North Anna/Surry PCS Data Diode Implementation

Dominion Energy®

R*Time Installation

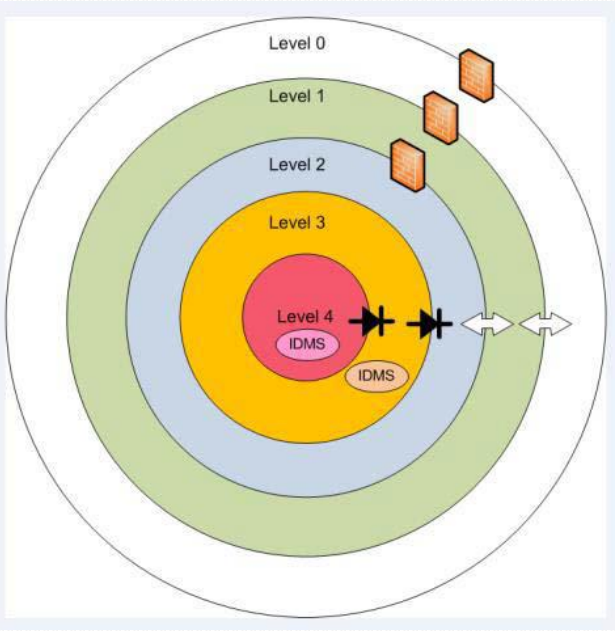
December 2017

- Installed Data Diodes at both Surry and North Anna Power Stations
- Implemented R*Time in Emergency Planning facilities
- Maintained the same Plant PCS (SAIPMS) within the Control Room
  - Created an isolated system

What drove us

Milestone 8

- Full cybersecurity plan implementation accompanied by continuous evaluation and monitoring.

