HSI Technology Evolution and Effects on Operators

August 26, 2008

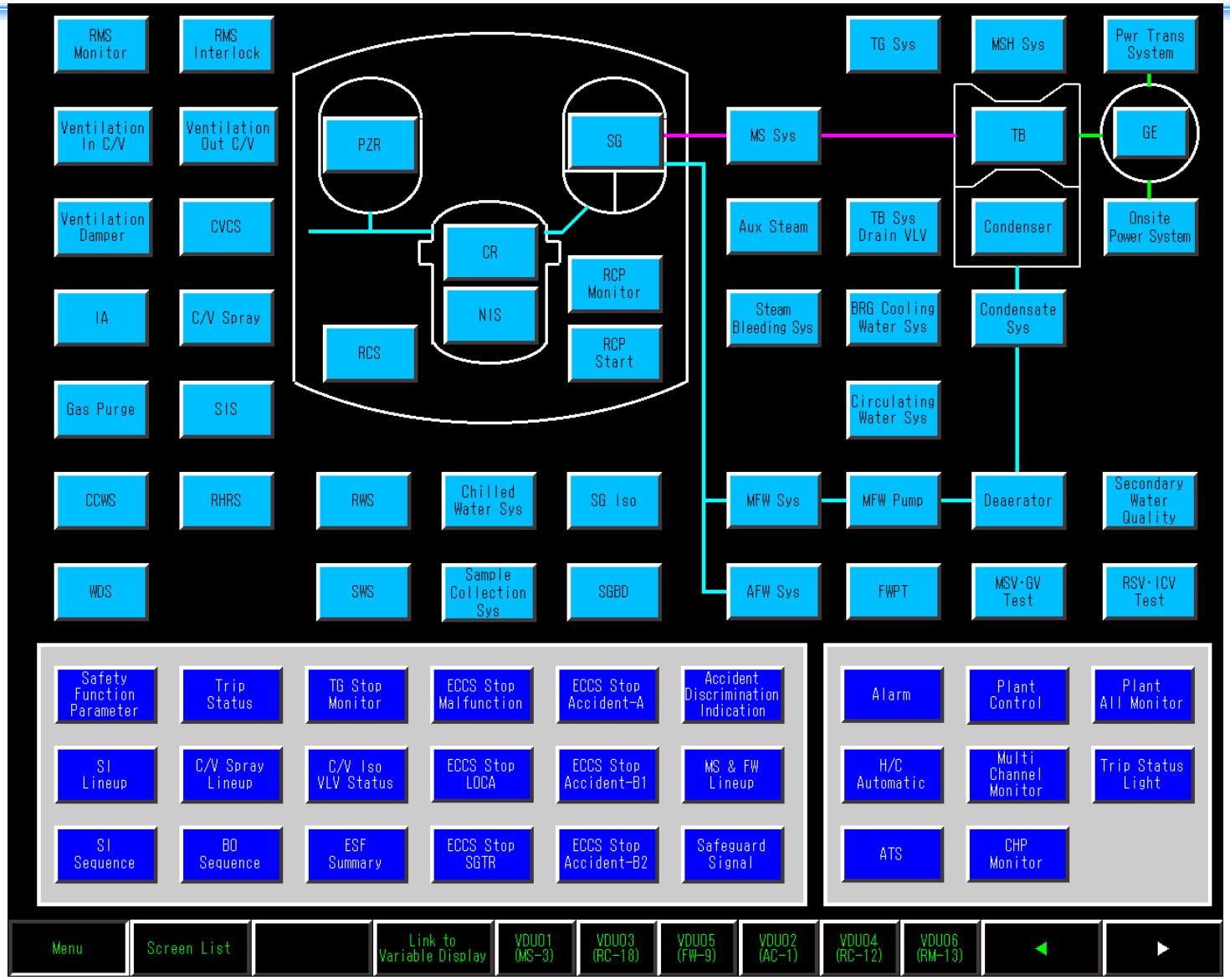
Overview

- HSI technology evolution in new control rooms will change some operator tasks
- This presentation highlights a few key areas for the US-APWR

Information & Controls Accessibility

- **All information and controls are easily accessible to each operator**
  - ✓ Video Display Units with hundreds of display pages
    - Menu selectable
  - ✓ Multi-division VDUs
    - Control all safety divisions and non-safety from same VDU
- **Very different than the geographic distribution of instrumentation and controls on conventional panels**
  - ✓ One RO can monitor and control all plant functions
  - ✓ With two ROs, the division of responsibility between ROs can be function based rather than system based
    - For example, one RO can be responsible for all systems (safety and non-safety) for controlling the same function (eg. RCS inventory).

