Process Control Systems
Industry Conference

Industrial Network Design Panel

La Jolla Torrey Pines, CA
28 Aug 08
Craig S. Schiro - Moderator
ExxonMobil Development Co.
PCSF Board Of Directors
Oil & Gas Sector

Orientation / Background

- **Security that is not enabling, is not useful to achieving the mission of the enterprise**
- **Securely bringing the work to the right people and systems independent of geographic location and time is an industry need**
- **Information at the "atomic level" must be securely accessible in right time by the right person or system in order to accomplish mission of the enterprise**
- **The most pervasive technologies are not proprietary technology or solutions**
- **There is great power in the fact that we expanding connectivity to control systems however there is increased potential of increasing risk**
- **In many enterprises such as ours, we operate under fundamental tenants where there is no compromise to Safety, Health, Environment, Security (SHES)… Nobody gets hurt!**
- **Certainly the issues to address and solve the above are not going to be solved within this 105 minute panel session.**
- **The Industrial Network Design Panel will address two topics**
  - Network Segmentation
  - Legacy and Mobile End Devices
- **We have two of the largest network security solution providers on the panel to offer current technology solutions that we can use to address some of these concerns**

Panelists

- Raphael Pereira (Chemtech)
- Jules Vos (Shell)
- Larry Spoonemore (Southern)
- Eric Cosman (Dow)
- Steve Venema (Boeing)
- Steve Hargis (Enterasys)
- Serhii Konovalov(Cisco)
- Craig Schiro ExxonMobil - Moderator

Session Objectives:

- **Using a cross-sector end-user group alongside solution providers drive towards understanding** common **design elements applicable to ICS networks.**
- **Using this panel session, demonstrate the** value of cross-sector end-user, solution provider collaboration **by working a limited set of topics as a sample.**
- **Stimulate interest in continuing the collaboration on other related topics through a PCSF supported Working Group**

Agenda

- **Introduction (Craig Schiro) - 10 minutes**
- **Panel Discussions – 50 minutes**
  - Topic #1, Network Segmentation - 15 minutes
    - Eric Cosman, ChemITC Survey
    - Jules Vos & Steve Venema
  - Topic #2, Legacy and Mobile End Devices - 15 minutes
    - Larry Spoonemore & Raphael Pereira
  - Solution provider input - 20 minutes, 10 apiece
    - Serhii Konovalov (Cisco)
    - Steve Hargis (Enterasys)
- **Audience driven panel Q&A – 40 minutes**
- **Wrap up and next steps – 5 minutes**
  - Propose next step options to continue this collaboration and dialogue (PCSF Working Group?), future vision (IETF)

Process Control Systems
Industry Conference

American® Chemistry Council

ChemITC

Eric Cosman
(Dow)

Purpose

- **Survey ChemITC members and others to collect information on their experience with network separation**
- **Identify lessons learned, challenges faced and general trends**
- **Basic questions:**
  - Are companies practicing network separation?
  - If so, what are the results?

Survey Design

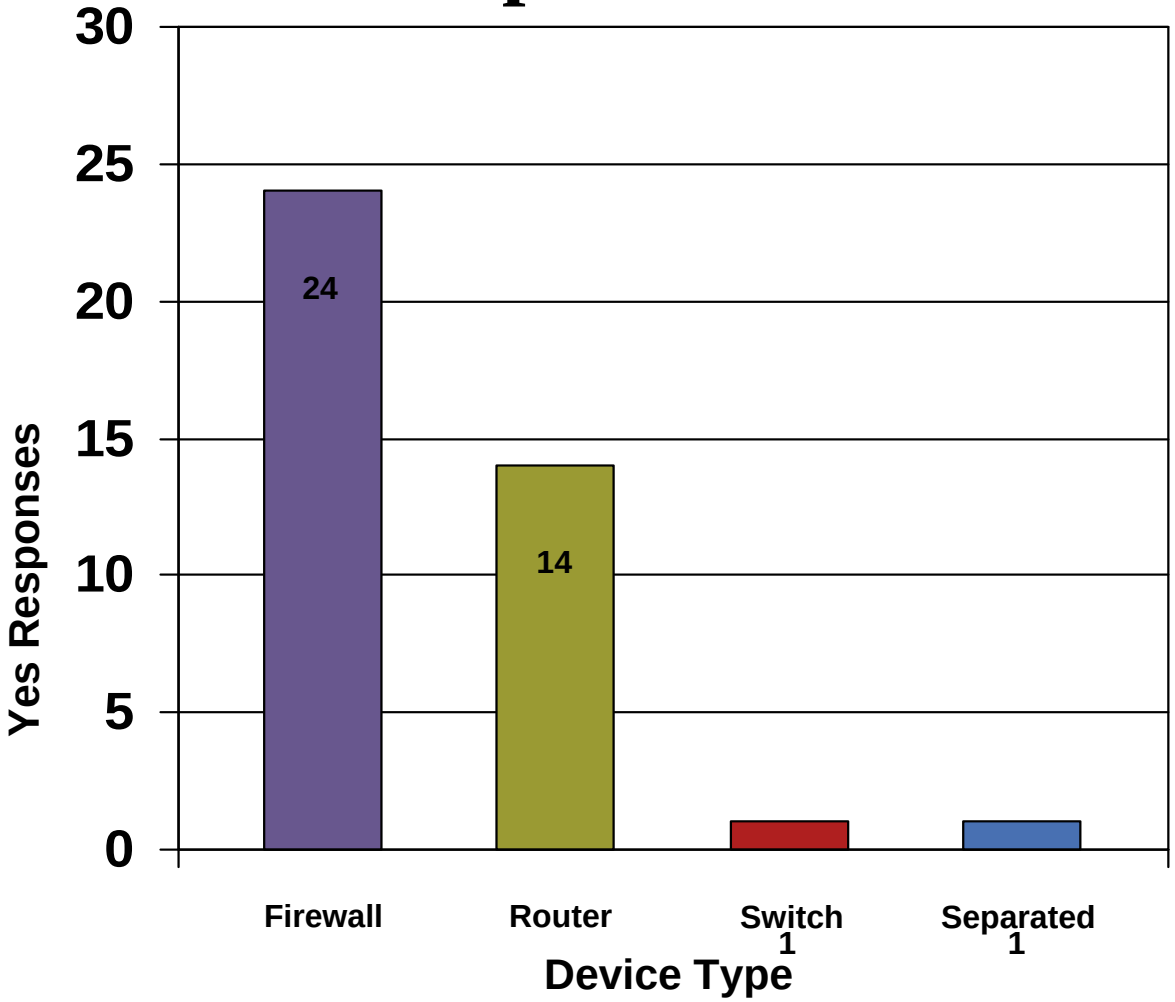
- **Fourteen questions in three categories**
  - Network separation practices
  - Program status
  - Operation and support
  - Assessment of results

Response

- **Thirty responses received**
  - 15 identified as ChemITC members
  - 6 from other organizations
  - 9 unspecified (early responses)
- **Response rate compares favorably to number sent**

Selected Results

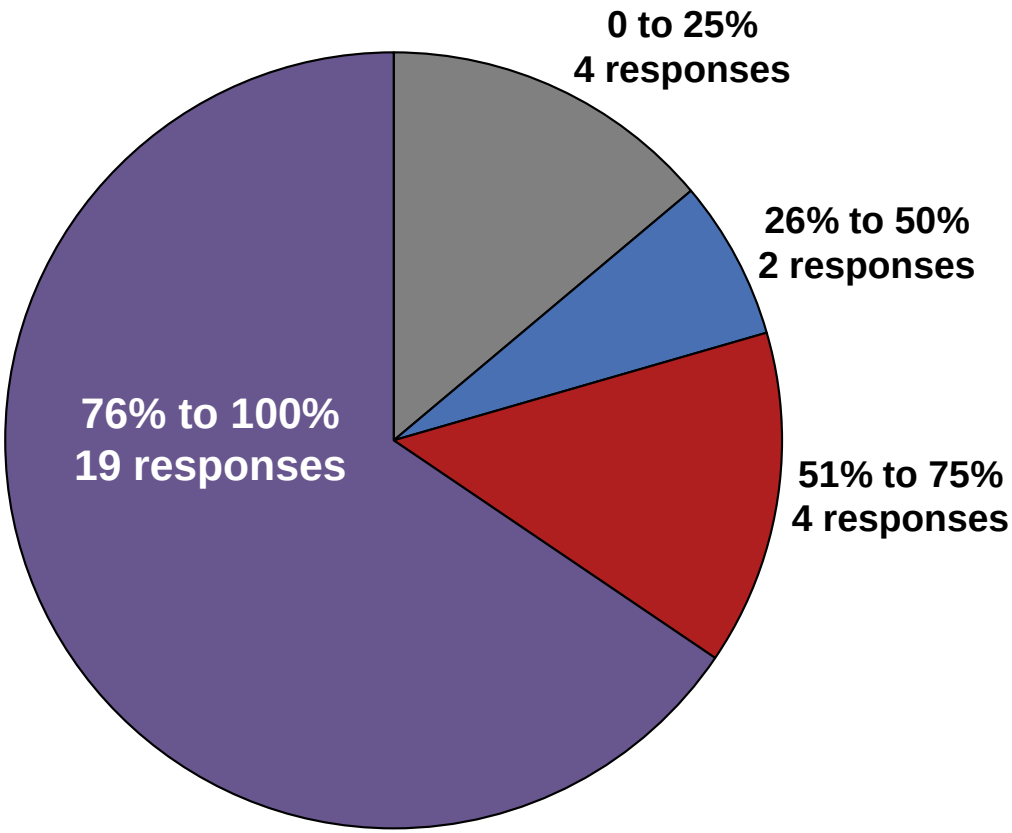
Network Separation Devices



- 24 (80 percent) use firewalls
- 10 use both
- 4 use router only
- Only 1 response indicated complete <u>physical</u> separation

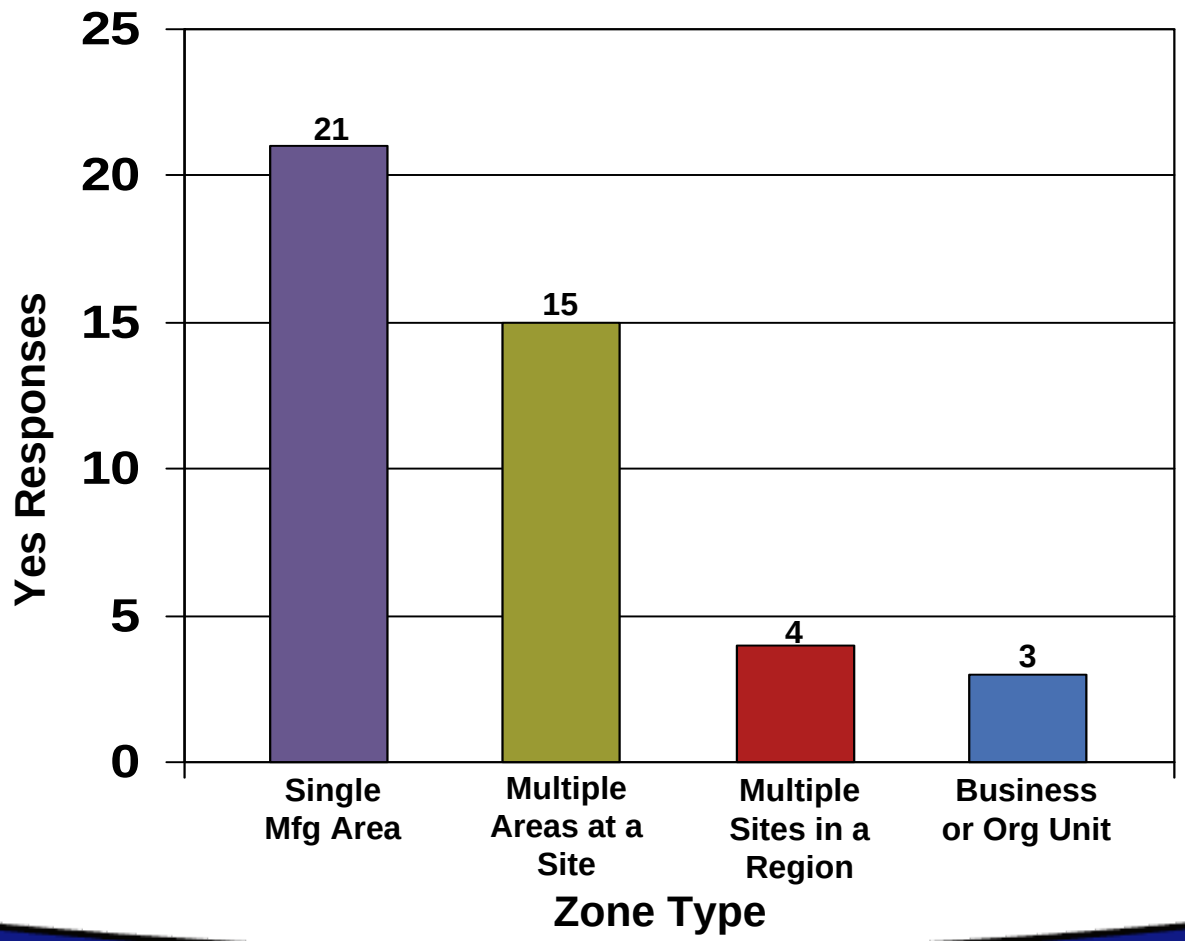
Process Control Systems Industry Conference