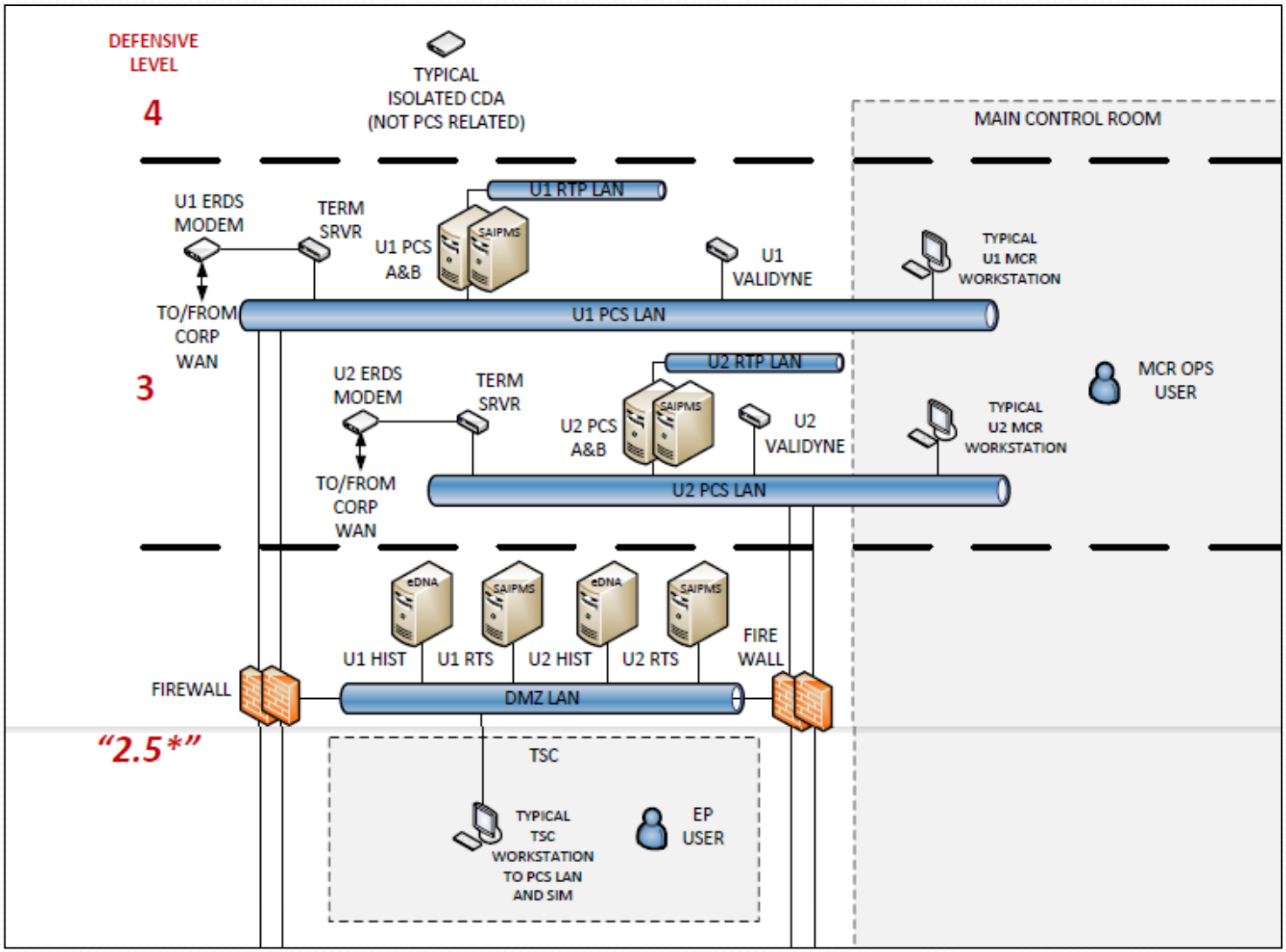


Level 0 – The Internet
Level 1 – Corporate WAN
Level 2 – Station LAN
Level 3 – Security/EP Infrastructure (PCS)
Level 4 – Safety and Security

