CONTROL SYSTEM CONSIDERATIONS CHP PLANTS

John Beaudry, PE

6/9/2014

Overview

- Types of Control Systems
- Reliability and Availability
- Strategy
- Network Protocols
- Cybersecurity issues
- Alarm Management
- Examples

Types of Controllers

- **Direct Digital Control Systems**
- **Distributed Control Systems**
- **Programmable Logic Controllers**
- **SCADA**

Direct Digital Systems (Building Automation Systems)

- **Designed for HVAC Controls**
  - Built in Routines for Air Handlers, VAV Boxes, Energy Saving
  - Network to Chillers, CRAC Units, Roof Top Air Handlers, etc.
  - Scheduling for Occupancy
  - ASHRAE 90.1, Energy Code Required Routines Built In.
- **Tightly Integrated Graphics and Controls**
- **Reliability Is Not Designed Into Base Product**
- **Proprietary Marketing Limits Support**

DDC Systems are Not the Normal System of Choice for CHP

Distributed Control Systems

- **High Reliability**
  - Designed for Redundancy (Controllers and HMI) - $$$
- **Tightly Integrated Graphics and Field Controllers**
- **Originally Replacement of Single Loop Control (Analog Control)**
- **Support network limited for some DCS vendors**

Programmable Logic Controllers

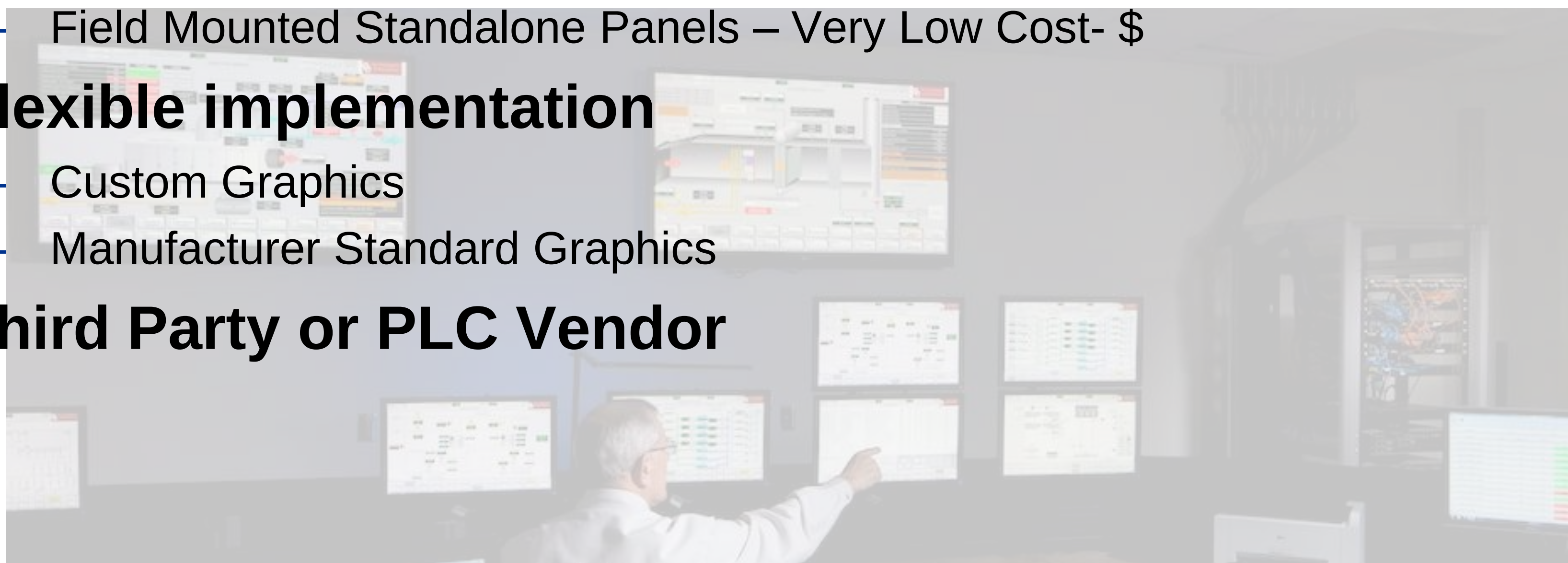
- **Scalable from High Reliability to Lower Cost**
  - Relay Replacement (Low Cost) - $
  - Redundant PLC's (High Relability) - $$
- **Originally Replacement of Relays**
- **Flexible Implementation**
- **Large Support Networks**