Implementation Status



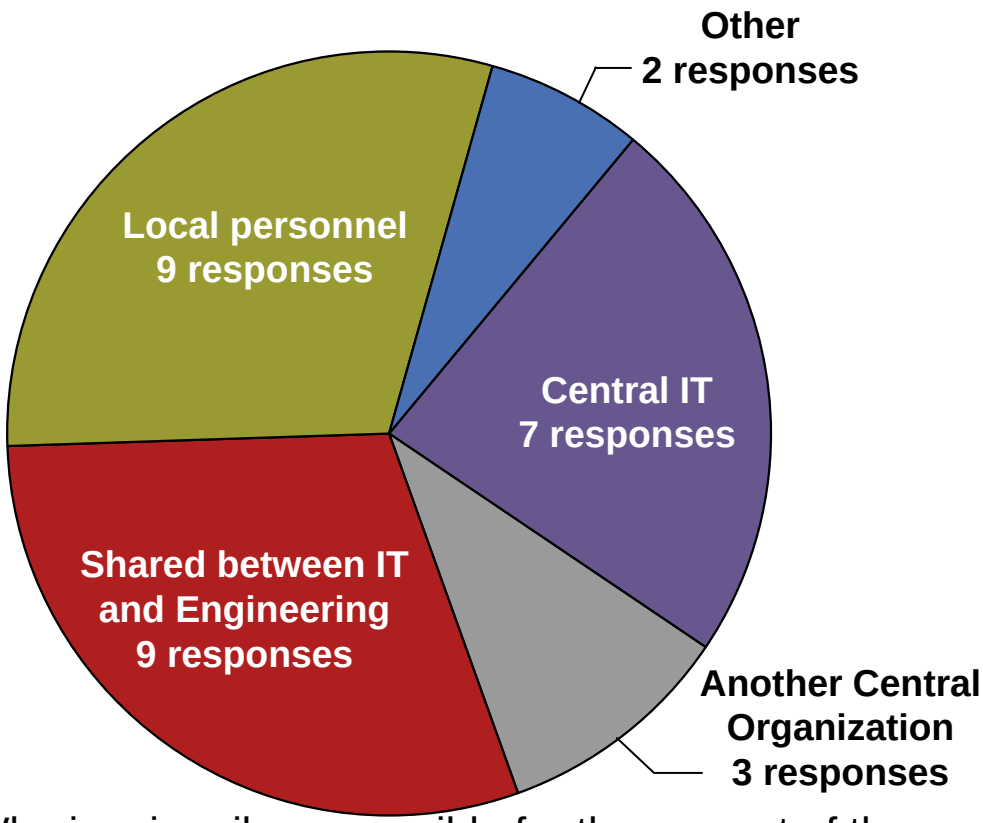
- More than 60 percent of respondents indicate program is 75 to 100 percent complete
- Only 20 percent show a program in the early stages

Zone Types



- Primary focus is on a single plant or unit
- A site-wide approach is also quite common
- Some attempts to address larger geographical areas (region or business unit)

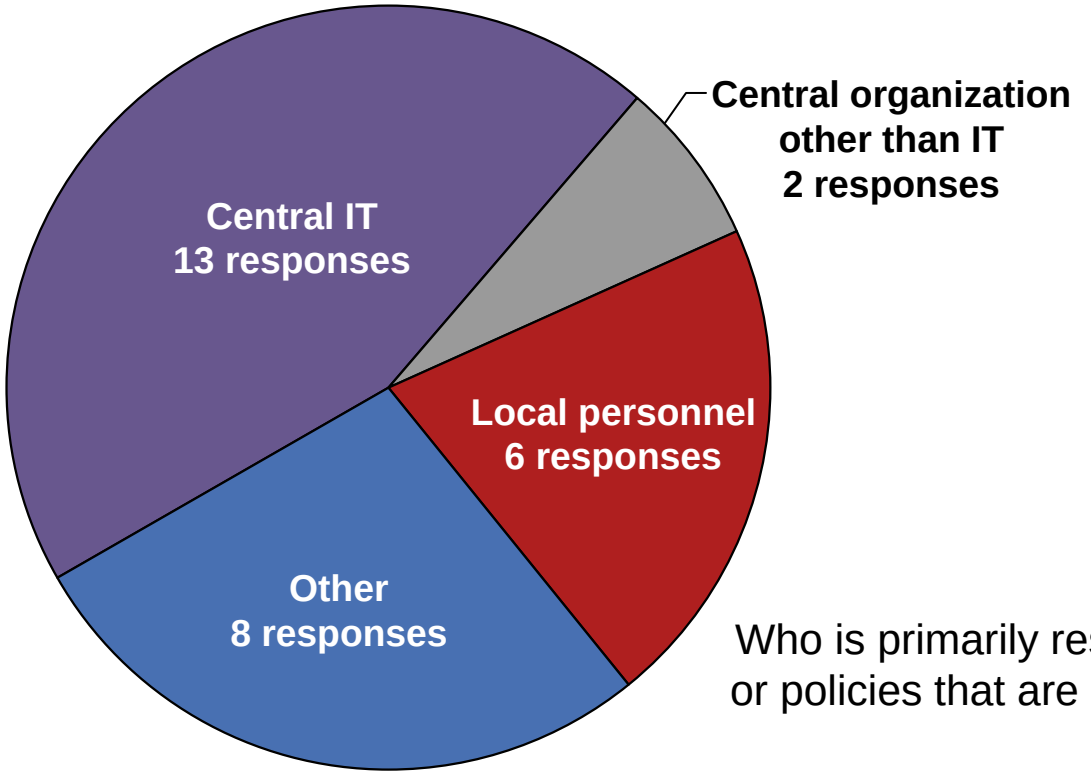
Process Control Support



- Less than 25 percent use the Central IT organization
- 30 percent use site personnel
- 30 percent share responsibility between IT and Engineering

Who is primarily responsible for the support of the systems used in process control?

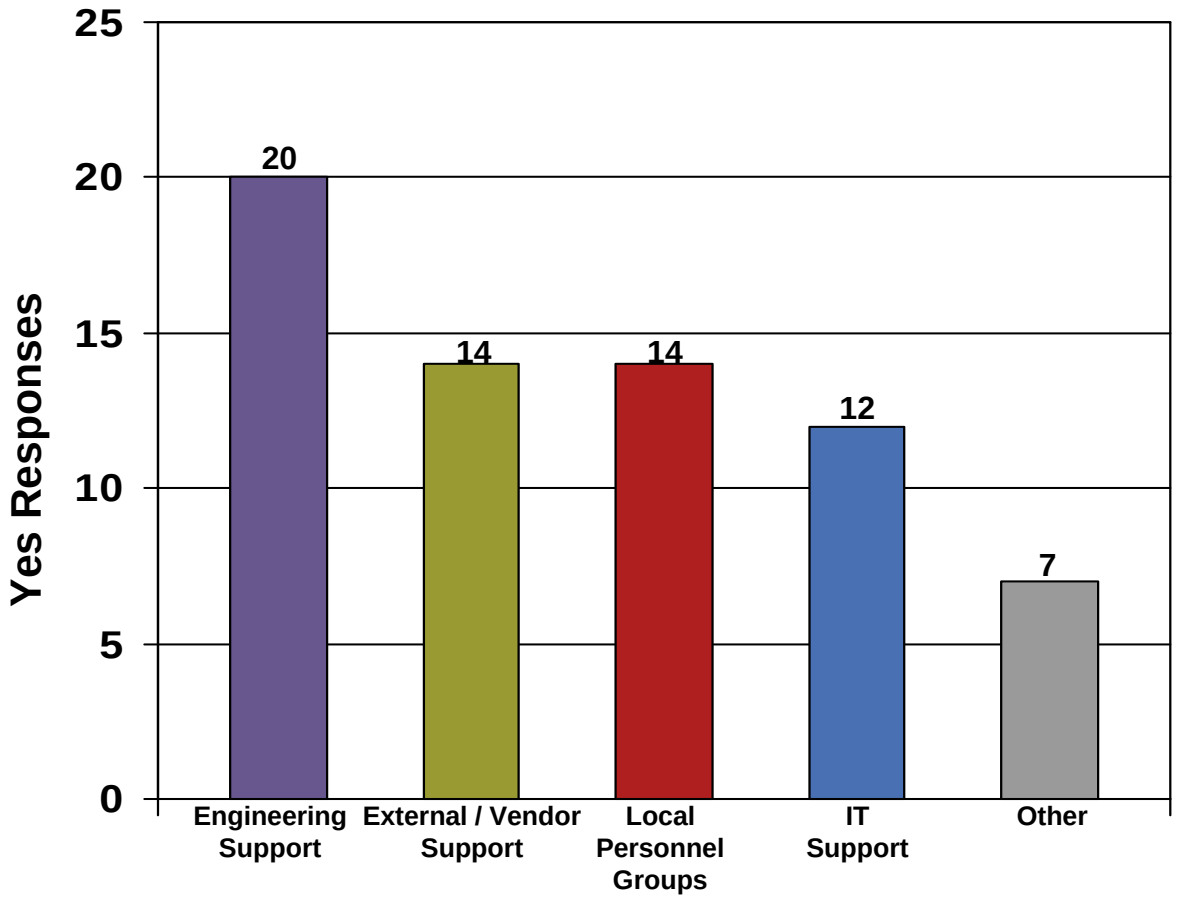
Rule Approval



- **Much more diversity in approach**
- **Less than 50 percent place this responsibility with their central IT organization**

Who is primarily responsible for approving the rules or policies that are used on your network separation devices?

Remote Access



- 90 percent have employed remote access
- Only about 50 percent use external vendors