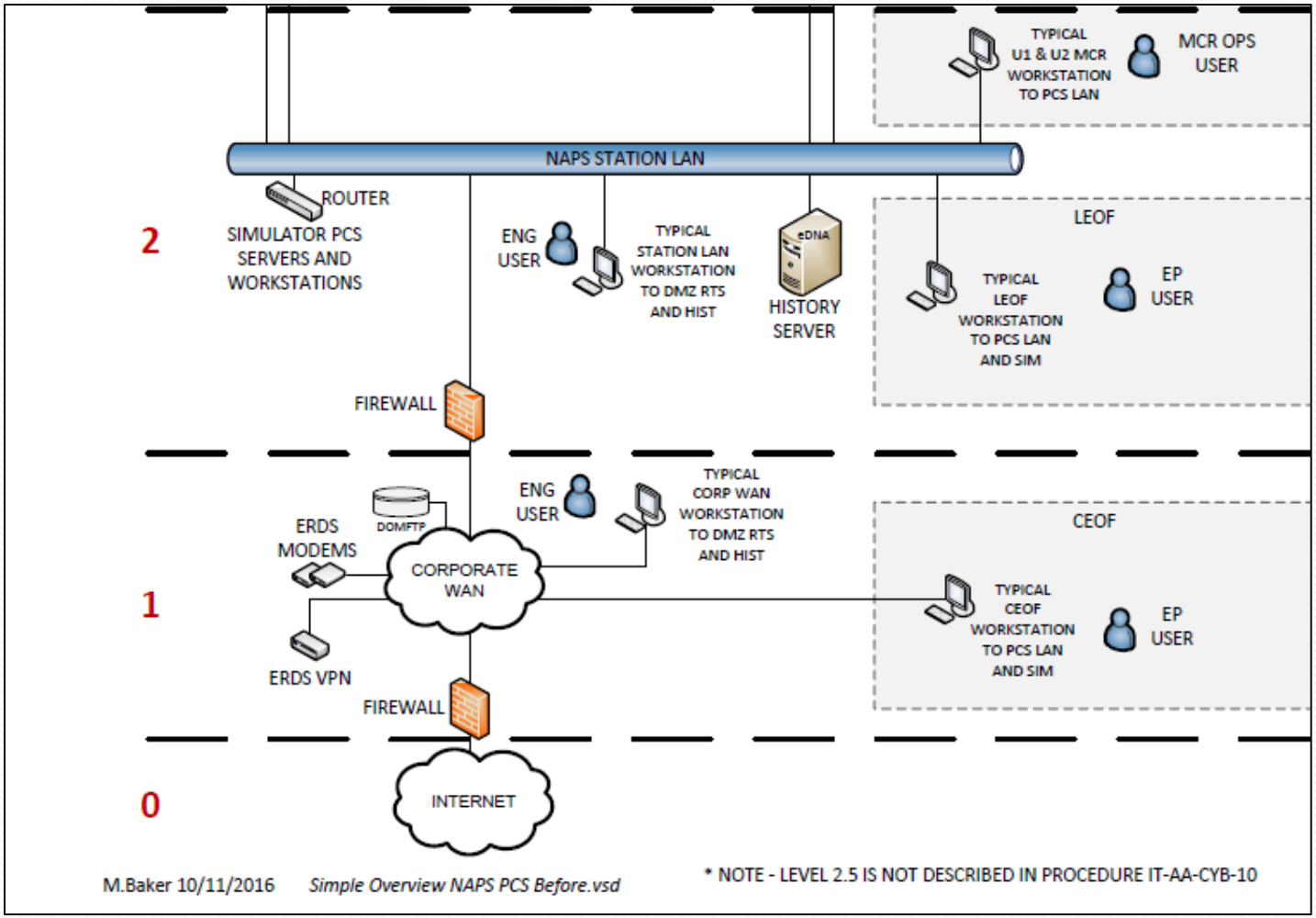
What Drove Us

To improve the cyber security defensive architecture of the Plant Computer System (PCS), a deterministic one way data flow for critical networks was applied via data diodes. This enforced unidirectional data flow from the protected PCS LAN to server.

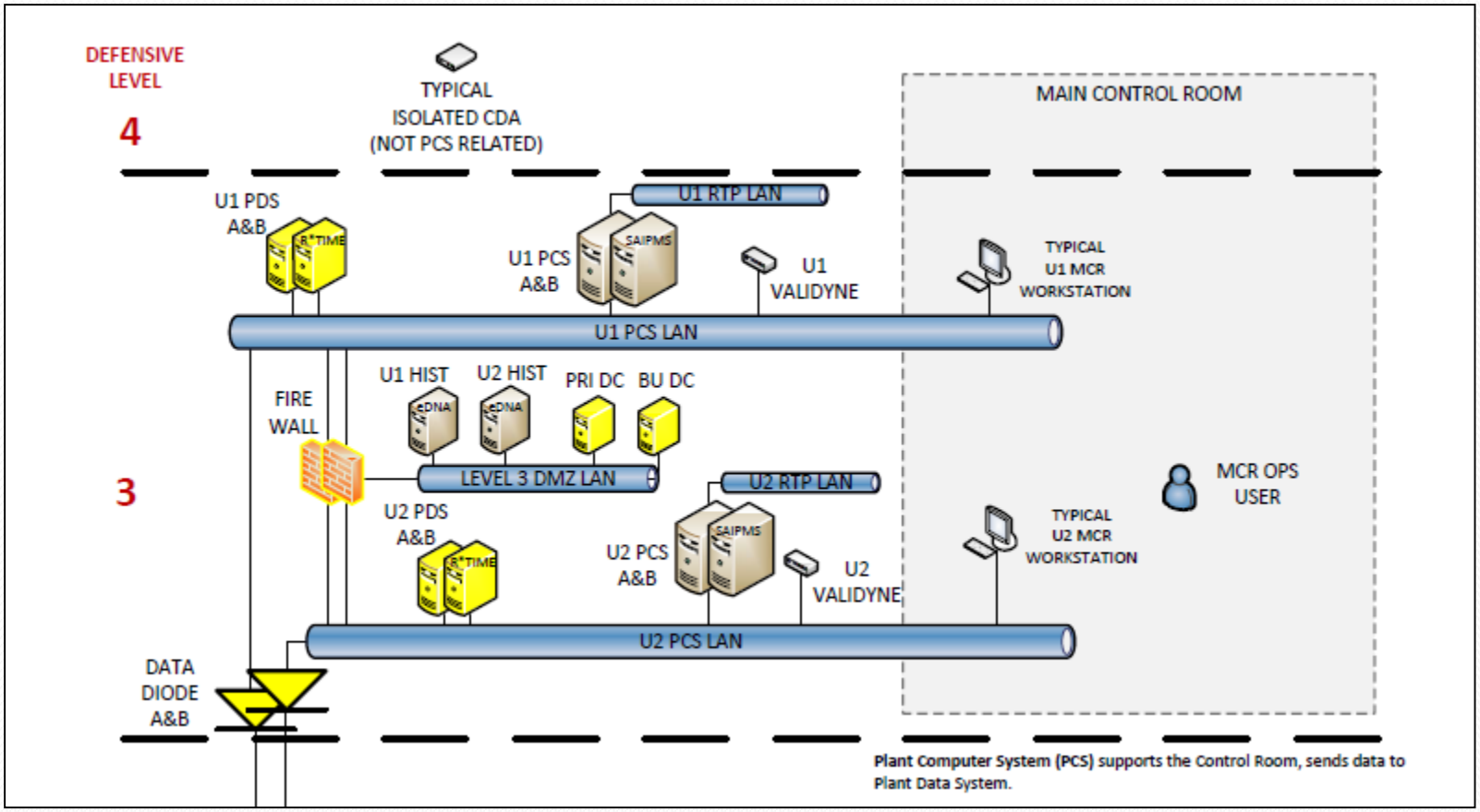
Configuration (pre Data Diode)