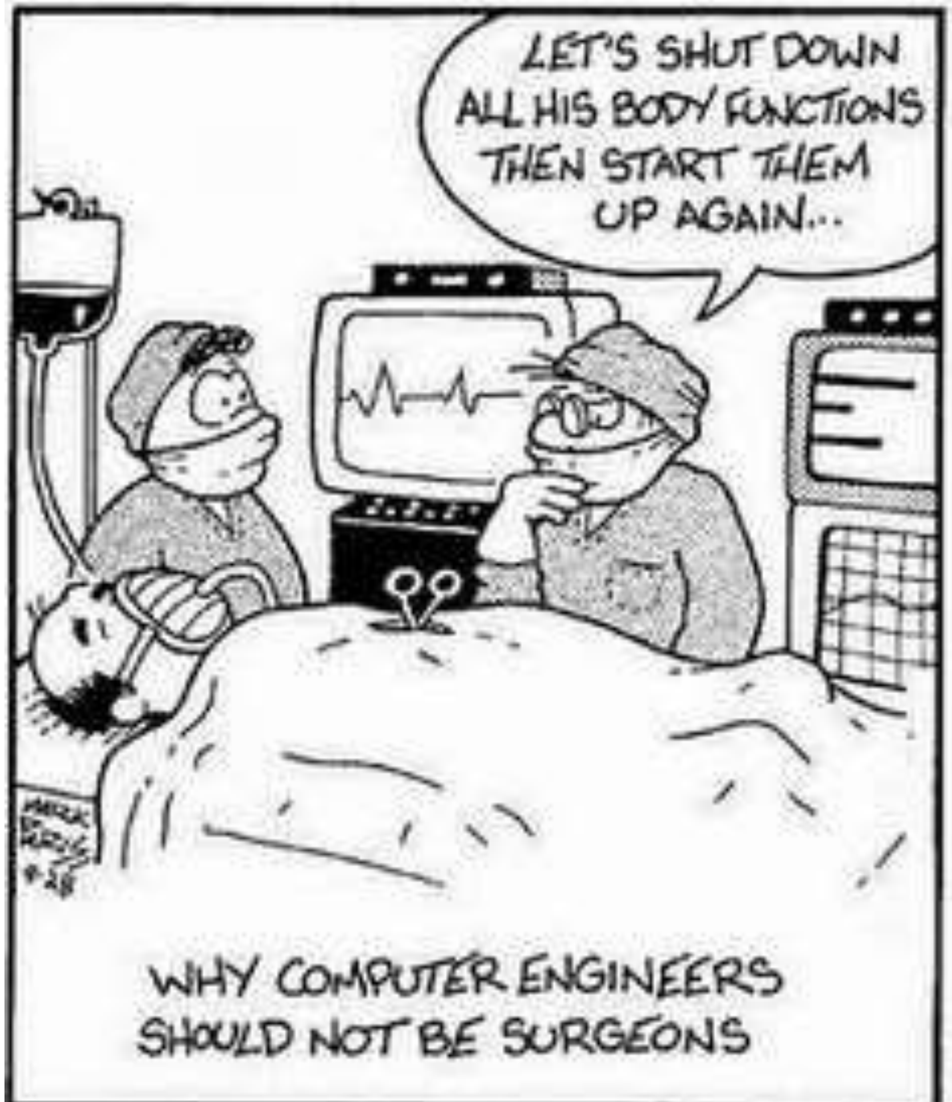
Virtually No Difference Today Between DCS and PLC or PAC Hardware

JACOBS

SCADA

- **Graphics Representation of the Process**
- **Data Collection for Human-Machine Interface or HMI**
- **Historical Data**
- **Scalable from High Reliability to Lower Cost**
  - Server Grade Redundant Equipment - $$
  - Capable of Virtual Server Redundant Applications -$$
  - Field Mounted Standalone Panels – Very Low Cost- $
- **Flexible implementation**
  - Custom Graphics
  - Manufacturer Standard Graphics
- **Third Party or PLC Vendor**




LET'S SHUT DOWN ALL HIS BODY FUNCTIONS THEN START THEM UP AGAIN...
WHY COMPUTER ENGINEERS SHOULD NOT BE SURGEONS

JACOBS

Reliability vs. Availability

- **Reliability –the control system doesn't shut down the process upon a failure of the control system. Usually *economic* impact.**
- **Availability - probability that the control system shuts down the process when needed. Usually *safety* related.**

Reliability vs. Availability

- A highly reliable system may not be a safe system. Both are desired, but there is a tradeoff between reliability, availability, and cost.
- Balance of Plant high reliability (economic).
- Boiler Safeties high availability (safety)
- Processor and Network redundancy eliminates some single points of failure and may increase the availability and reliability.
- Triple Modular Redundancy is an approach to achieve high reliability with high availability. TMR is very expensive.