Look for more information at http://www.chemicalcybersecurity.com

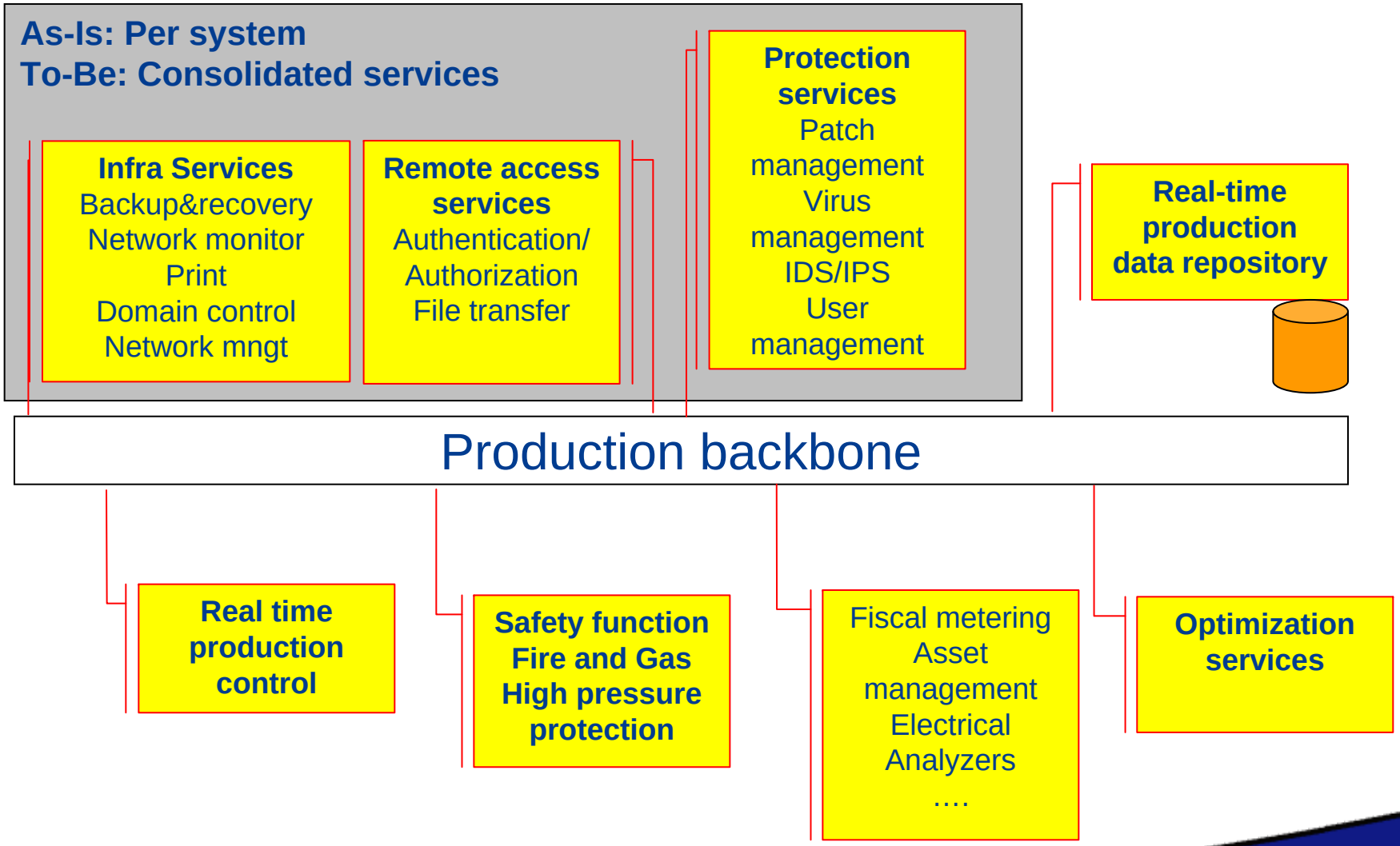
Thank You

Process Control Systems Industry Conference

End Users Requirements

Jules Vos
Shell

Security related functions in total architecture



Architecture design criteria

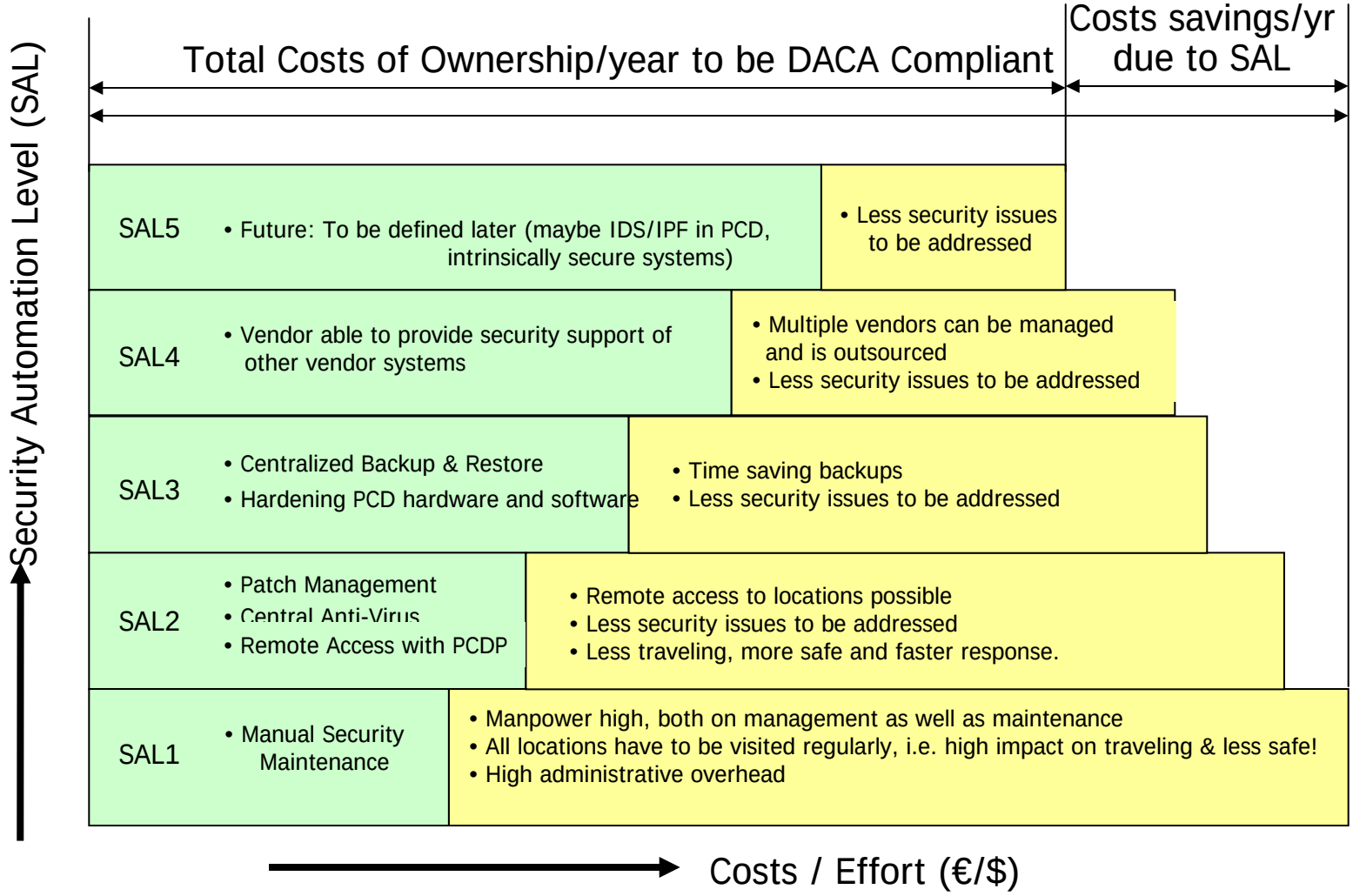
- Objectives shall be an integrated process control domain. So mandatory business and IT principles shall be defined and communicated to vendors
- Vendors shall be able to seamlessly integrate into the end-user infrastructure without a duplication of functionality and services.
- Minimum access: User, system and application access to any components within the PCD shall only be allowed for which they have explicit access privileges.
- Consider logical separation of groups of systems within the process control domain
    - to reduce the impact of security incidents
    - to protect against hopping
    - to separate system responsibility
- Physical separation of control and safety systems
- Design shall take system, function and data criticality into account.
- Include all business critical systems such as DCS, SIS, SCADA, metering, electrical, vibration monitoring, rotating, subsea, QMI, Data Hist, Asset man. Etc.

The majority of remediation work includes processes and procedures

System security…the lifecycle approach

- IT security awareness for **all** control domain users
- Embedding of Data Acquisition and Control Architecture (DACA) in all (system) lifecycle stages
    - Design – *services – applications -infrastructure*
    - Implementation – *hardening – malware prot.*
    - Testing – *vulnerability check*
    - Operation – *patch/virus mngt – portable media – changes – backup and recovery*
    - Demolition – *destruction of sensitive data*
- Avoid publication of sensitive information
    - Topology – IP address – Model code's
- Excellent security governance
    - Quick and strict response to new vulnerabilities

Compliancy and vendor capability



Compatibility
(Vendor effort)
80-90 % CAPEX

Compliance - Compatible
(Shell effort)
80-90 % OPEX

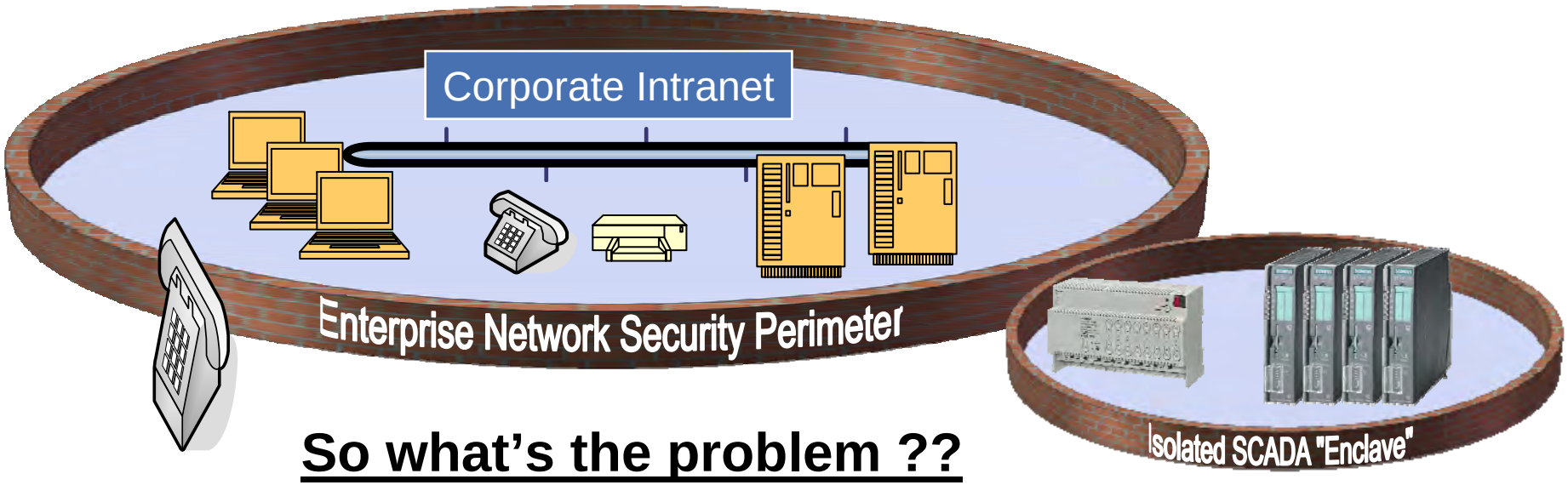
Compliance
According to ITCI-117
(Shell Security Requirements)

Process Control Systems
Industry Conference

SCADAnet Overview

Steven C. Venema
Boeing

SCADA Connectivity Problem Statement



So what's the problem ??

- Need for reduced wiring plant costs implies no more parallel networks
- Need for wireless connectivity implies centralized spectrum management
- Need for standard network capabilities like DHCP, DNS, 802.1x, etc.

We have little or no power to improve this in the near term due to long product life cycles (decades!) and current industry practices

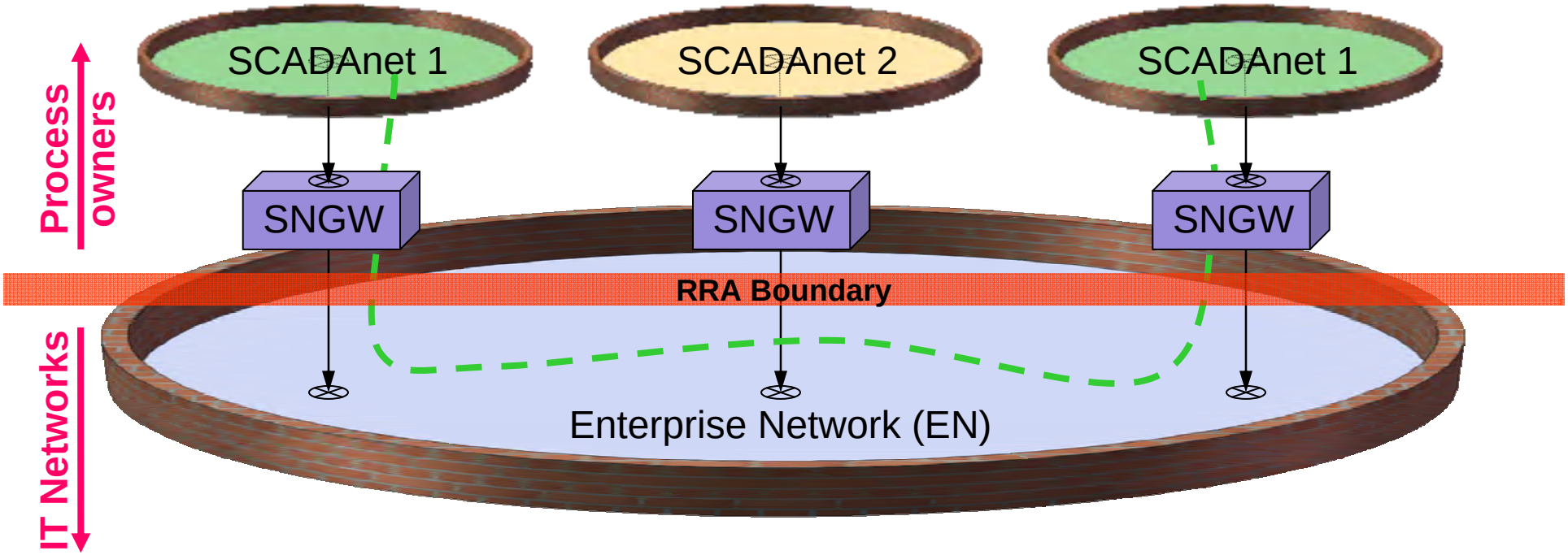
**** Need to work this in the Standards communities ****

**** Need a scalable interim solution ****

SCADA Connectivity Goals

1. **Leverage standards-based enterprise LAN/WLAN infrastructure**
   - Minimize use of non-standard connectivity infrastructure
2. **Provide data isolation "Enclaves" for SCADA device groups**
   - Address the weak security posture of legacy/new SCADA equipment
3. **Enable process owners to rapidly deploy and alter SCADA connectivity**
   - Maximize flexibility, minimize IT and facility impacts
4. **Allow for flexible mixture of network technologies**
   - Wired & wireless, private and shared links, link redundancy

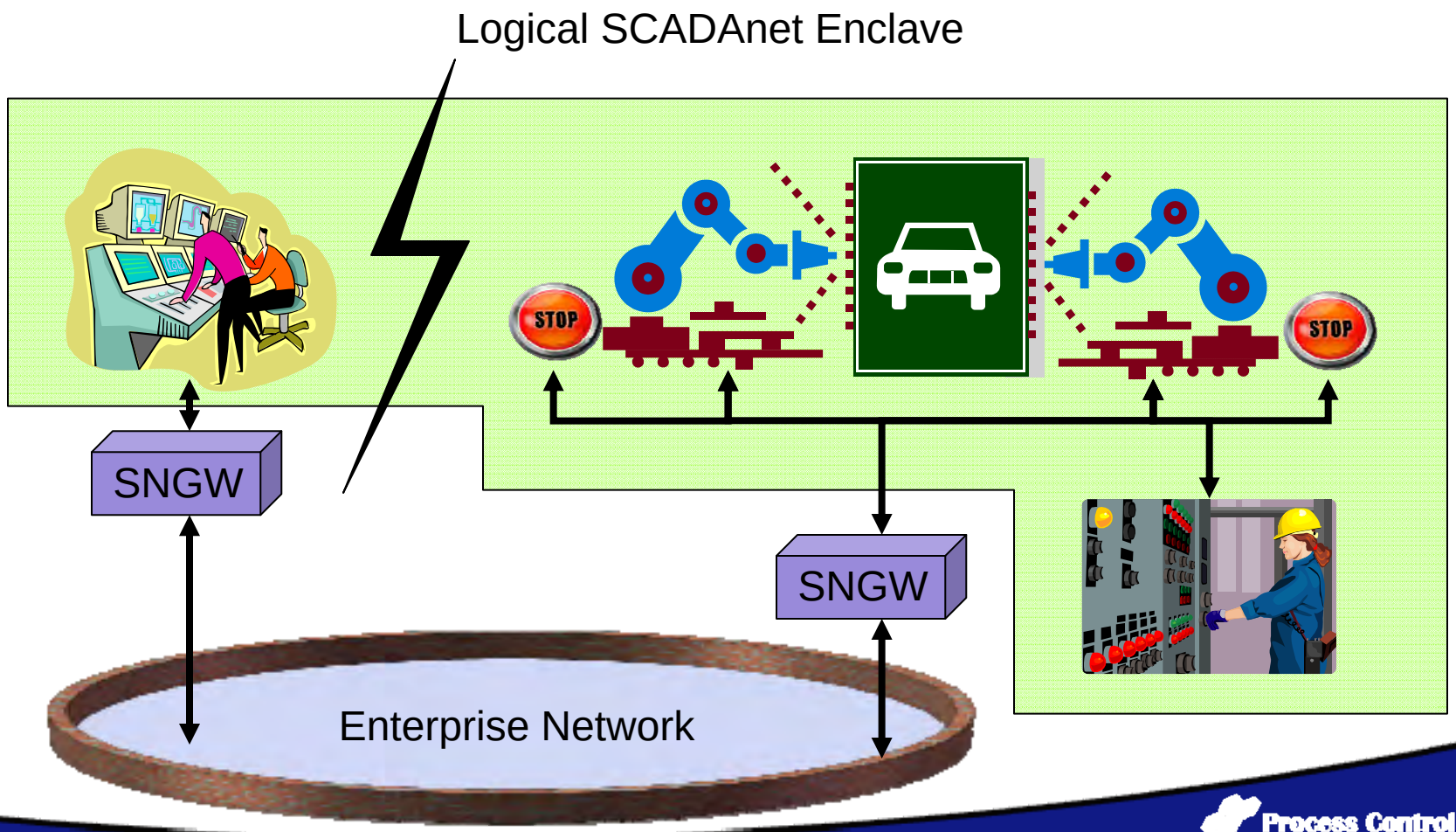
High-level SCADAnet Architecture



- Gateways contain SMA Implementation, including
  - Enterprise PKI Certificates
  - LAN and WLAN (WEP or WPA authentication)
  - Directory-based configuration and connection policy
- EN sees Gateways as standard wired/wireless clients
  - SCADA device traffic appears as encrypted IPSEC packets between Endboxes
- SCADA devices in a given enclave live on a private, isolated virtual network

