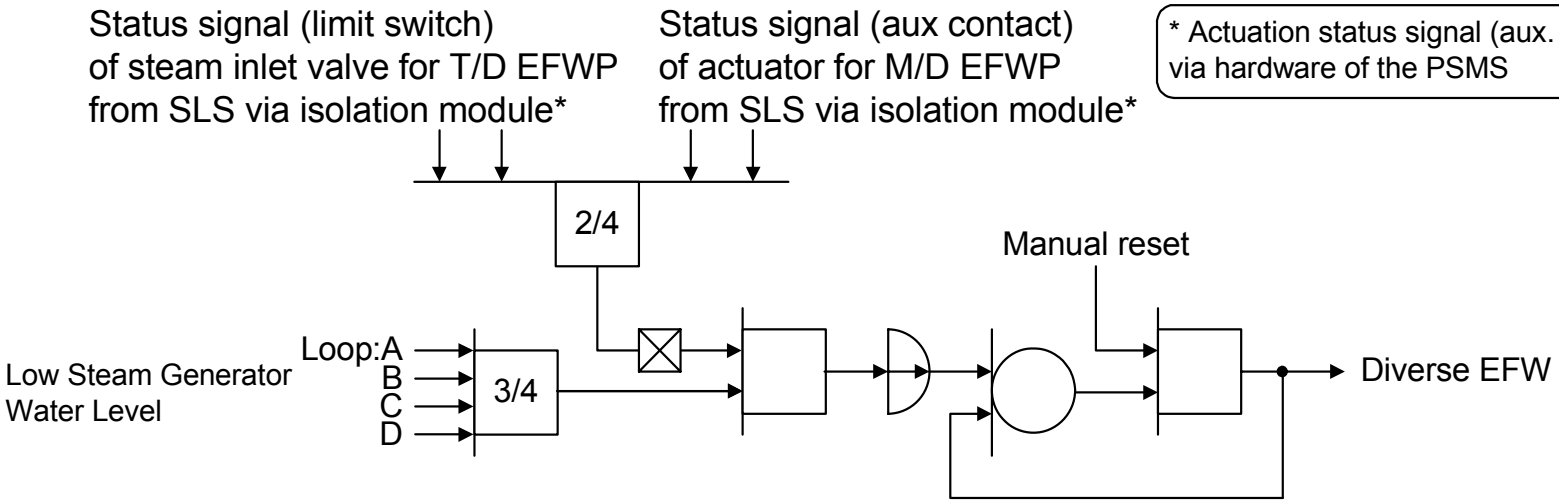
- There are two DAS subsystems designated
  - ✓ Diverse Automation Actuation Cabinet 1 and 2
- Both must function to generate actuations or alarms
  - ✓ Single actuations are separately alarmed by the normal alarm system as DAS equipment failures
- Both subsystems actuate on 2/4 or 3/4 inputs
- DAS is designed to allow the PSMS to actuate first
  - ✓ DAS actuation is delayed; PSMS is not
  - ✓ DAS setpoints are less conservative than PSMS
- DAS actuations and alarms are blocked if the PSMS actuates (ie. no CCF)
  - ✓ RT is blocked separately from EFW
- DAS is an energize to actuate system