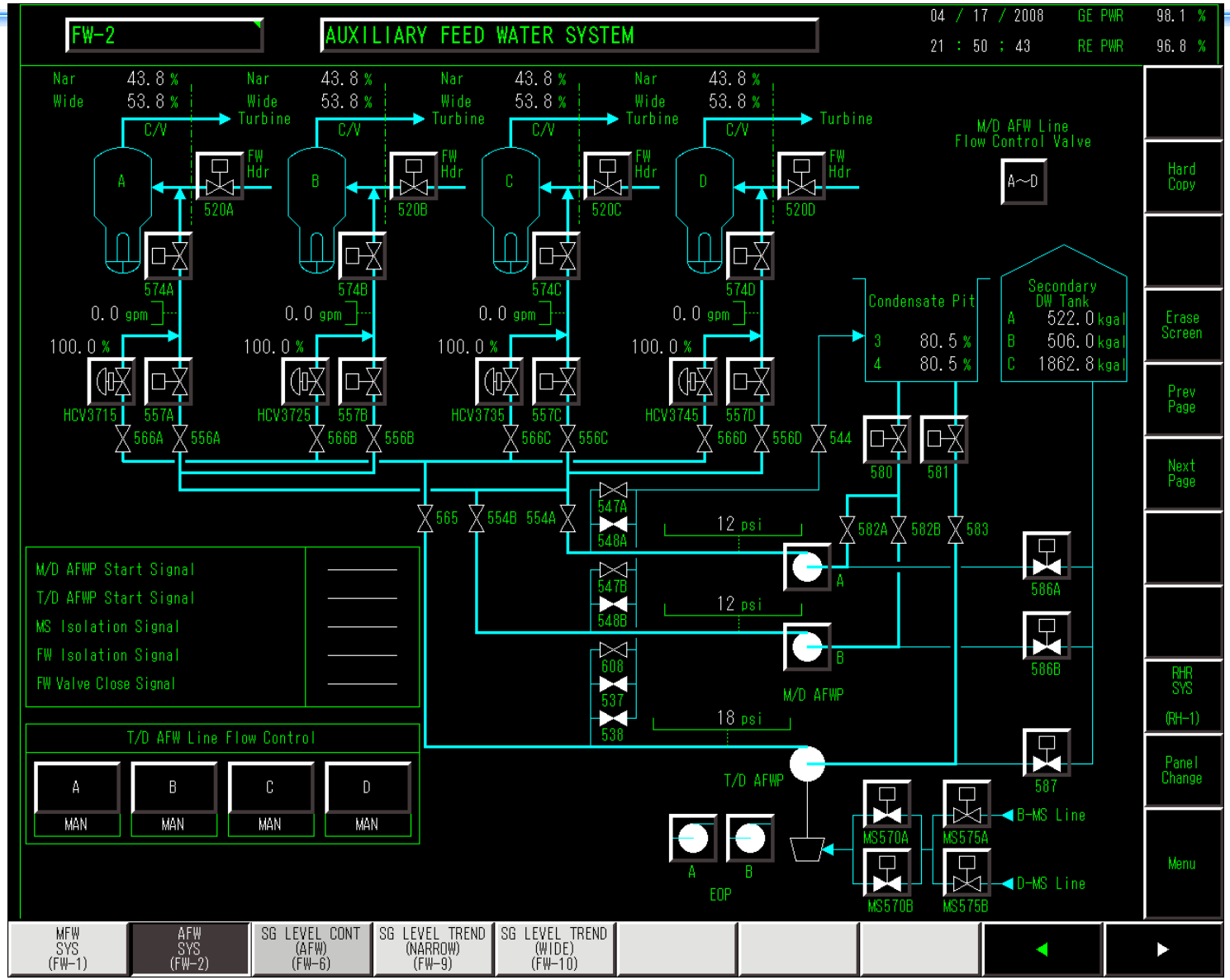
Operational VDU – Screen Menu



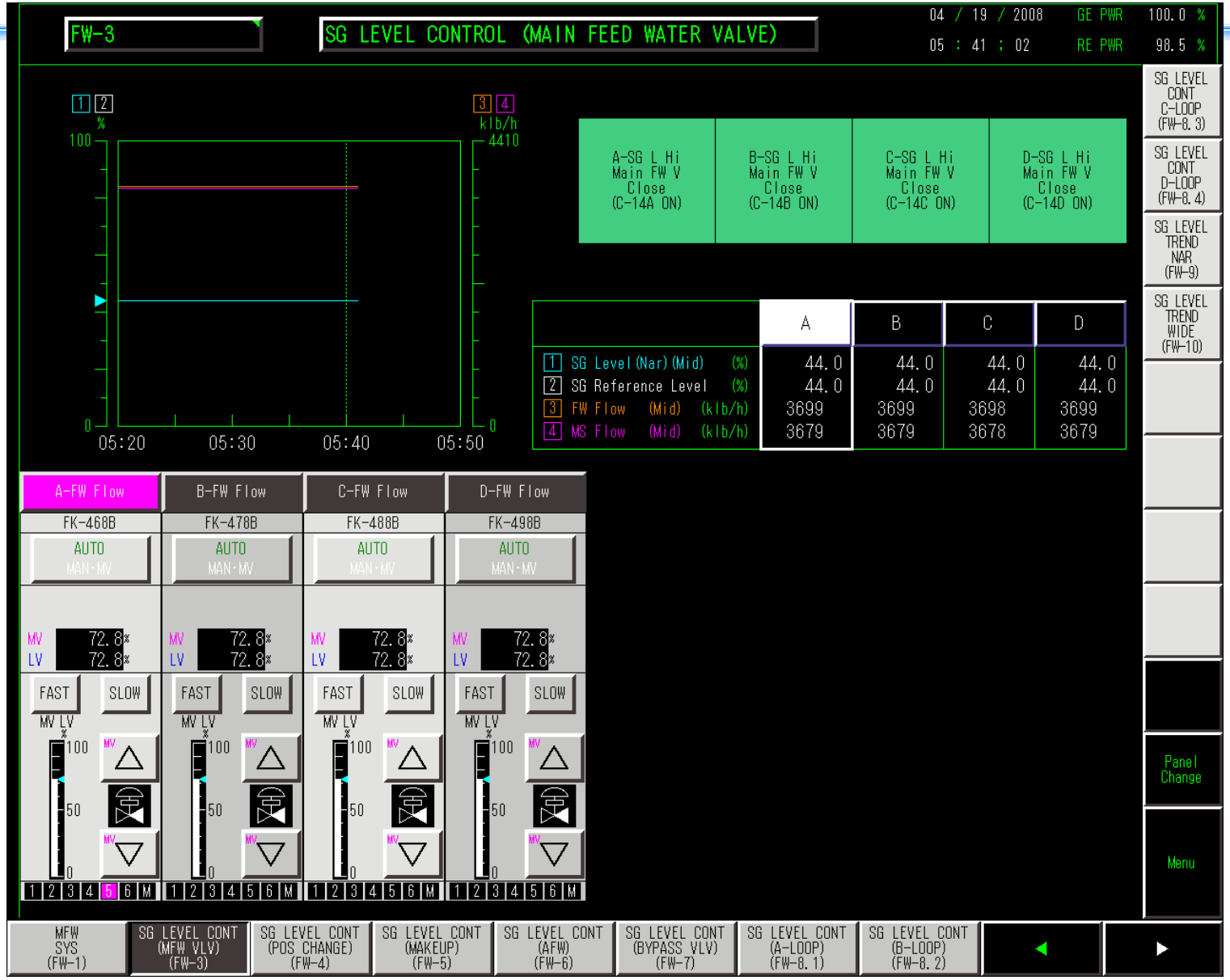
System display request area

Emer display request area

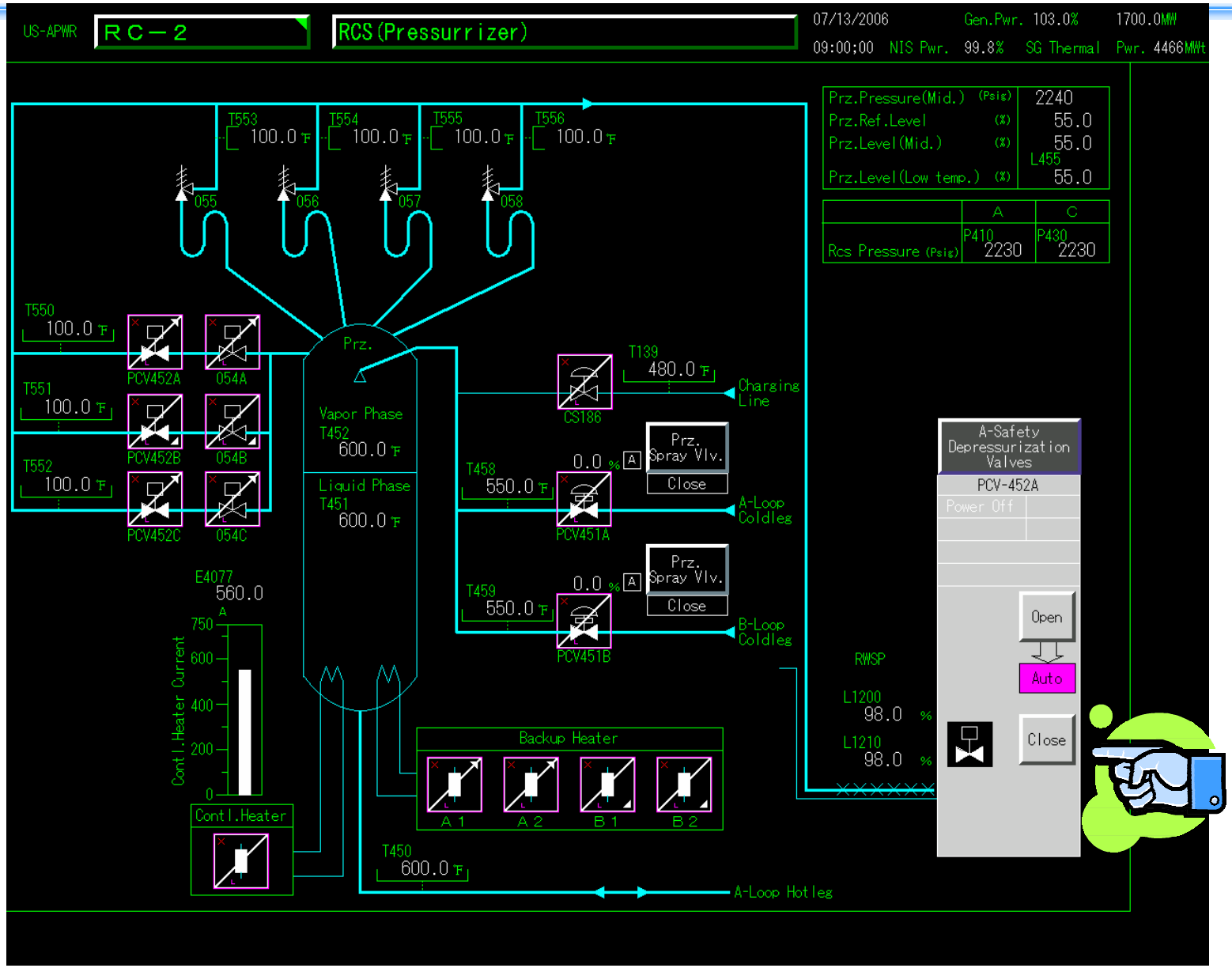
Operational VDU - Monitoring



Operational VDU - Control



Operational VDU - Multi-Division



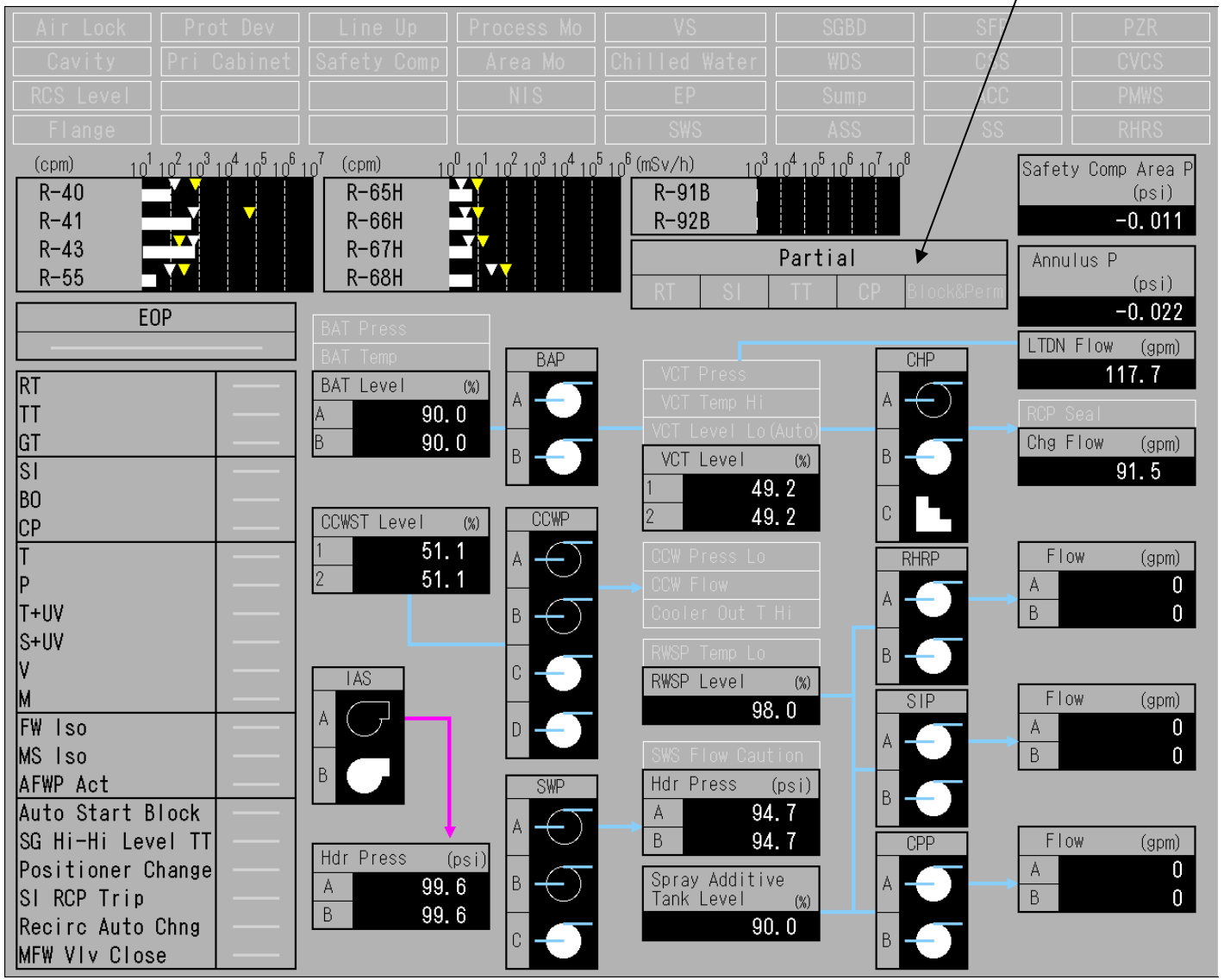
Automated Cross Channel Checks

- **Computers continuously perform cross channel checks**