Example: Local assembly cell with remote monitoring

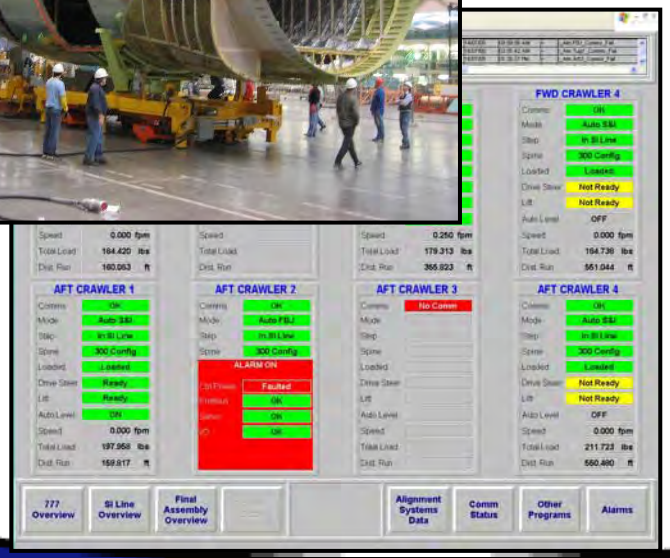
- **Hard real-time requirements use local connectivity**

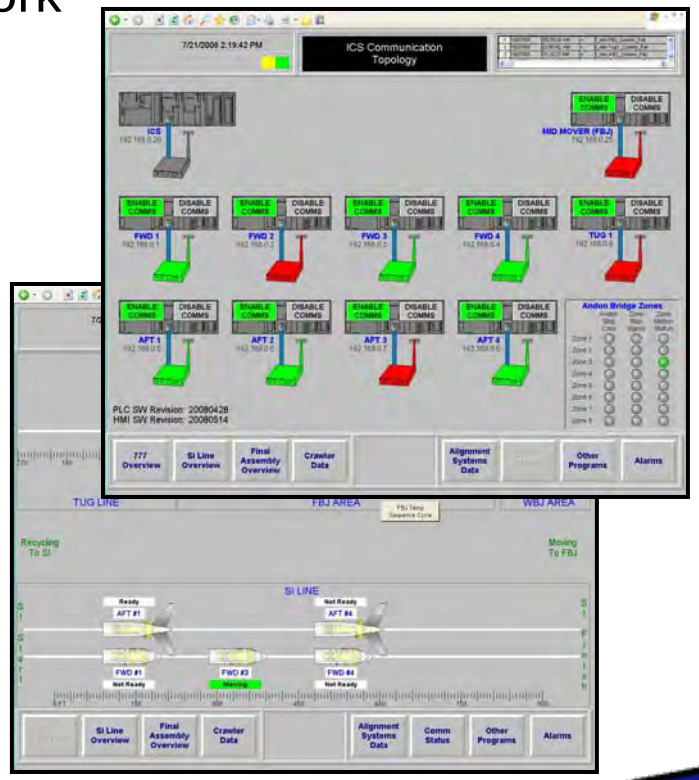


Internal Implementation Status

- **Using 777 F/A as a pilot program**
  - 9 “Crawlers”, F/A tug, Integrated Control System (ICS)
  - Using both wired & wireless LAN’s, Enterprise PKI
  - Enterprise directory interfaces in work

SNGW





Process Control Systems
Industry Conference

Legacy and Mobile Devices

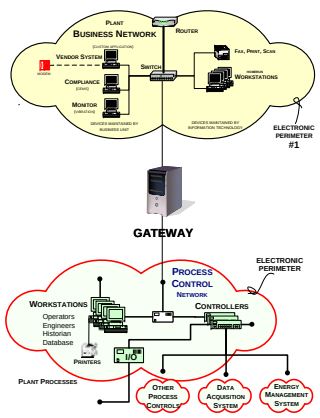
Larry Spoonemore
Southern Company

THE JOURNEY: The Evolution of Securing Process Control Networks

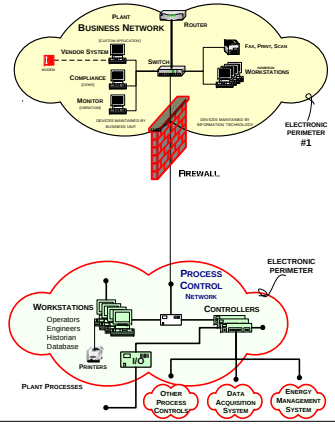
PAST PRESENT FUTURE

TIMELINE

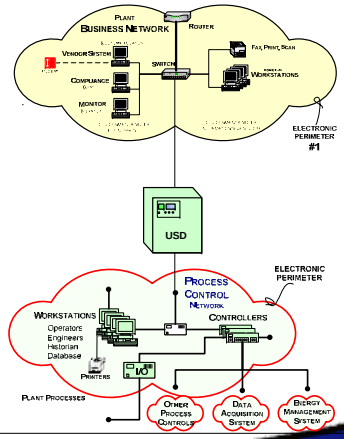
MINIMAL SECURITY:



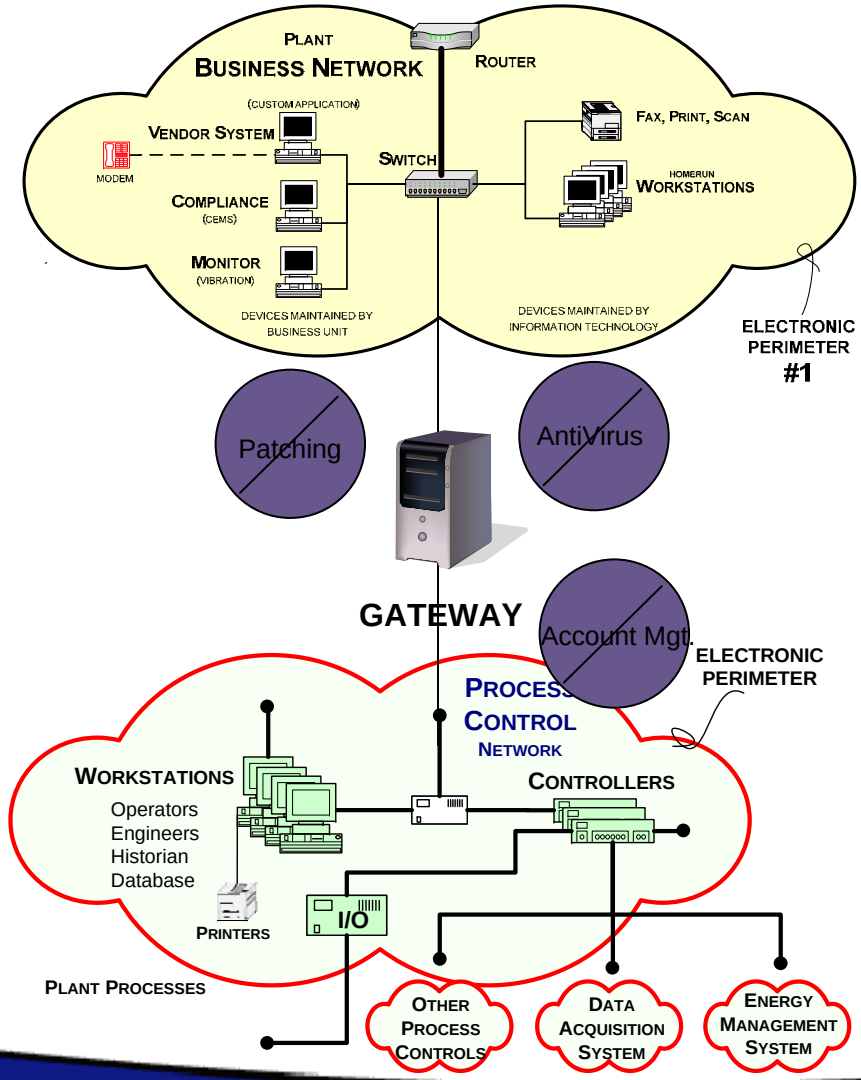
BETTER SECURITY:



IMPROVED SECURITY:



MINIMAL SECURITY



1 - Business To Control Network

2 – Gateways

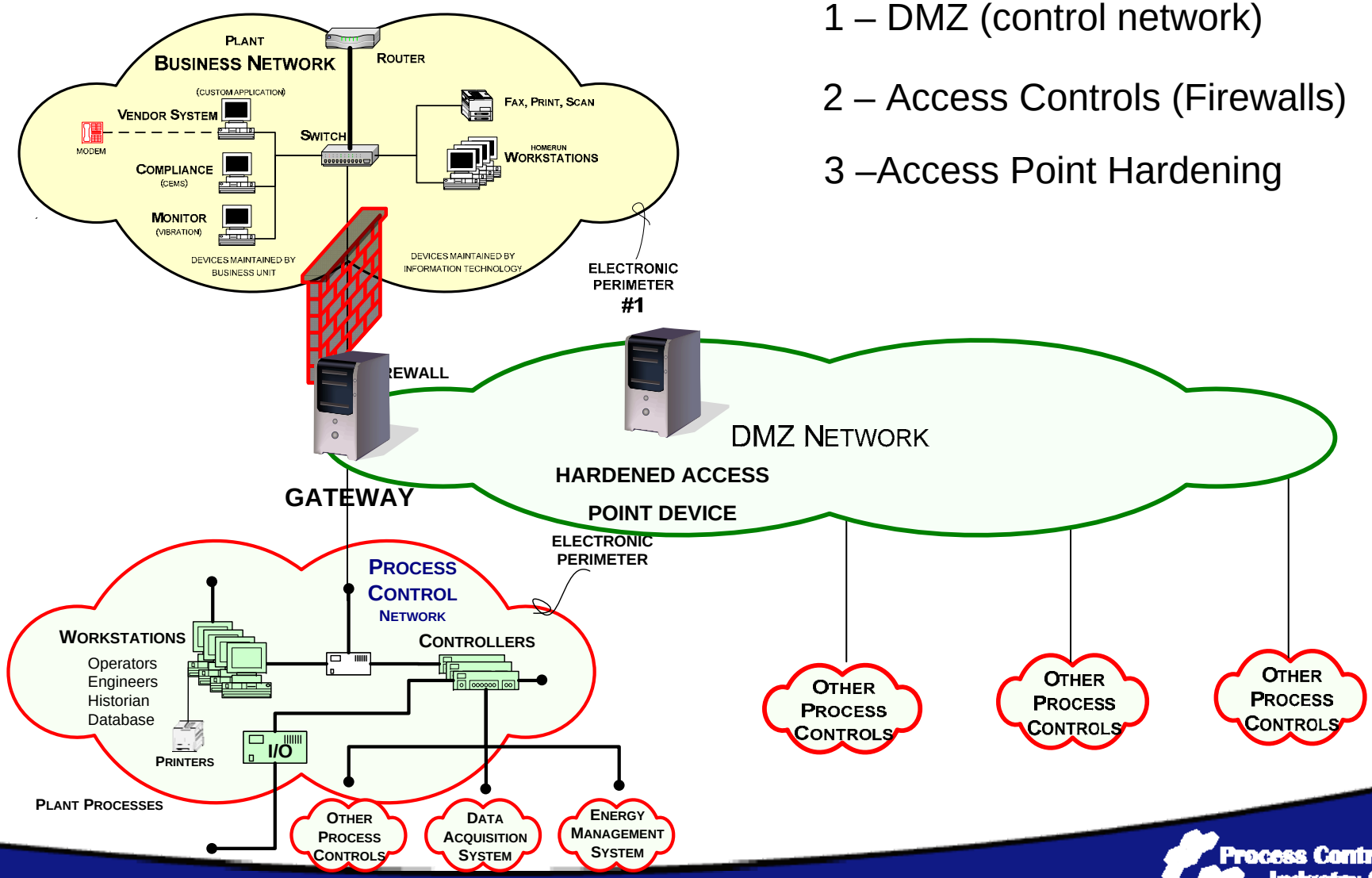
3 – Unmanaged devices/systems

BETTER SECURITY

1 – DMZ (control network)

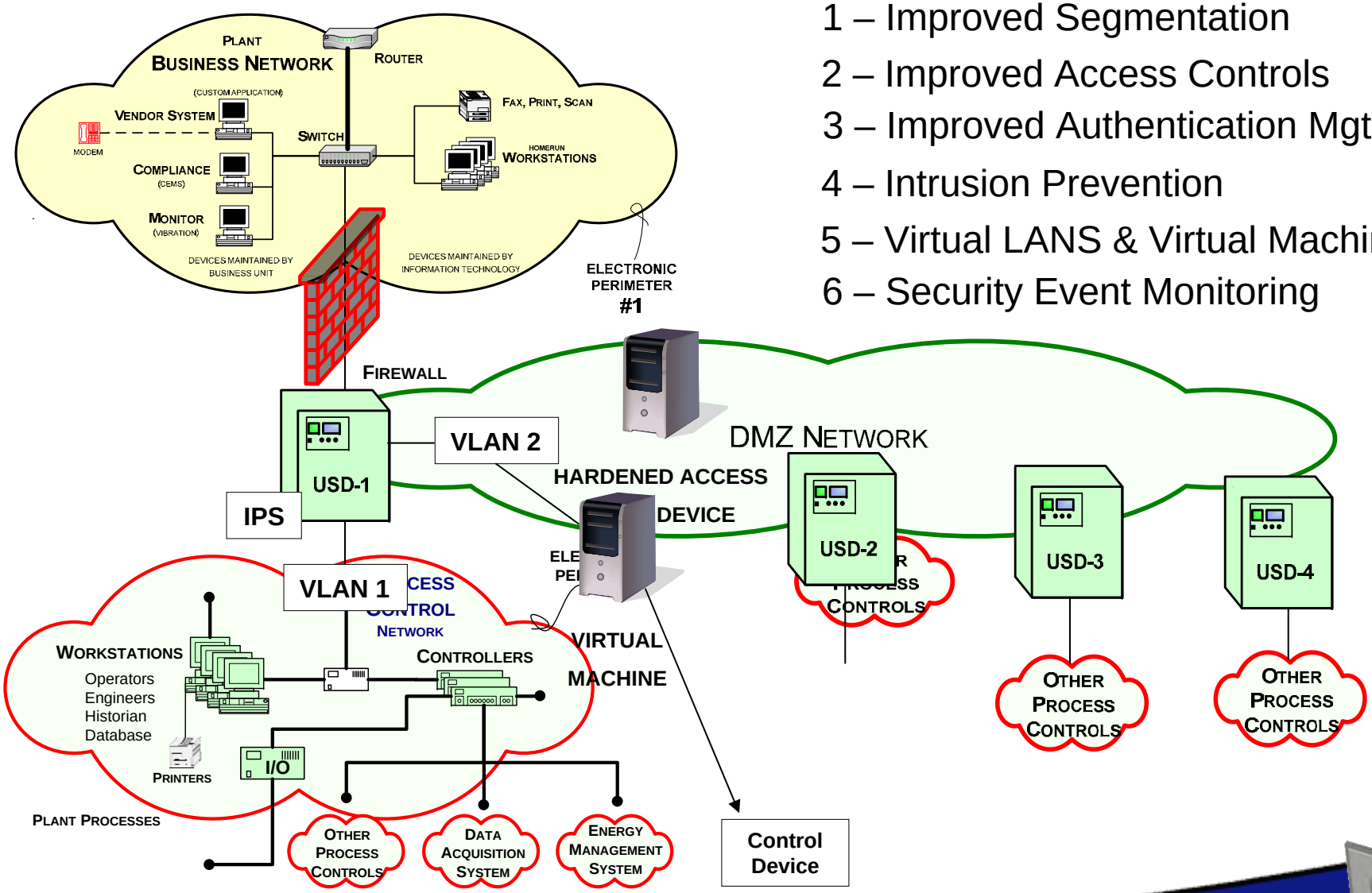
2 – Access Controls (Firewalls)

3 –Access Point Hardening



IMPROVED SECURITY

1 – Improved Segmentation
2 – Improved Access Controls
3 – Improved Authentication Mgt.
4 – Intrusion Prevention
5 – Virtual LANS & Virtual Machines
6 – Security Event Monitoring



THE JOURNEY: The Evolution of Securing Process Control Networks

PAST PRESENT FUTURE

What is the Message?