Reliability – Availability – Cost

Strategy of Controls

- **Stick Built Controls Strategy**
  - All Stick-Built Controls where single Plant Control System
  - Vendors provide detailed Sequence of Operation description
  - Advantages:
    - **Common hardware software for all systems**
  - Risks:
    - **No Single point of responsibility – potential finger pointing**
    - **Higher cost of hardware, integration, engineering**
- **Vendor Skid Controls Strategy**
  - Skid stand alone vendor skid controls
  - May be integrated into larger Control System
  - Advantages:
    - **Vendors single point of responsibility**
    - **Cost effective**
    - **Stand alone operation**
  - Risks:
    - **Hardware from multiple vendors**

JACOBS

Vendor Skid Controls Specification

- **PLC, or DCS – Common Platform**
- **Local HMI (Human Machine Interface) for Local Control**
- **Communication Media**
  - Ethernet
  - Serial
- **Communication Protocols**
  - Native to PLC, or DCS (Ethernet IP, Profibus)
  - Common Protocols (i.e. Modbus RS-485, Modbus TCP/IP, BacNet)
- **Redundancy**
  - PAC, PLC, or DCS
  - Network communications to Plant Control System
- **Interlocks to Plant Control System**
  - Hardwire vs. Networked

Networks

Ethernet

- **Modbus TCP/IP**
- **Ethernet IP**
- **DNP3 LAN/WAN protocol**
- **IEC 61850 GOOSE**
- **ProfiNet**
- **BACnet IP**

Serial

- **Modbus RS-485**
- **Proprietary RS-485 Networks (AB DH+, Modbus+, Genius I/O)**
- **BACnet MSTP**
- **LonTalk**
- **ArcNet**

Although all use Ethernet Media they do not talk nor coexist on the same network

JACOBS

Network Reliability

- **Field I/O**
  - Low bandwidth requirements but fast failover
  - Device Level Redundancy (ring without a switch)
  - Proprietary Rings (N-Ring, HIPER Ring, Turbo Ring)
  - Proprietary Communications (i.e. Controlnet, Profibus DP)

- **PLC to PLC Communication**
  - Device Level Redundancy
  - Proprietary Rings (N-Ring, HIPER Ring, Turbo Ring)
  - Managed Switches
- **PLC to SCADA Communication**
  - High Bandwidth
  - Managed Switches

Field Communication Issues

- **Network Diagnostics**
  - Software for failure conditions
  - Alarming
- **Distributed processing**
  - Equipment such as VFD’s, MCC’s may have logic at the device.
  - Loss of communication may result in motors not capable of being stopped
  - Software may behave differently than hardwired devices (i.e. Auto over-riding Hand control)
  - Motor Fail Logic will not alarm if communications are lost.

JACOBS

Cyber Security

- **Standard IT Security**
  - Require each individual to Login
  - Change Passwords
  - Limit access rights
    - SCADA and PLC development applications should be limited to qualified individuals
    - Standard Login won't allow devices to be stopped and started or Setpoints changed
    - Operator has rights to change setpoints, start and stop devices, but not tune loops or change software
    - Burner Management , HRSG Combustion Controls, Combustion Turbine , Gas Compressors should require special access. May want to limit changes to vendor.
    - Lock out flash drives, CD's, Email, Internet inside the Plant Control System?

Cyber Security

- **Network Security**
  - DMZ Level between Business Network and the Plant Control
  - Firewalls capable of filtering on content and source.
  - VLAN’s with MAC Address Limits on Control Network
- **Patching SCADA/PLC Software and Firmware**
  - US Dept Homeland Security ICS-CERT identifies Hardware Vulnerabilities
  - Firmware Updates may need to be scheduled around downtime.
- **Limit Physical Access**