  - ✓ Operators don't need to do this anymore
- **Monitoring and control displays show one parameter, not four**
  - ✓ Four are available on diagnostic level displays
- **Control systems use all channels**
  - ✓ No effect from single channel failures
- **Operators respond to channel deviation alarms**
  - ✓ Check system level effect (usually none, Partial Trip)
  - ✓ Confirm deviation
  - ✓ Check Tech Spec LCOs
  - ✓ Longer term action
    - Maintenance work order

Automated Actuation Checks

- **Computers check correct actuation of all ESF system components**
  - Pump start, valve line-up
  - ✓ Operators don't need to do this anymore
- **Operators respond to "Not OK" alarms**
  - ✓ Confirm alternate train is "OK", including performance
  - ✓ Longer term action
    - Confirm "Not OK" status
    - Restore to "OK" status
    - Maintenance work order

Large Display Panel



Automated BISI

Bypassed or Inoperable Status Indication

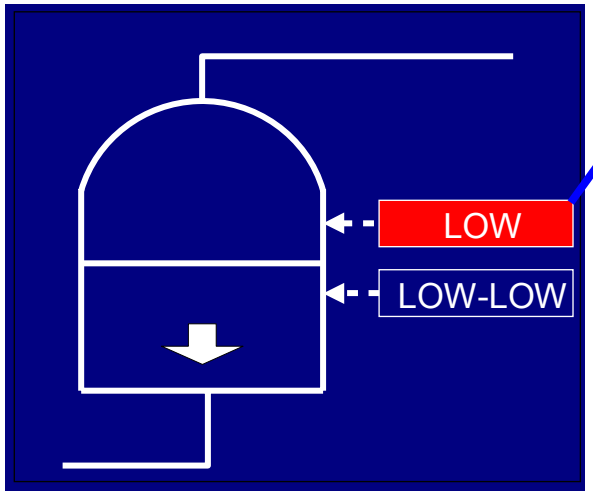
- **Computers monitor components for inoperable or misalignment conditions**
  - ✓ While in standby mode
- **Computers determine and display effects at train level**
  - ✓ Operators don't need to do this anymore
- **Operators respond to "Not Ok" alarms**
  - ✓ Confirm "Not Ok"
  - ✓ Check Tech Spec LCOs
  - ✓ Longer term action
    - Restore to "OK" status
    - Maintenance order