1. **Segmentation & Security-In-Depth** are good, but not enough
2. **Control Vendors**: Provide hardened systems with secure access
3. **Solution Providers**: Security management controls can not rely on know vulnerabilities
4. **Process Control Community**: Partner with control vendors, solution providers, and Government. To meet this challenge we must join forces.

Process Control Systems
Industry Conference

Legacy and Mobile Devices

Raphael Pereira
Chemtech

Legacy and Mobile Devices

- **Devices are very vulnerable to network attacks like spoofing, replay attacks, buffer overflow and other common attacks.**
  - How could we could restrict packages send to devices?
  - How could we protect the interception and changes on data send by devices to SCADA systems?
- **Devices requires a real-time networking.**
  - How this could be addressed in a TCP/IP networking?
  - And protocols like STP and rapid STP, Are you planning a new one to attend this requirements?
- **Its normal the use of RAS solutions with serial protocols and others to devices send messages to a communication server and than to SCADA.**
  - How could we address security to this communication?

Legacy and Mobile Devices

- **End-users (water sector and metals and mining) are using Wireless (GPRS, EDGE and 802.11) to take data from mobile equipments, to advance your technology and to remove serial campus communications.**
  - How could we address information security?
- **It's normal to find in field network old devices (20, 10 and 5 years old) integrated with new devices.**
  - How could we design the networking for this scenario?
- **MTU systems normally are older systems.**
  - How could we protect MTU Systems?
- **Scada devices normally don't have a strong authentication feature and this could permit an attacker to connect and change logics.**
  - How could we protect unauthorized access to SCADA devices networking?

Legacy and Mobile Devices

- **Are the weakest link of the control process**
  - Live in external areas
  - Use older protocols
  - Proprietary systems
- **Responsible for all field information collection**
  - SCADA and Engineer believes in information sent by devices
  - Devices information is correlated in Control systems
    - What could happen if someone intercept some of devices traffic and changes the values.
    - Is the control system identified that? And OCS? What could happen with the process?

Legacy and Mobile Devices

- - How could we could restrict packages send to devices? (Focus protect to spoofing, replay attacks, buffer overflow and other common attacks the devices may be unprotected)
- - Devices requires a real-time networking, with a expected behavior. How this could be addressed in a TCP/IP networking? And protocols like STP and rapid STP, Are you planning a new one to attend this requirements?
- - Its normal the use of RAS solutions with serial protocols and others to devices send messages to a communication server and than to SCADA. How could we address security to this communication?
- - End-users (water sector and metals and mining) are starting to use Wireless (GPRS, EDGE and 802.11) to mobile equipments and to substitute serial campus communications. How could we address information security?
- - Its normal to find in campus networking devices with 20, 10 and 5 years old integrated with new devices. How could we design the networking for this scenario?
- - How could we protect MTU Systems?
- - Scada devices normally don't have a strong authentication feature and this could permit an attacker to connect and change logics. How could we protect unauthorized access to SCADA devices networking?

Solution provider input - 20 minutes, 10 apiece

- **Technology Solutions**
  - **Serhii Konovalov Cisco**
  - **Steve Hargis Enterasys Networks**

Process Control Systems
Industry Conference

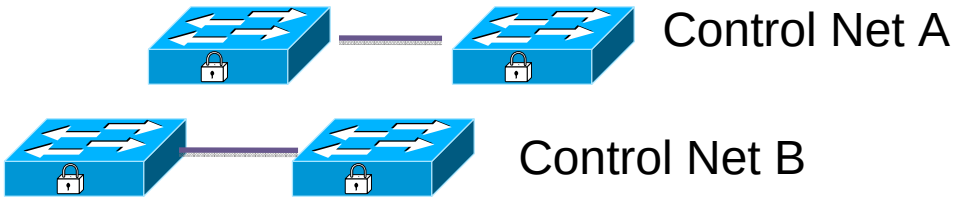
Industrial Network Design Panel Session

Network Solutions

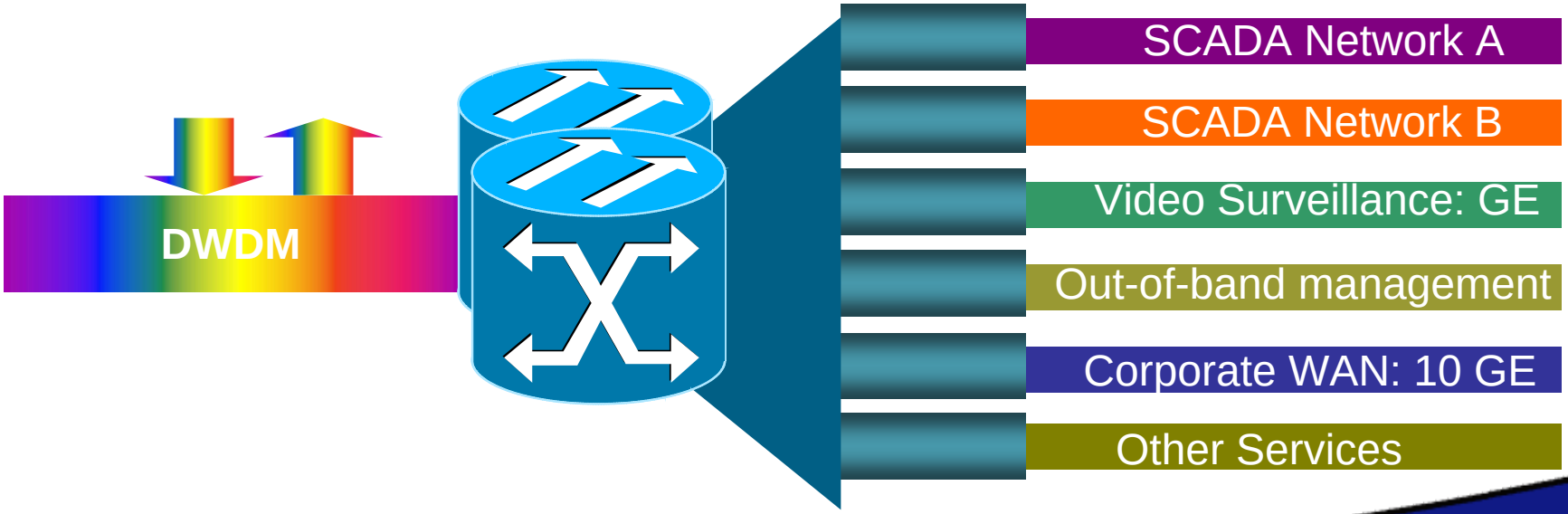
Serhii Konovalov
Cisco

Segmentation Type: Physical

- Physical

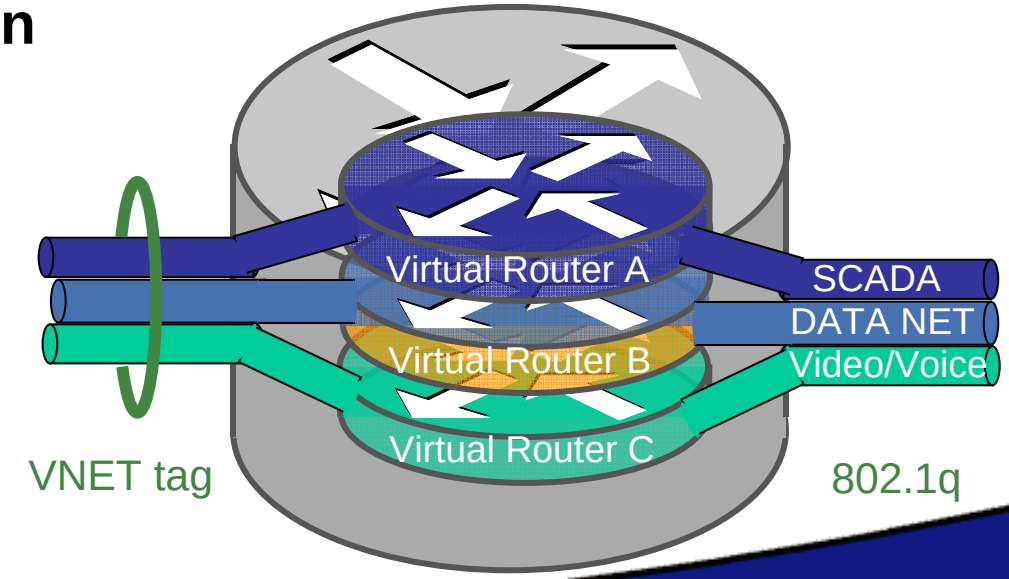


- PHY (DWDM, CWDM, SDH)