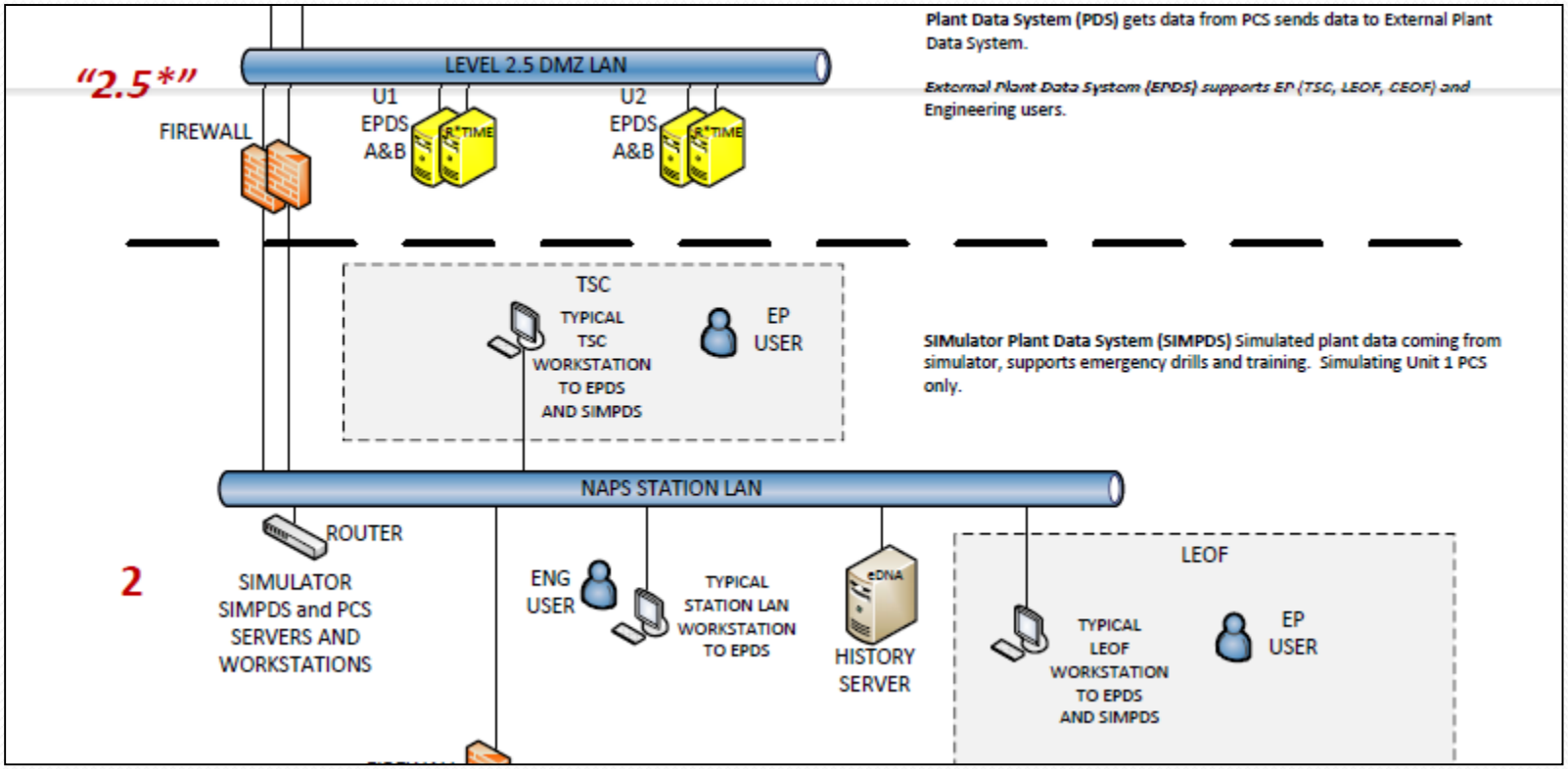
Configuration (pre Data Diode)