Alarm Management

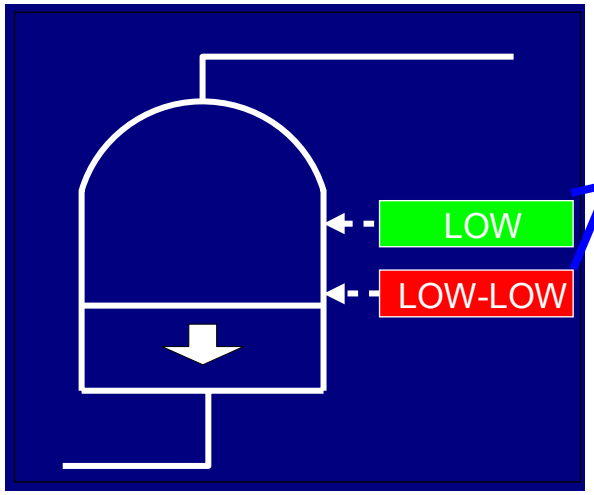
- **Alarm avalanche conditions are common in current alarm systems**
  - ✓ EOPs and training do not credit the alarm system
- **Alarm avalanche conditions are significantly reduced by**
  - ✓ Signal validation
    - – based on automated cross channel checks
      - One process alarm, not one for each division
  - ✓ Cause-consequence dependency logic
    - Plant mode
    - Equipment mode
  - ✓ Prioritization logic
    - Highlights degrading conditions
- **Allows the alarm system to be credited**

Dynamic Alarm Priority Rules (1/3)

Higher prioritization rule



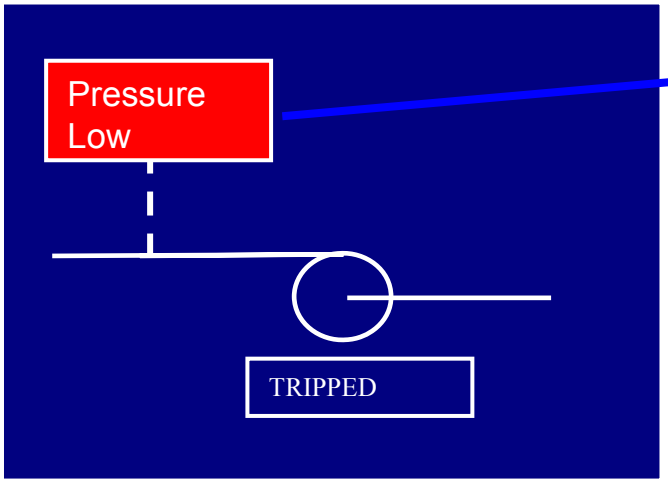
Low alarm is displayed as Priority 1 (alarm information) until the tank level reduces to the Low-Low alarm setpoint.



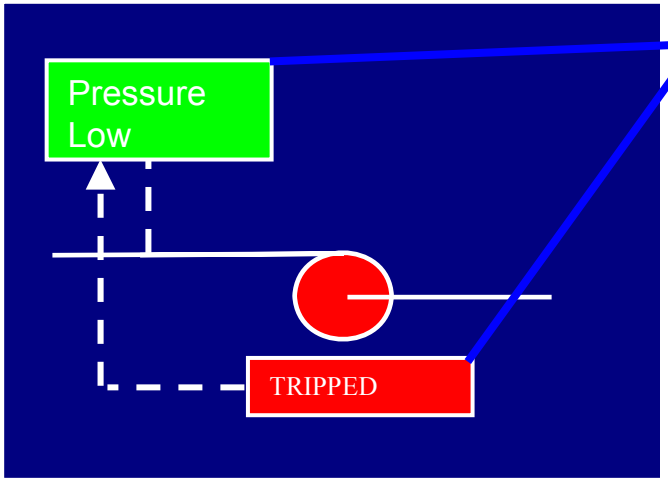
When the level reaches the Low-Low alarm setpoint, the Low-Low alarm is displayed as Priority 1 and the Low alarm is changed to Priority 3 (status information).