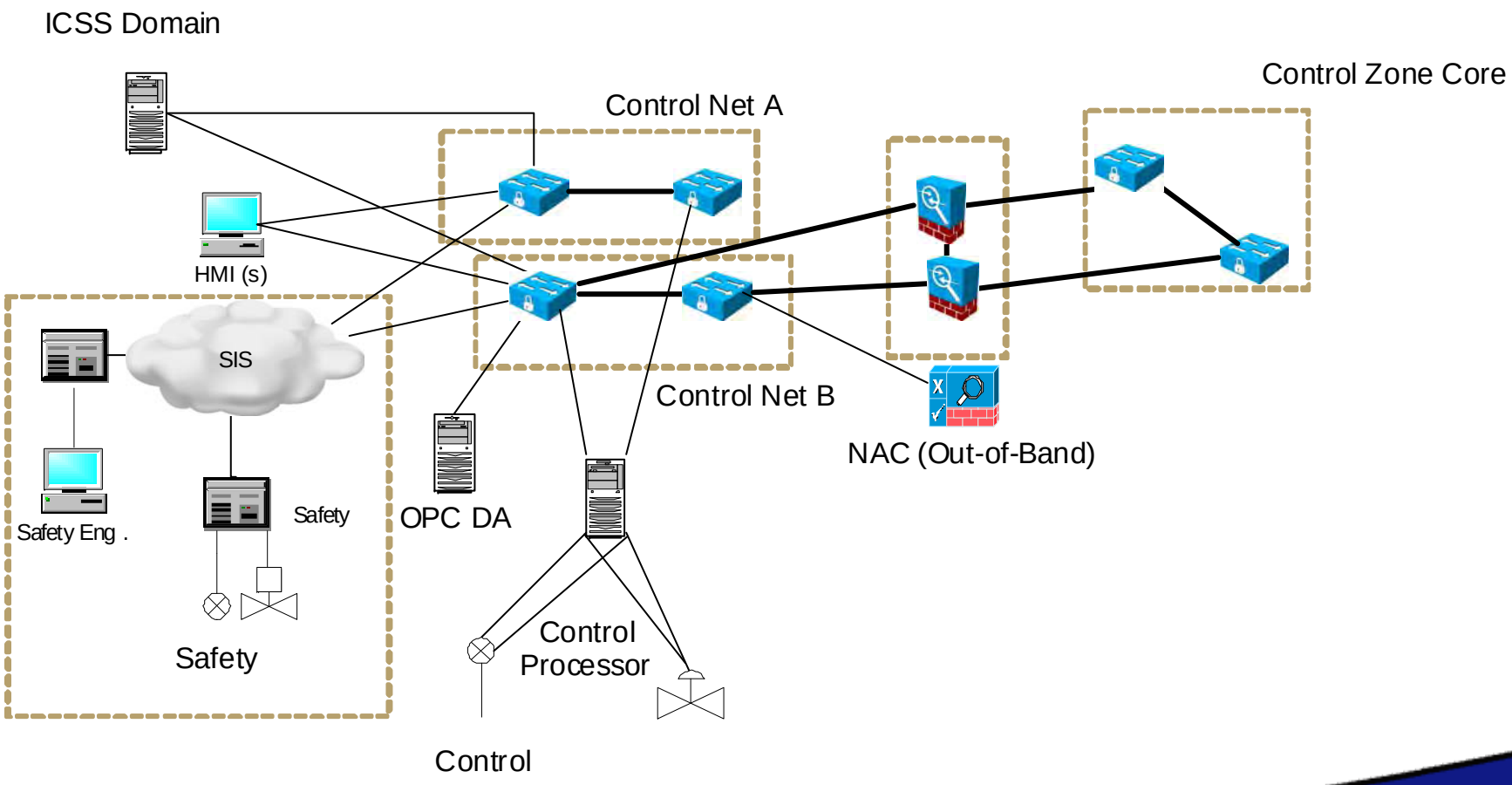


Segmentation type: Logical

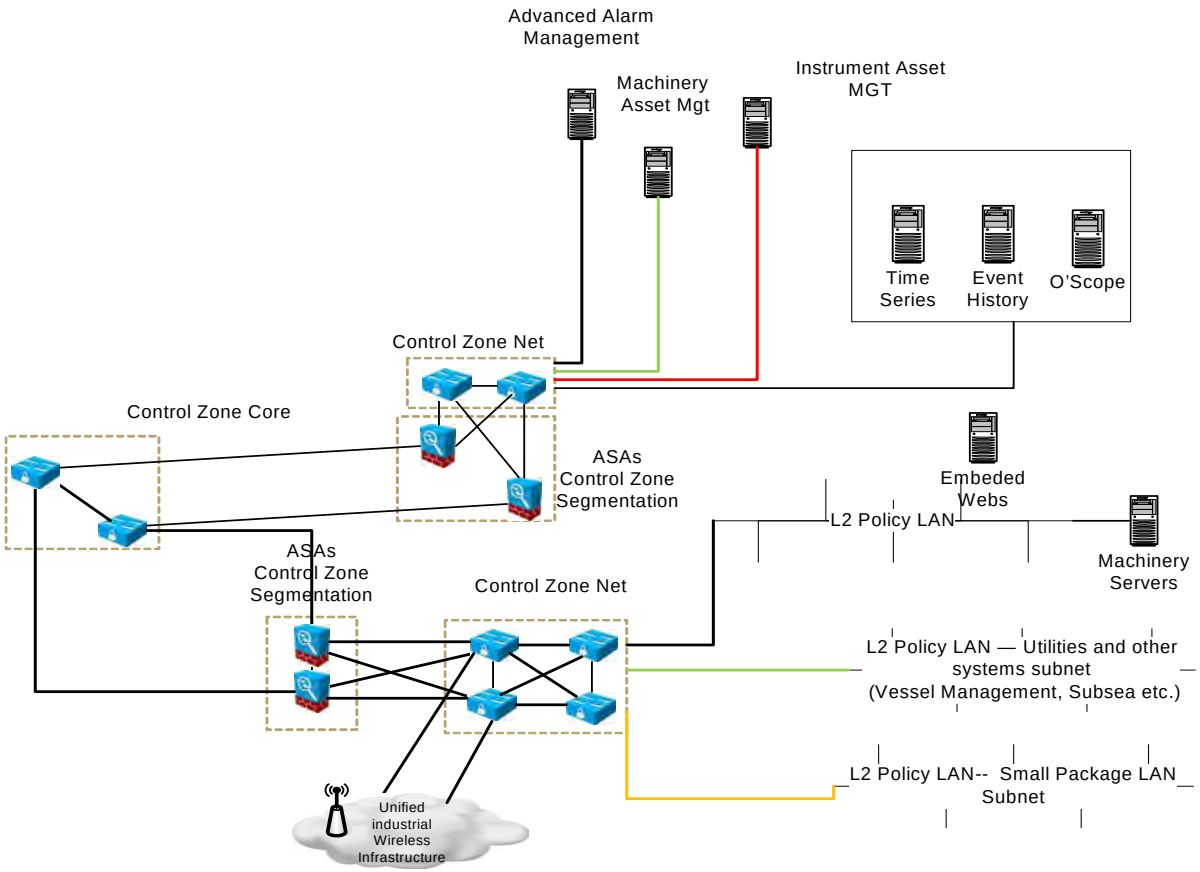
- **Layer 2: 802.1Q, VACL**
- **Layer 3: VRF-Lite (Virtualized Router)**
- **Security Services:**
  - Virtualized Firewalls/IPS/VPN Concentrators
- **Role-based segmentation**
- **Wireless: SSID, VLANs**



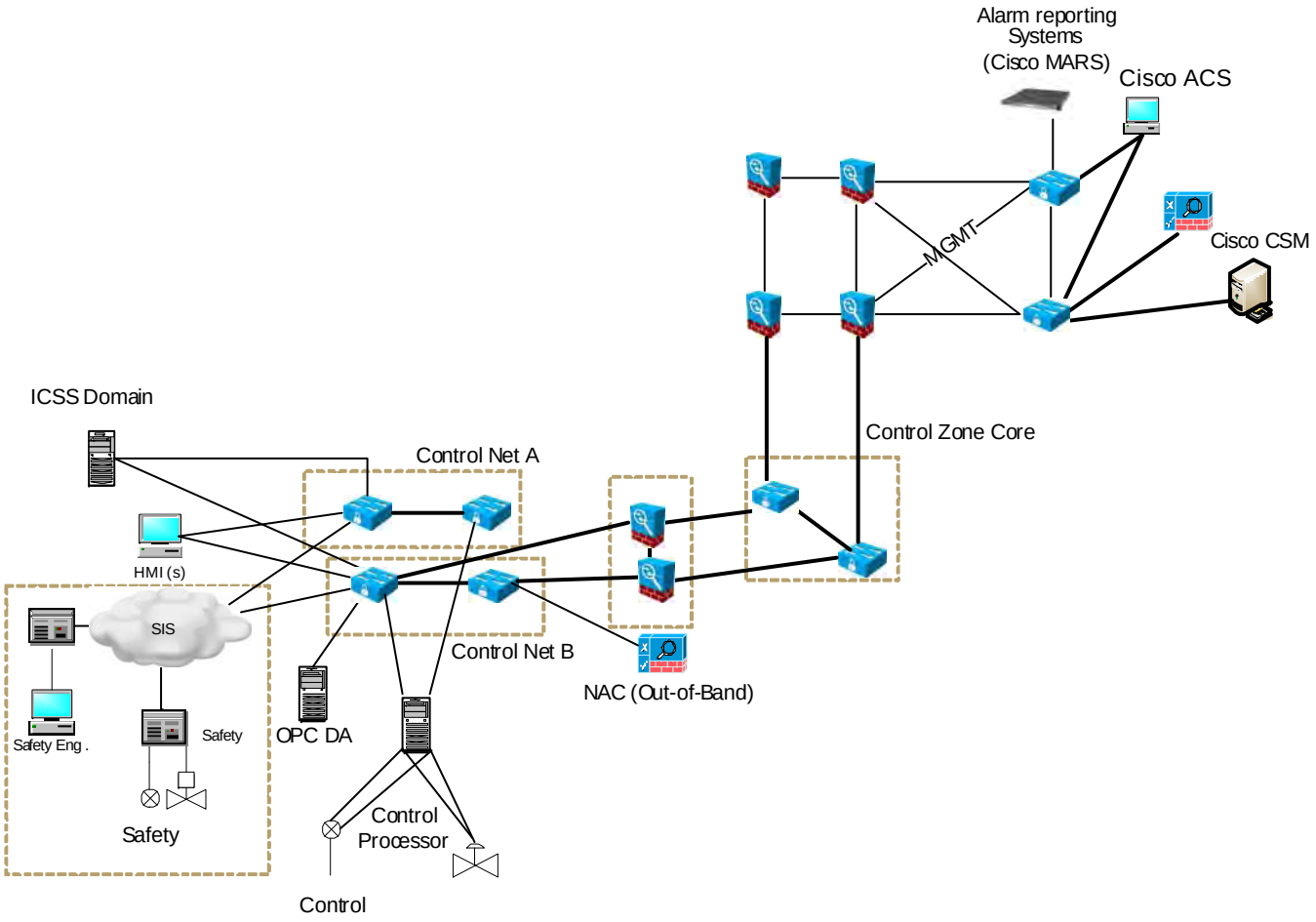
Physical Segmentation



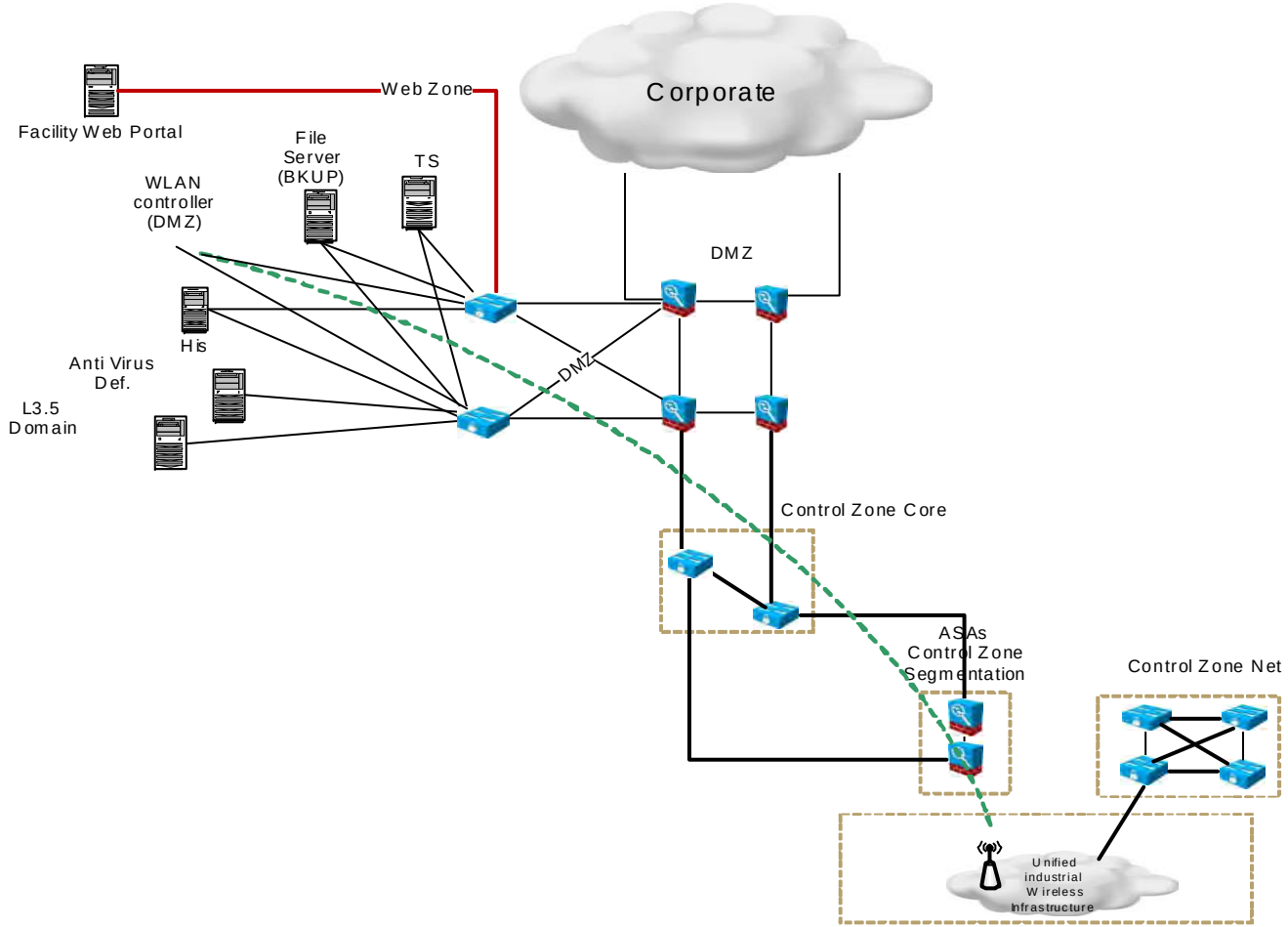
Logical Segmentation



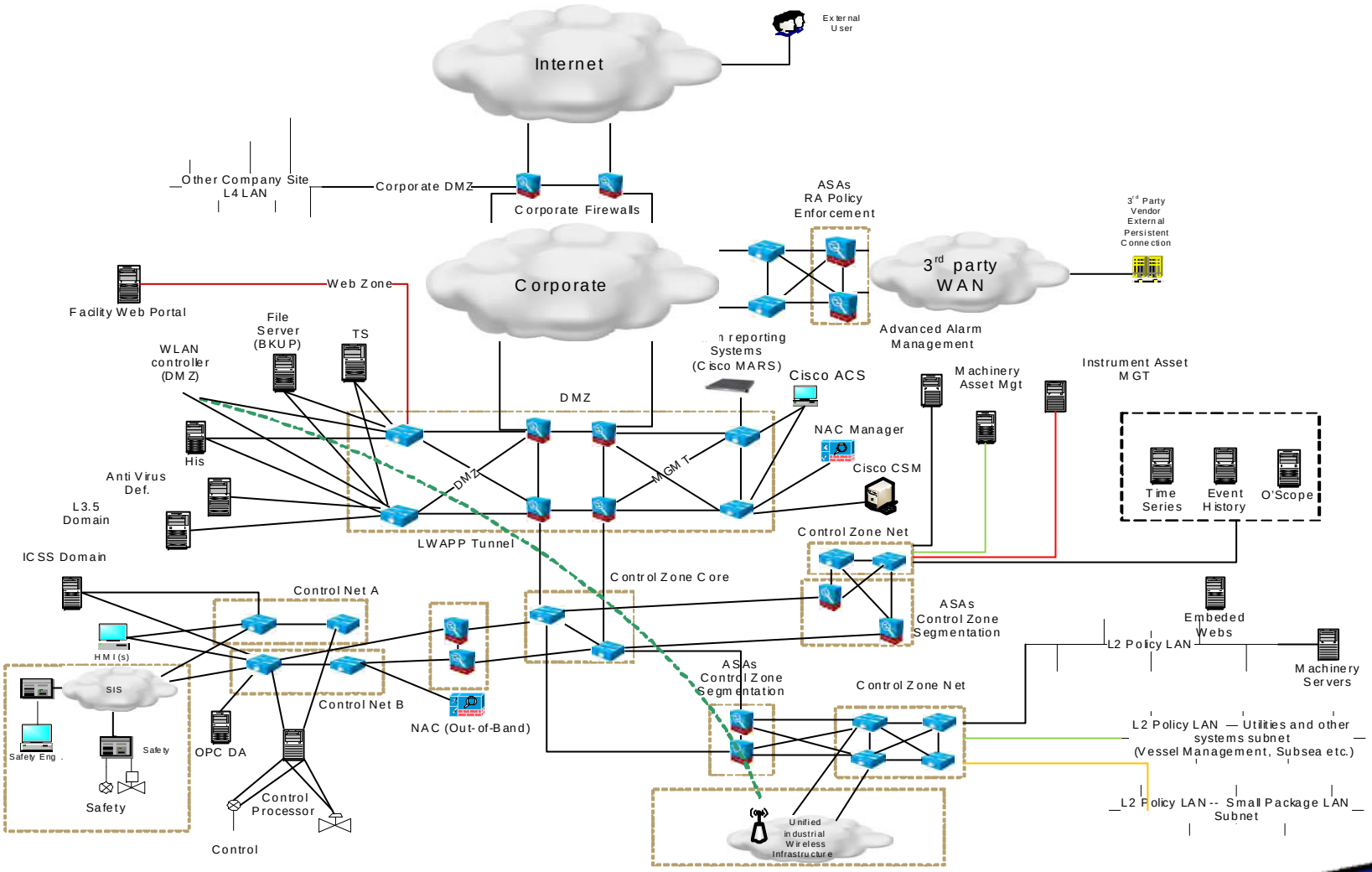
Role based Segmentation (NAC)



Wireless Segmentation



Putting it Together



Process Control Systems
Industry Conference

Industrial Network Design Panel Session

Network Segmentation

Steve Hargis

Enterasys Networks

A Policy-Based Network Maximizes Communications

- **The policy-enabled network understands context**
  - Who, want, where, when, etc.
  - This context can be used to allow or restrict communications in the network in a granular fashion
- **Segmentation is logical – and controlled from a centralized policy management console**
  - Maintains security with *boundaries* for communications – while leveraging a common physical infrastructure
- **Enables secure and deterministic communications!**
  - Business justified communications – process enablement.