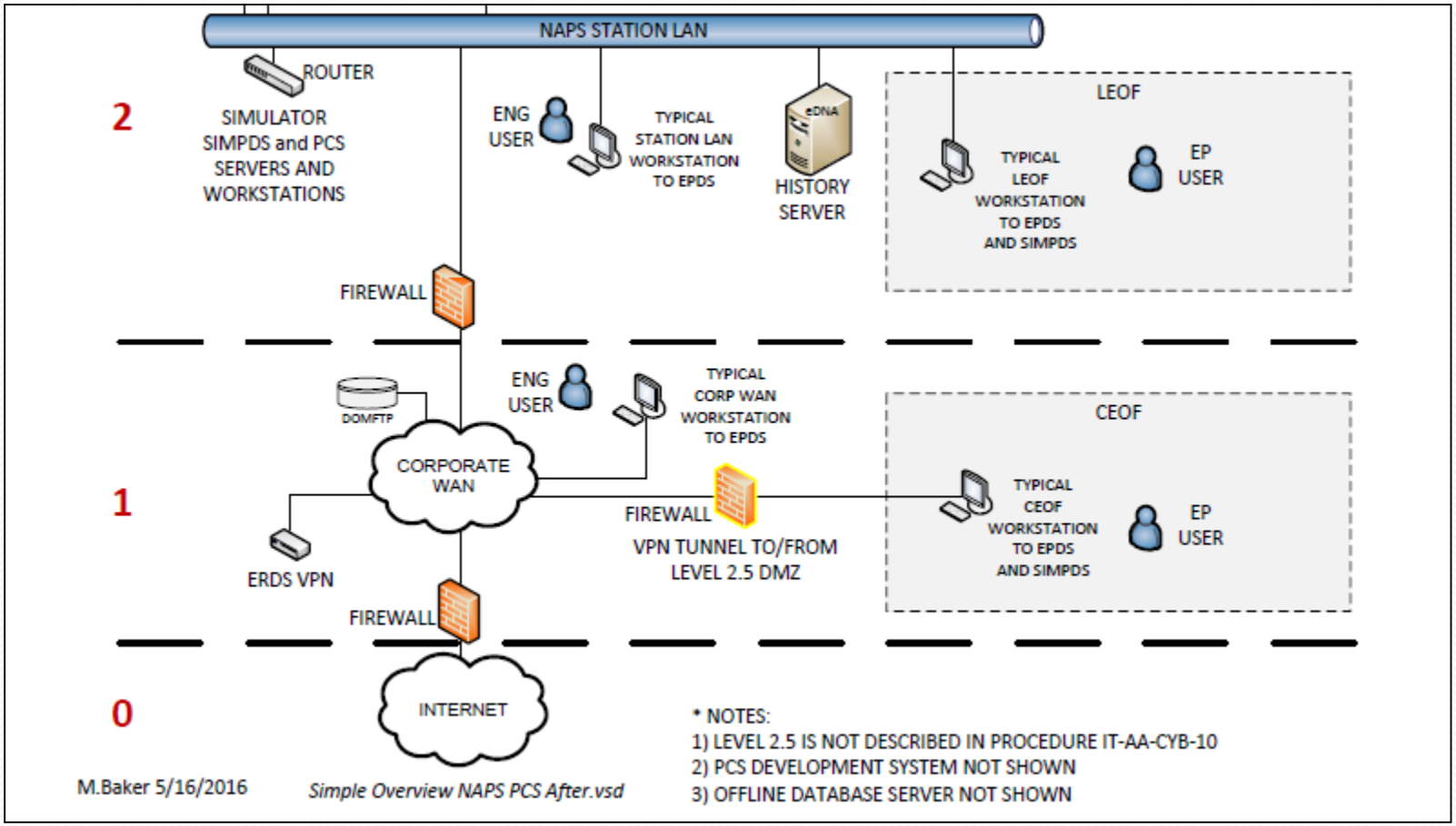
Configuration (post Data Diode)



Configuration (post Data Diode)



Configuration (post Data Diode)