Dynamic Alarm Priority Rules (2/3)

Cause-consequence equipment rule



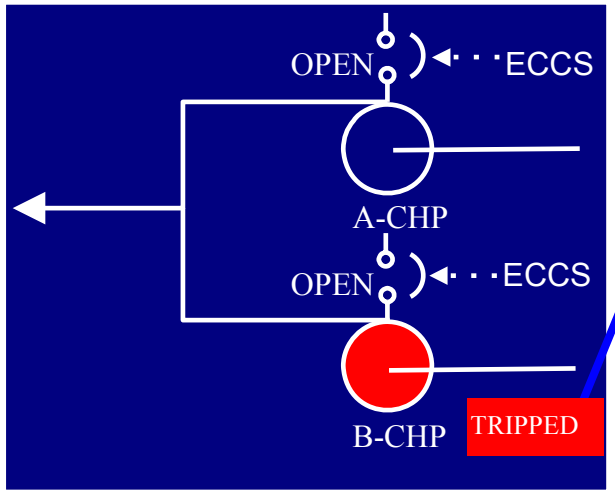
A low discharge pressure alarm is displayed at priority 1 if there is no cause for the alarm.

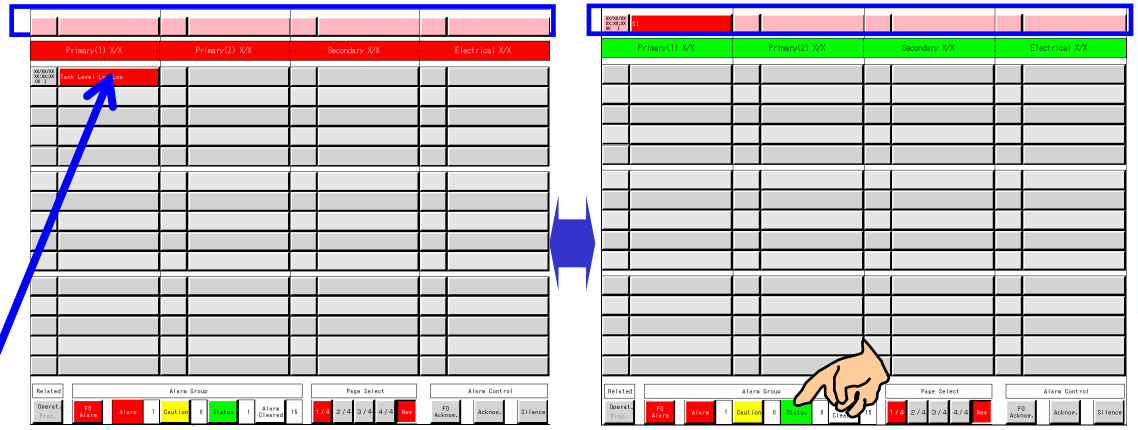


However, the low pressure alarm (“result” alarm) is regarded as Priority 3 when the pump is stopped by the interlock alarm (“cause” alarm) which is displayed as Priority 1.

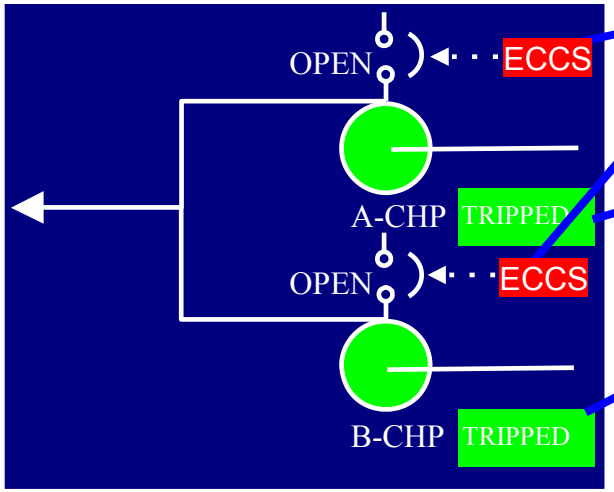
Dynamic Alarm Priority Rules (3/3)

Cause-consequence mode rule





A charging pump trip is displayed at priority 1 if there is no cause for the alarm.