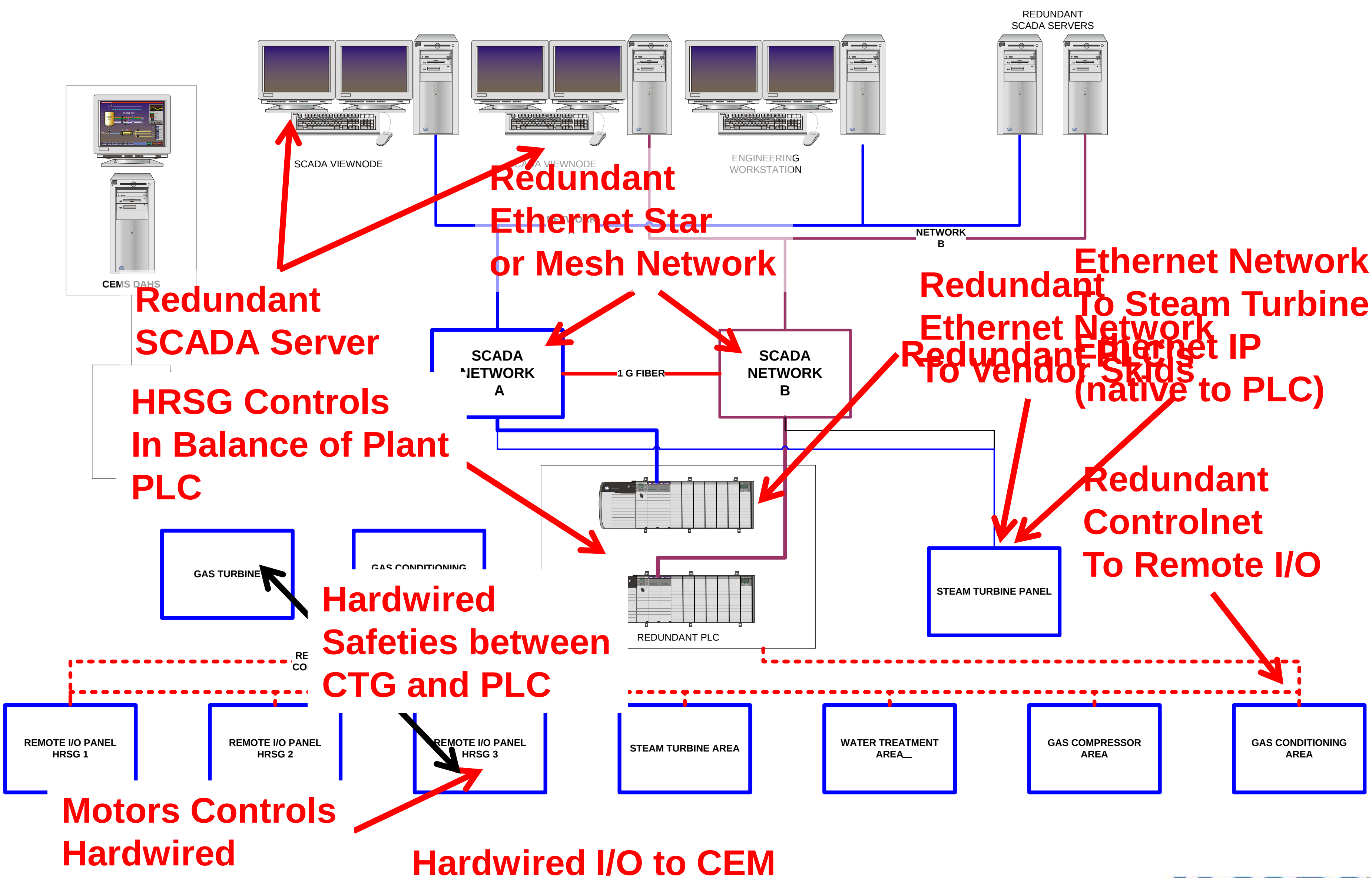
Don’t Forget Alarm Management

- Refinery hardwire alarms ignored (horn wiring cut) when too many/ too frequent alarms.
- Steam Turbine was loosing lube oil, but the operator didn’t see the alarm because the large number of alarms. Close call to loosing all lube oil.
- Large Semiconductor Plant Central Utility Plant couldn’t see motor alarms, nor start/stop motors when DeviceNet network failed. DeviceNet communication alarms were buried in the large number of alarms.
- Cogen Plant lost SCADA communication because Ethernet failure alarms weren’t noticed. Although redundant processors, switches, SCADA servers, system lost complete visibility. Lost ability to shut down HRSG from control room.