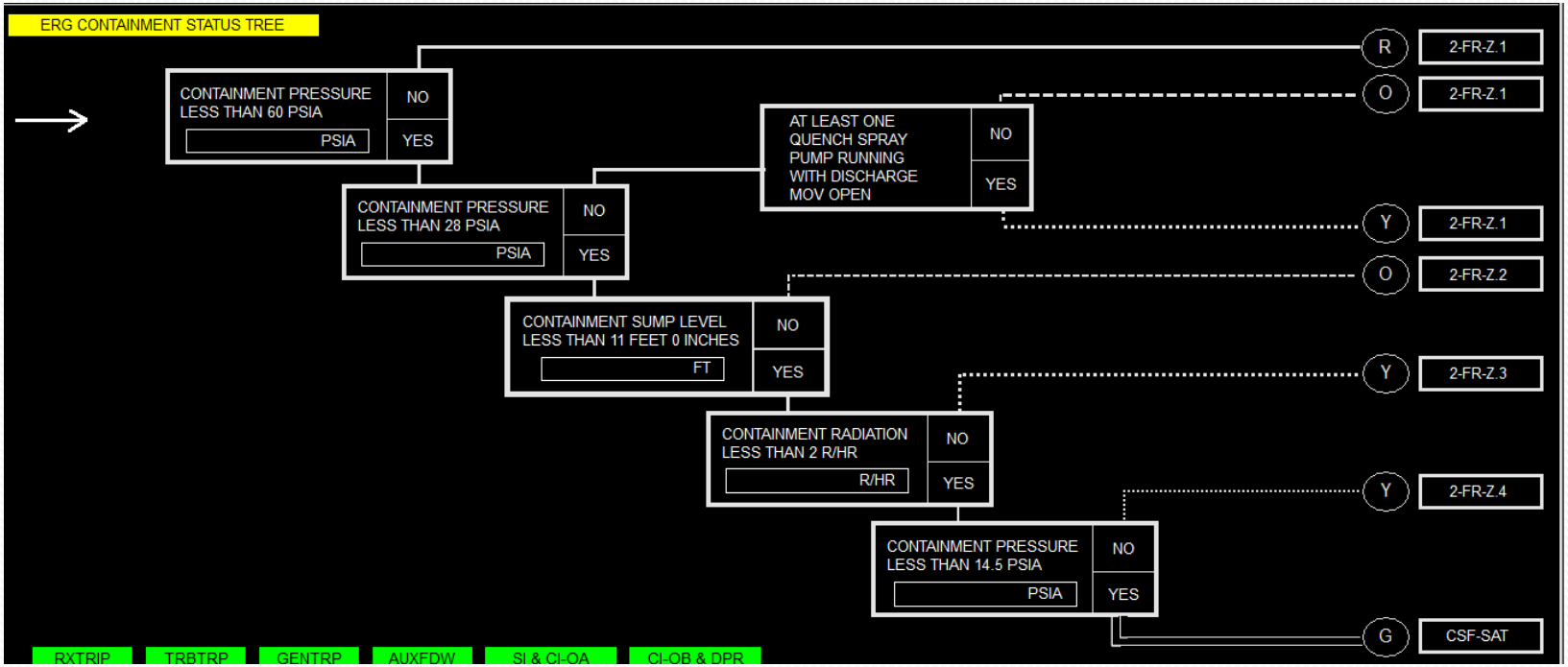
What PCS functions were impacted?

An evaluation was done to determine what processes would be lost by implementing Milestone 8:

- Flux Map Data
  - Files not available for analysis on the Corporate LAN
- Logs and reports
  - Logs that were stored on level 3 server could no longer be accessed outside the PCS LAN (72 hour Power History, Equipment Run Time, Post Trip, Integrator, etc.)
- MIDAS
  - Data no longer sent via FTP from the Plant PCS server