Applying a Policy Framework to Process Control Networks

Device	Role	Services	Rules
Data Acquisition Server	Data Collection	Control and Safety Information Equipment Health System Historian	Allow Necessary Protocols - MOD/TCP Port 502 - SOAP/XML - Telnet - Binary Port 4840 Deny Unnecessary Protocols - HTTP - FTP - DHCP Port 546 & 547 - ICMP - IGMP - GVRP

Simple Administration is Paramount

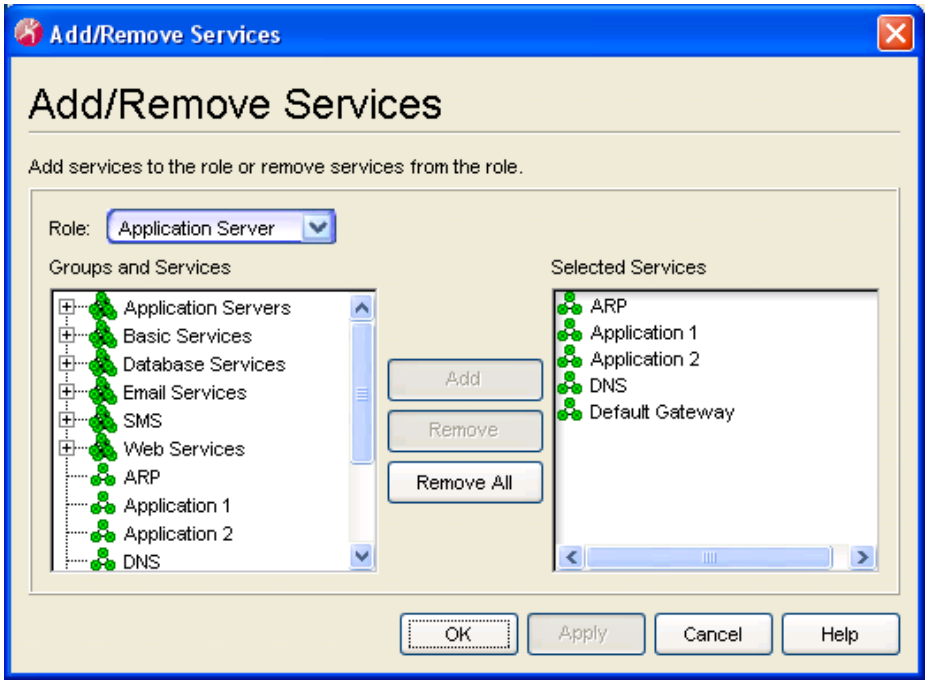
Non-Centralized / Complex Approach

```
!
ip nbar port-map custom-01 tcp 3389
ip nbar port-map dns_tcp tcp 53
ip nb
ip nb
ip nb
ip nb
ip nb
!
!
class
 matc
access-list 101 permit tcp any host 192.168.1.10 eq 80
access-list 101 permit tcp any host 192.168.1.10 eq 443
access-list 101 permit tcp any host 192.168.1.11 eq 21
access-list 101 deny ip any any
access-list 102 permit tcp host 192.168.1.10 any eq 80
access-list 102 permit tcp host 192.168.1.10 any eq 443
access-list 102 permit tcp host 192.168.1.11 any eq 21
access-list 102 permit tcp 192.168.1.0 0.0.0.255
 172.16.1.0 0.0.0.255 eq 22
access-list 102 deny ip any any
access-list 103 permit tcp 172.16.1.0 0.0.0.255
access-list 101 permit tcp any host 192.168.1.2.11 10 eq 80
access-list 101 permit tcp any host 192.168.1 10 2.11 eq 443
access-list 101 permit tcp any host 192.168.1.2.13 11 eq 21
access-list 101 deny ip any any
access-list 102 permit tcp host 192.168.1 10 2.11 any eq 80
access-list 102 permit tcp host 192.168.1.10 1.11 any eq 443
access-list 102 permit tcp host 192.168.1.11 any eq 21
access-list 102 permit tcp 192.168.1.0 10 0.0.0.1 255
 172.16.1.0 0.0.0.255 eq 22
access-list 102 deny ip any any
access-list 103 permit tcp host 192.168.2.13 any eq 21
access-list 103 permit tcp 172.16.1.0 192.168.1.12 0.0.0.1
 172.16.1.0 0.0.0.255 eq 22 0.0.0.255 192.168.0.0
 0.0.255.255 eq 22
access-list 103 deny ip any any
access-list 104 permit tcp 172.16.1.0 0.0.0.255
 192.168.0.0 0.0.255.255 eq 22
access-list 104 deny ip any any
  set dscp af12
  priority percent 25
!
```

X *n* switches

Hours to deploy!

Centralized / Intelligent Management Approach



System wide

Seconds to deploy!

Pervasive Policy Enforcement

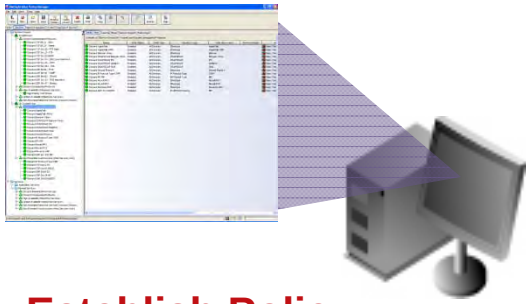
Network Policies

"MOD/TCP and OPC Protocols are mission critical communications."

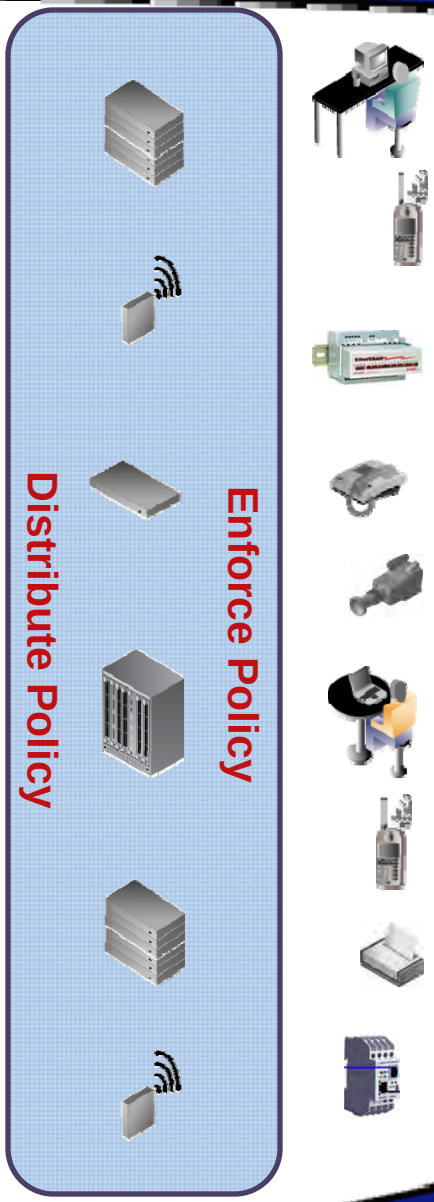
"A user or device must not use up too much bandwidth."

"A typical end system should never be a DHCP server."

"Only IT administrators should configure infrastructure components."