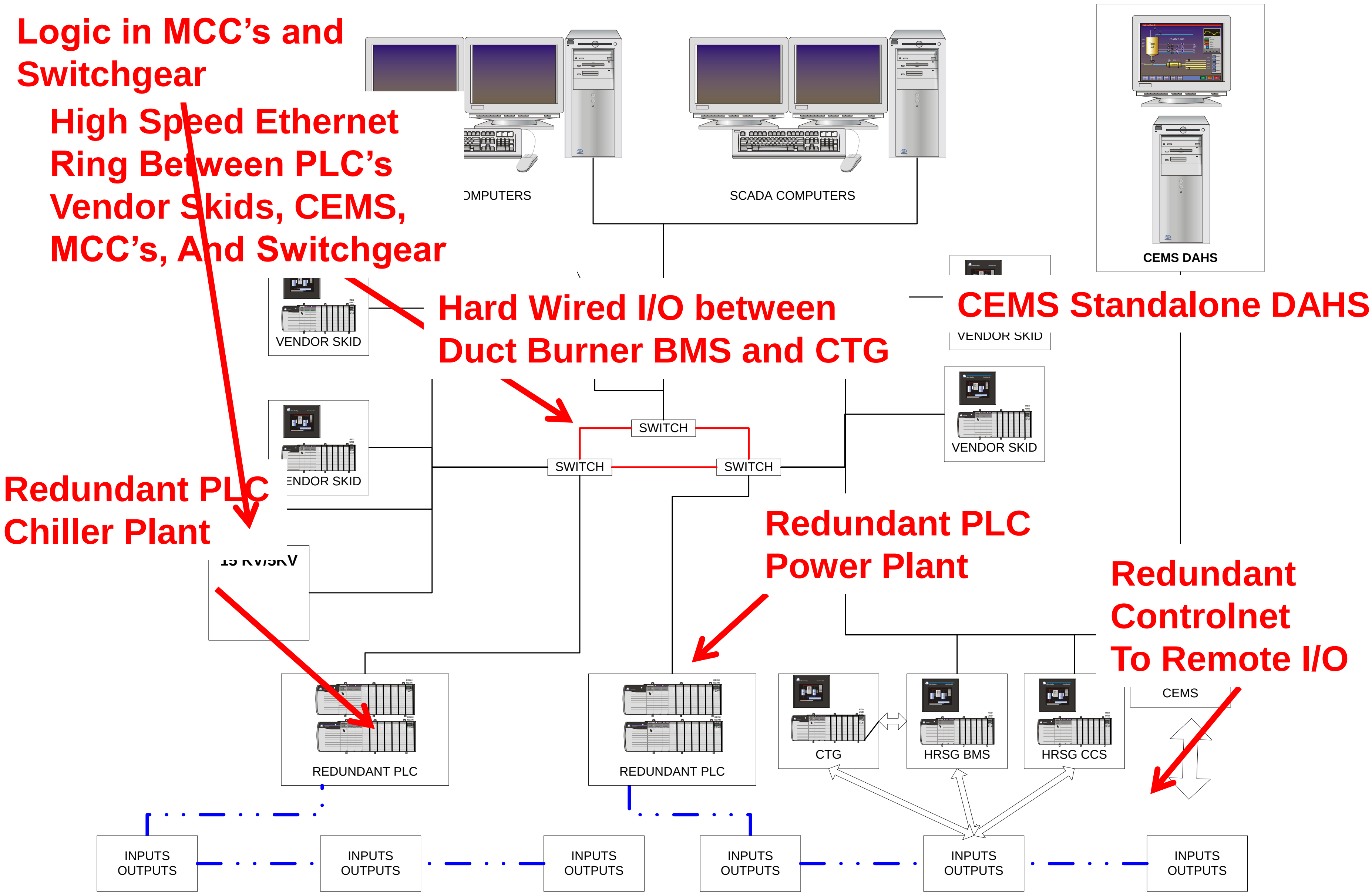
Alarm Management Strategies

- **Only Alarm Important Values – Use Historical Trending for Information**
- **Assign Alarm Priorities**
- **Categorize Alarms by Process Areas**
- **All Network Communications should be highest priority alarms**
- **Alarm Inhibiting**
- **Conditional Alarming**
  - Don't alarm equipment if the equipment is not running
    - **i.e. Inhibit HRSG drum level if the HRSG is down**
  - RODI conductivity shouldn't alarm when the product is being dumped

LA County Sanitation District Carson Plant



Oklahoma University



Overview

JACOBS

Further Reading

Security

- **NIST Special Publication 800-82 - Guide to Industrial Control Systems (ICS) Security**
- **Homeland Security - Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies**
- **Homeland Security - Common Cybersecurity Vulnerabilities in Industrial Control Systems**
- **ANSI/ISA-TR99.00.01-2007 - Security Technologies for Industrial Automation and Control Systems**

Reliability

- **ANSI/ISA 84 Functional Safety: Safety Instrumented Systems for the Process Industry Sector**