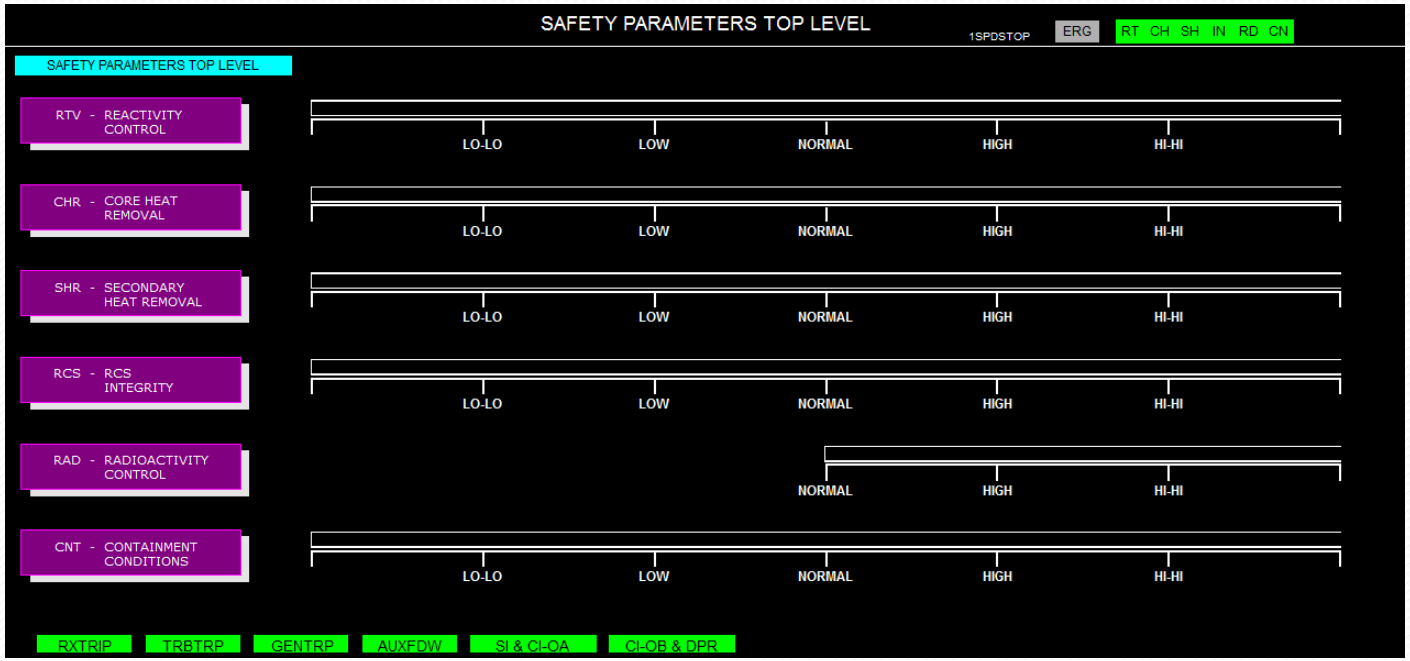
What PCS functions were impacted?

- ERG status tree
  - Impacted embedded calculations



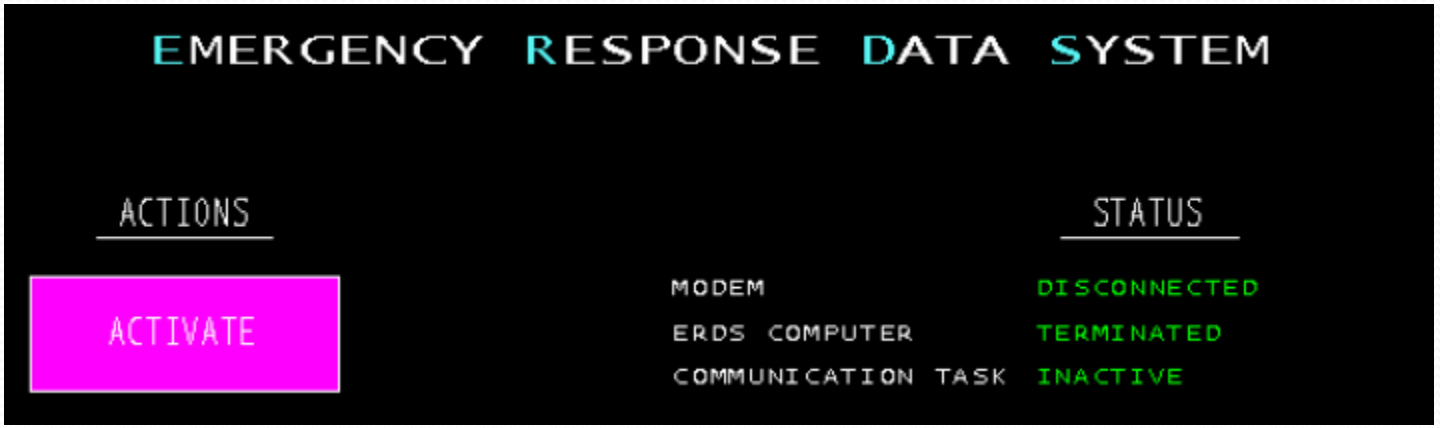
What PCS functions were impacted?

- Safety Parameter Display System
  - Dynamic bars would need to be recreated
  - Workstation monitoring could not track by IP address



What PCS functions were impacted?