RT, TT, MFW Actuation and Block

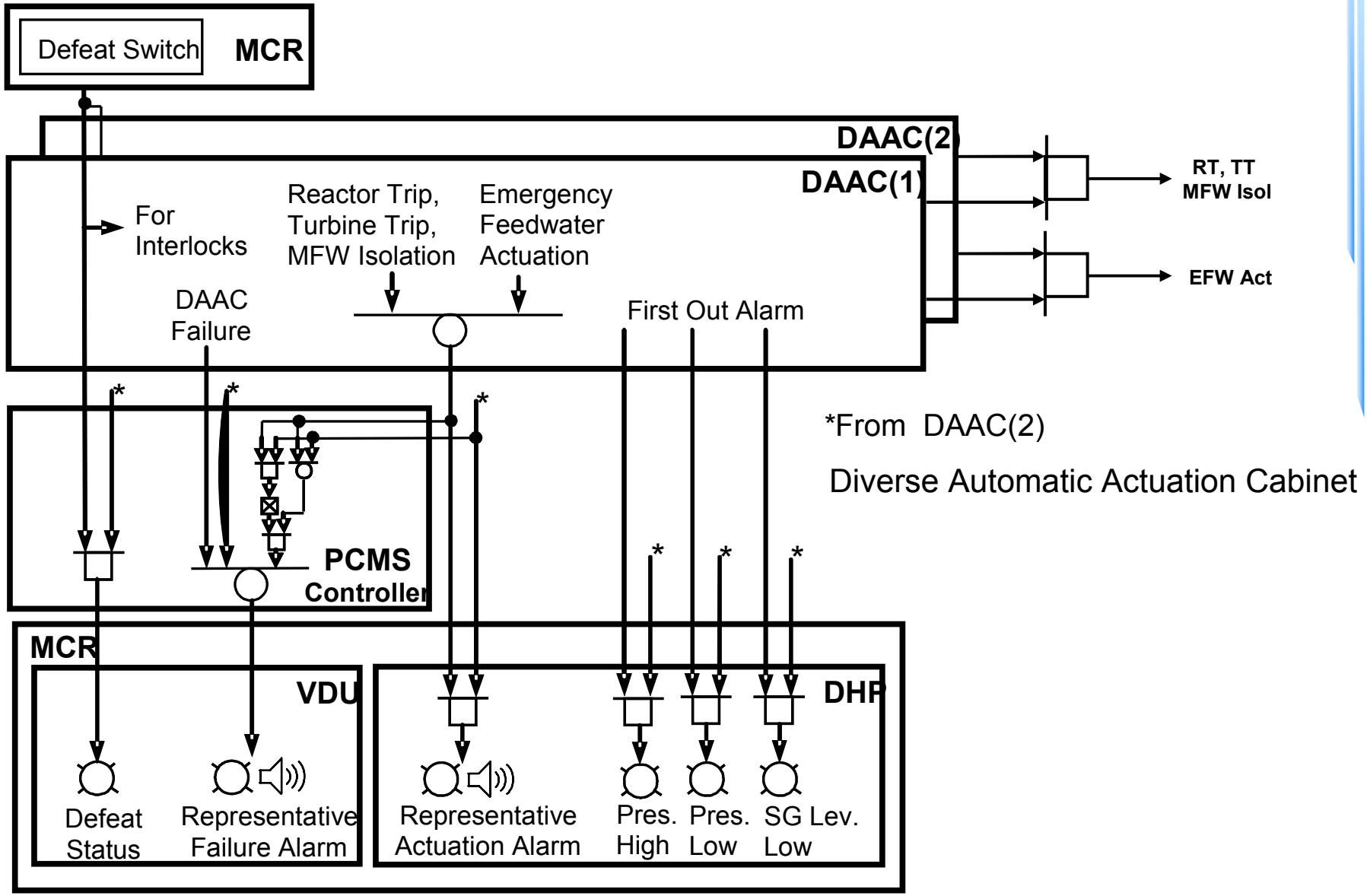


Note: Actuation status signal (aux. contact etc.) via hardware of the PSMS

EFW Actuation and Block



DAS 2/2 Actuation Configuration



Scenario Example - SBLOCA

- No CCF
  - ✓ RPS initiates reactor trip on low pressure
  - ✓ DAS actuation and alarm are blocked
  - ✓ ESFAS initiates ECCS at low pressure setpoint
- With CCF
  - ✓ No RPS/ESFAS actuation
  - ✓ DAS initiates reactor trip on low* pressure

    *lower setpoint than RPS
  - ✓ DAS initiates actuation alarm and low pressure first-out indication on DHP
  - ✓ Operator immediately initiates ECCS manually at DHP based on training and Special Event EOP
    - Time Available ~10 minutes