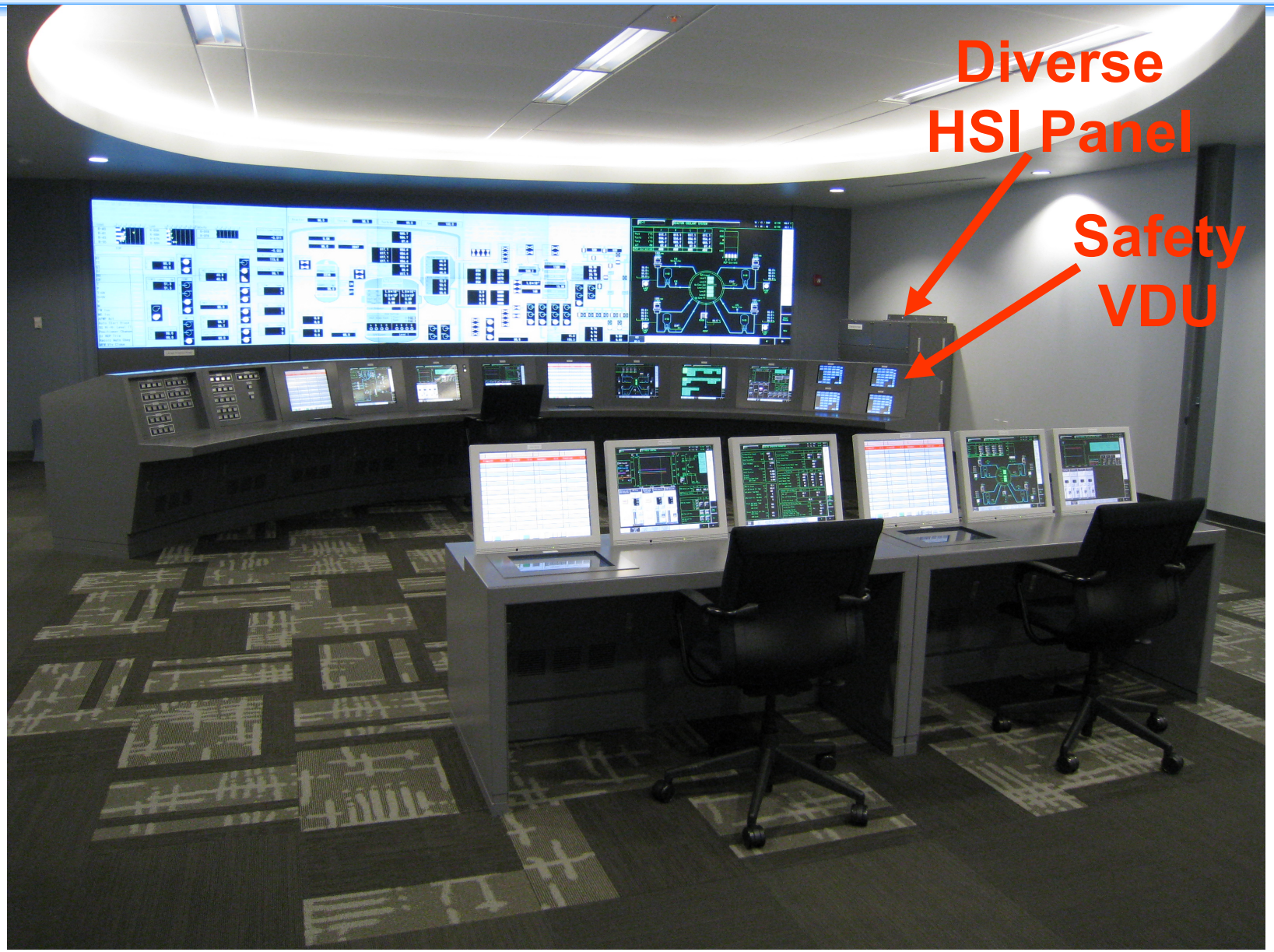


Charging pump trip alarms are regarded as Priority 3 (status information) when an ECCS signal is actuated.

Degraded HSI Conditions

- **Current control rooms**
  - ✓ HSI is an integral part of the plant systems and components (eg. pumps, valves, instruments)
  - ✓ Operators train to cope with plant component failures, not HSI failures
- **New control room**
  - ✓ HSI redundancy to minimize the potential for failures
  - ✓ If an unusual failure occurs, the effect can be much more global (eg. complete VDU freeze)
    - In addition to training operators for plant component/system failures, we must also train them for HSI failures
    - This is further complicated by NRC criteria for consideration of common cause failure
      - Adds even more training for beyond design basis events
  - ✓ Degraded HSI may be the most significant operator training challenge

Degraded HSI Conditions



Summary

- HSI technology evolution in new control rooms will reduce routine operator task burden
- Digital technology has proven highly reliable
- Regardless, operators must be well trained for degraded HSI conditions