- Emergency Response Data System (ERDS)
  - Data originates from Plant PCS and is transferred through a modem connected to a phone line
  - ERDS Modem/VPN Repeater was designed by Curtiss Wright to auto answer the incoming call and connect to the NRC through the NRC VPN.



What PCS functions were impacted?

- Real Time Server (RTS)
  - Used for MMI users on the Station LAN and Emergency Response Facilities (LEOF/TSC/CEOF)
  - Relied on bidirectional communications between Primary Servers and workstations on the Station and Corporate LAN.
  - Replicated Control Room displays as read only

Post Data Diode Installation

- R*Time allowed the display of plant data through the data diodes, replacing the function of the Real Time Server
- Majority of Plant PCS displays were replicated and validated in Factory Acceptance Testing (FAT)
- MIDAS
  - Now originates from R*Time servers
  - Reduction in connectivity issues

Post Data Diode Installation

- Owl Data Diode FTP function configured to FTP to the Level 2 Corporate Network Share
  - Flux Map files, logs and reports are manually transferred from the Plant PCS through the data diode on demand
- ERDS function moved to R*Time for better troubleshooting
  - Elimination of dial up modem and VPN Converter workstation
  - ERDS Data streamed directly to ERDS VPN appliances

Post Data Diode Installation

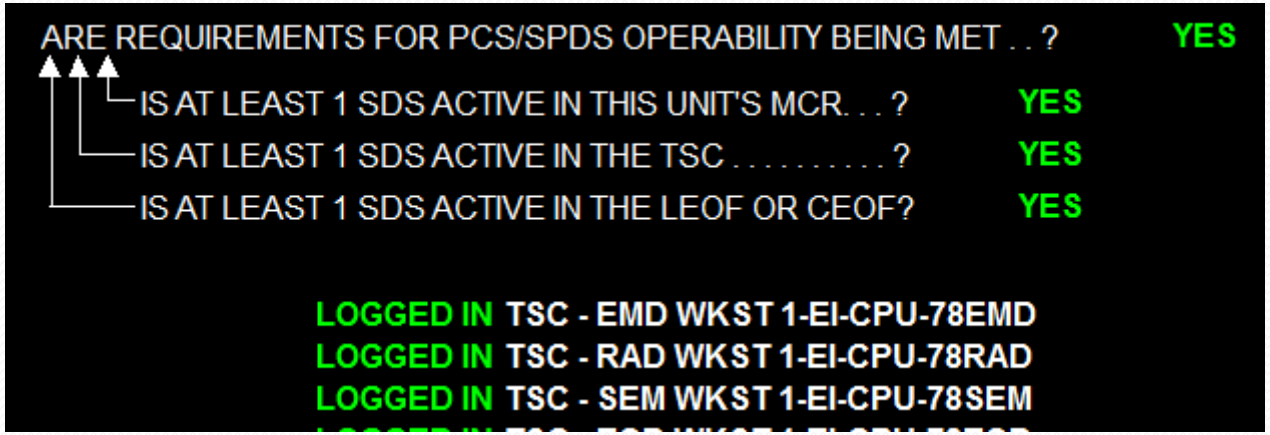
- Real Time Server (RTS) elimination
  - R*Time replaced the function of the RTS
  - R*Time made available to users on the Corporate WAN and all Emergency Facilities
- Simulator Archive Replay
  - Ability to replay pre-recorded archive data from drill scenarios
  - Display recorded data in emergency response facilities without requiring direct connection to Simulator

Issues

- Operator Rounds
  - Access to Plant PCS no longer available on
  - Cannot compare plant versus PCS indications in the field
- I&C technicians
  - Not able to use R*Time for PCS point Calibrations
- Reactor Engineering
  - R*Time data cannot be used for Reactivity Calculations
  - Log collection requires Plant PCS access

Issues

- R*Time display screens took longer to load compared to PCS.
- SPDS Workstation Monitoring required workstation names versus ip addresses



Lessons Learned

- More stakeholder participation from the start of the project was necessary
  - Operations, Engineering, Emergency Preparedness, Simulator Support
  - Site Acceptance Testing is not a proper place to modify functionality (multiple screens, function keys, basic screen design)
- Multi-departmental review of documentation needed
- Reviews of R*Time displays conducted in a more timely manner

Lessons Learned

- Ensure timely training is conducted prior to implementation
  - Engineers were not familiar with the functions available until 2 months after implementation

Questions?