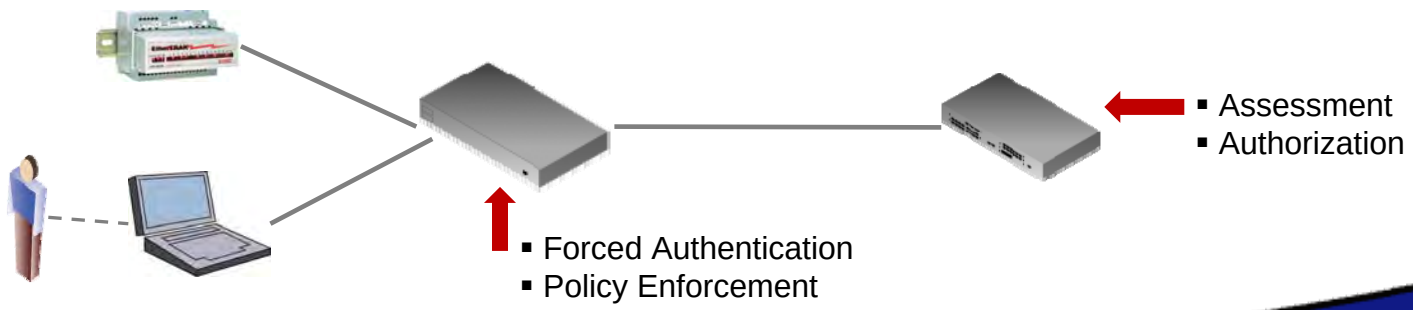


Establish Policy

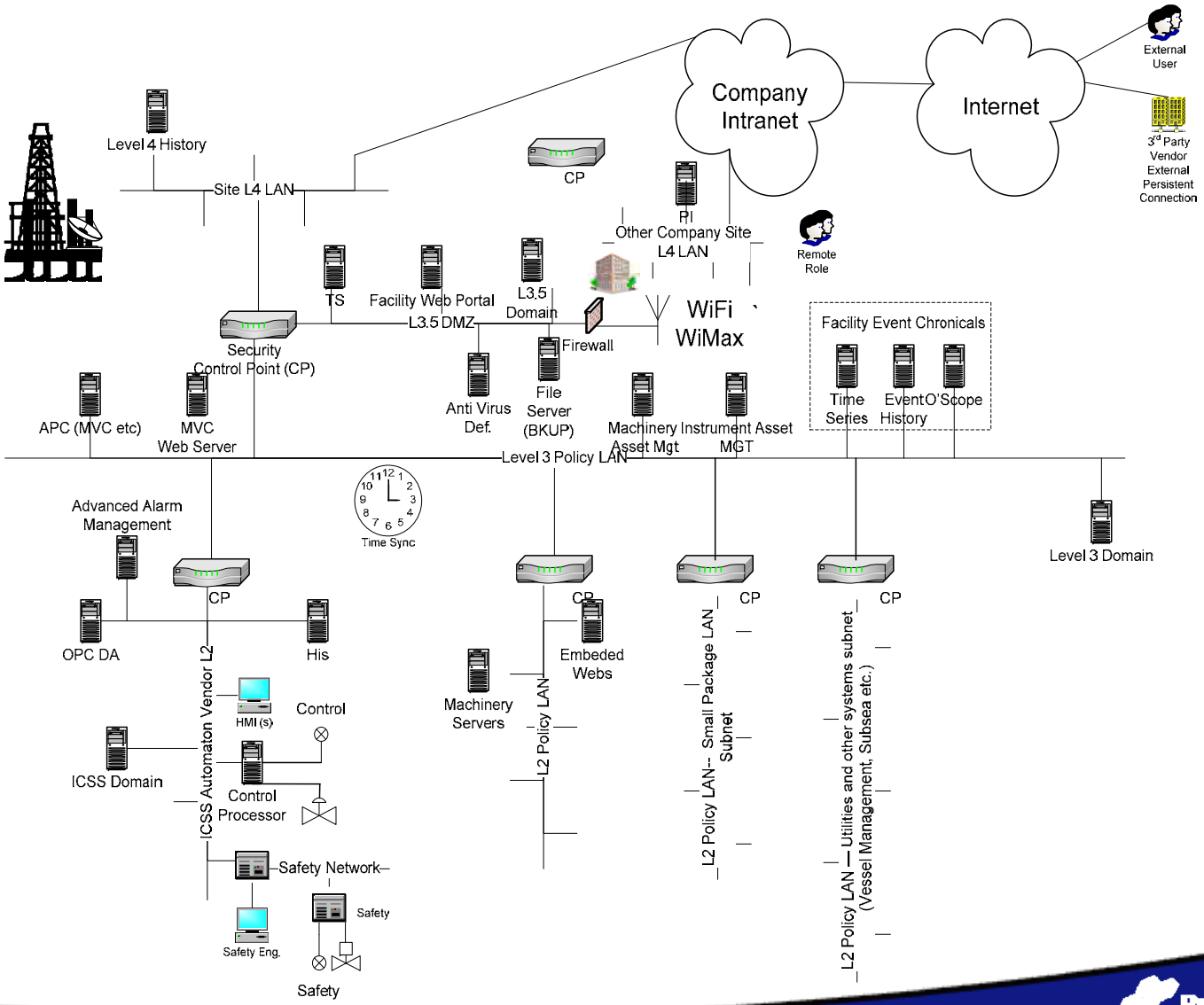


End System Based – Dynamic Enforcement

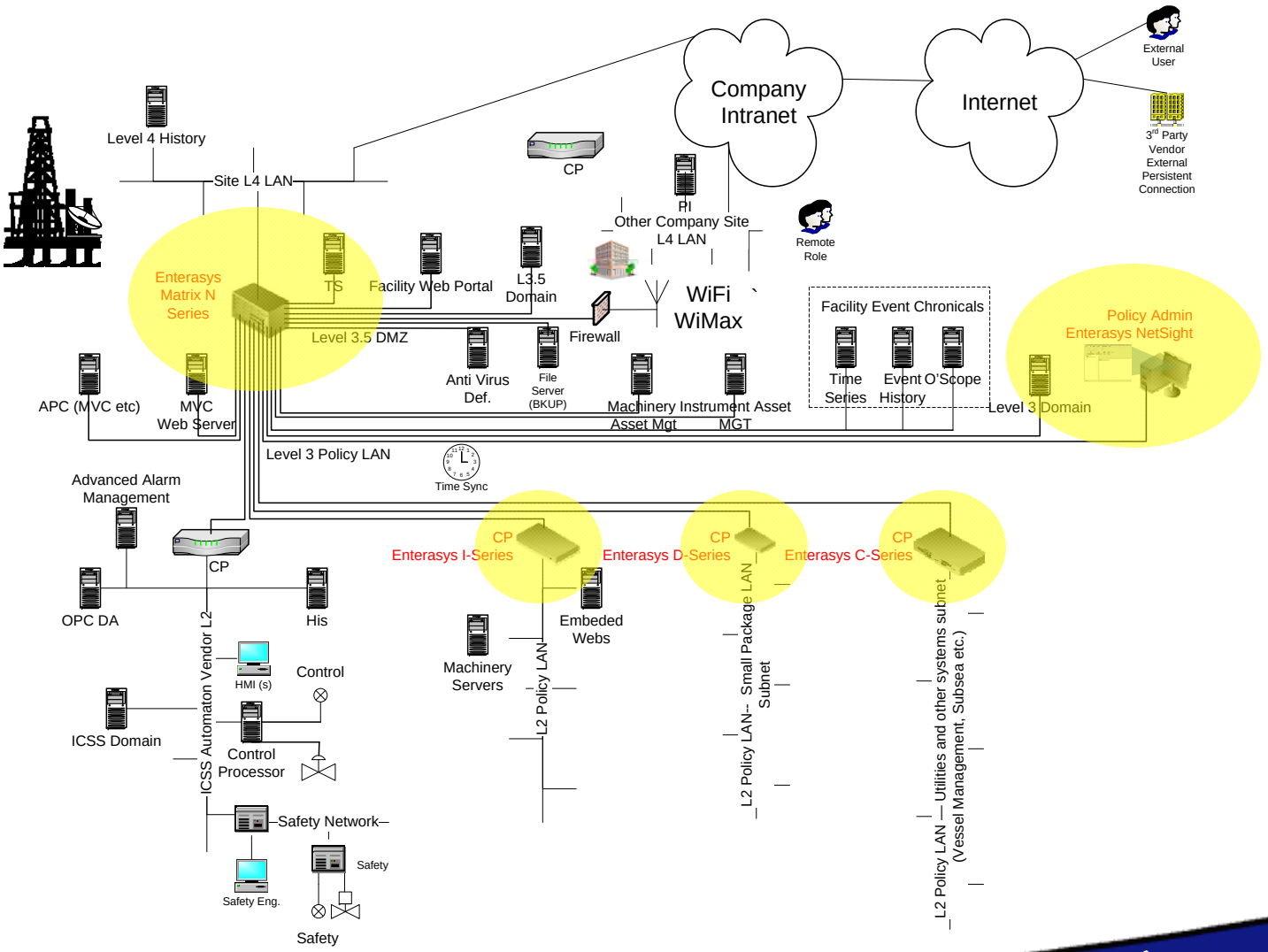
- **What is the type of device attempting to communicate on the network?**
  - MAC-Based Authentication
  - OUI Mask Association
  - Endpoint Detection (CDP, LLDP, LLDP-MED, SIP)
- **Who (if anyone) is using the device?**
  - Web-Based Authentication
  - 802.1X Authentication (Digital Certificates, Biometrics, etc.)
- **Based on the context of device type and user, what communications should be allowed?**
  - Enforced dynamically at the point and time of connection



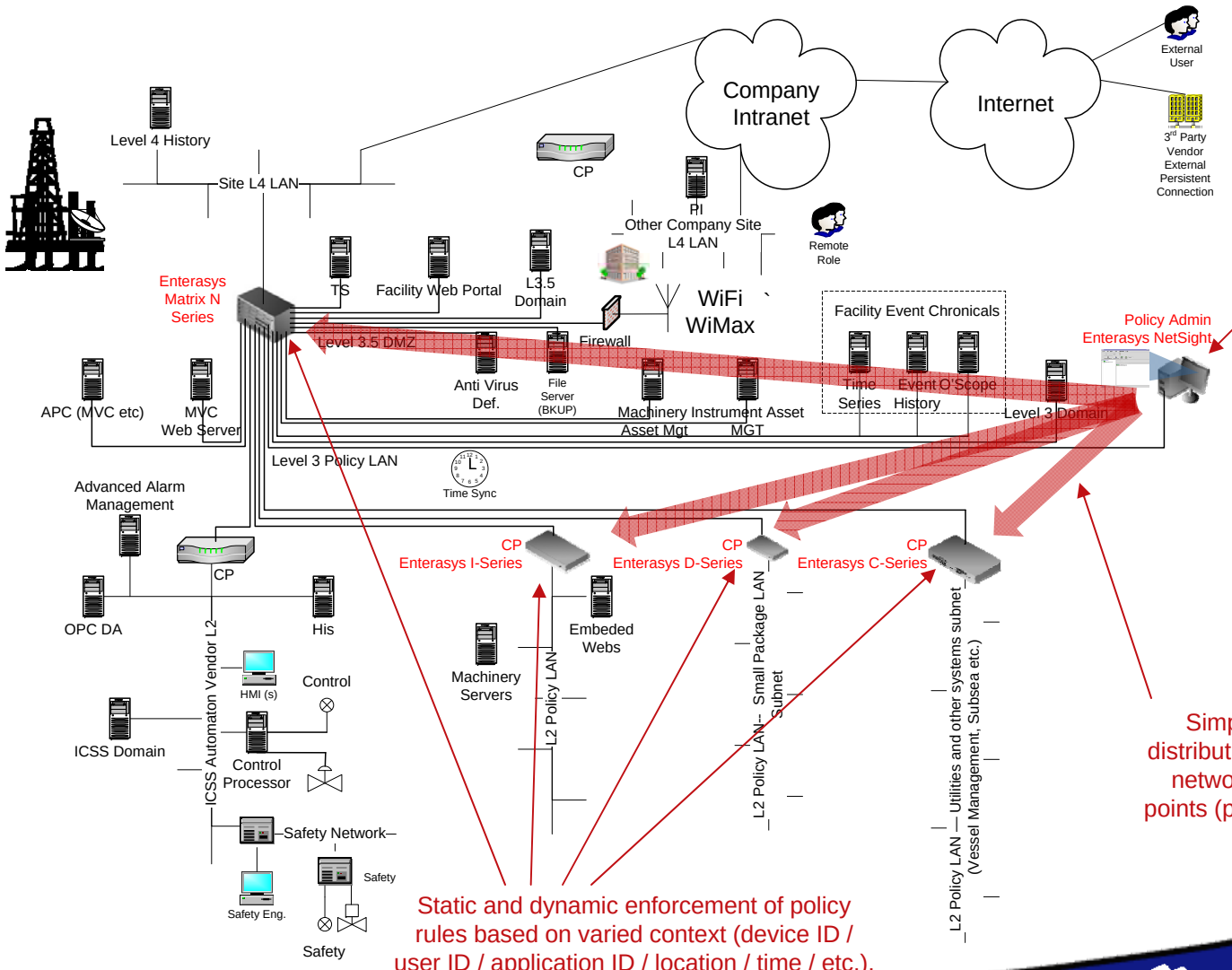
Upstream Facility Control Systems Design



Upstream Facility Control Systems Design



Upstream Facility Control Systems Design

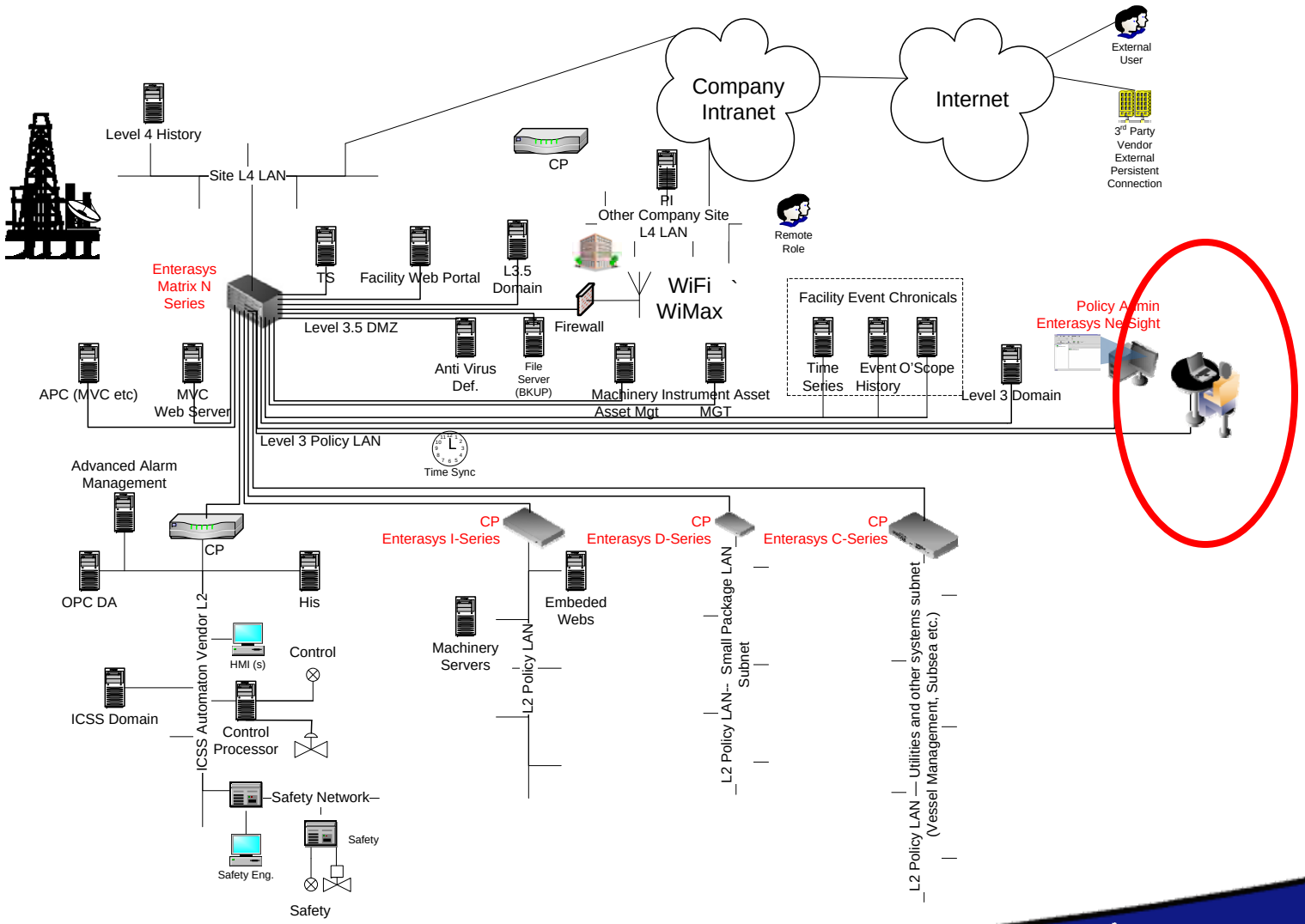


Centralized GUI management application for total network visibility and role-based policy profile configuration.

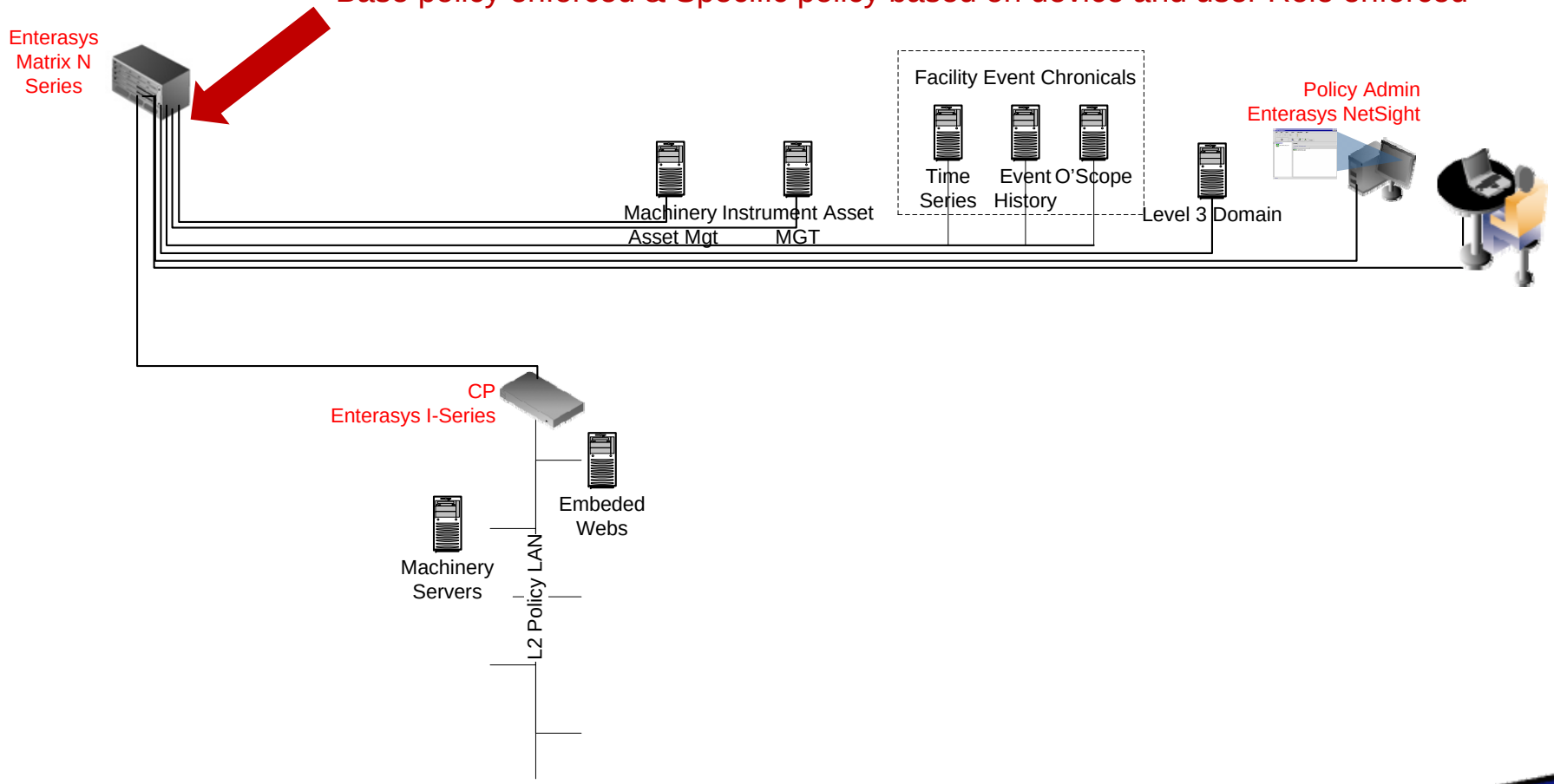
Simple (click of a button) distribution of policy profile to all network policy enforcement points (policy-enabled switches).

Static and dynamic enforcement of policy rules based on varied context (device ID / user ID / application ID / location / time / etc.).

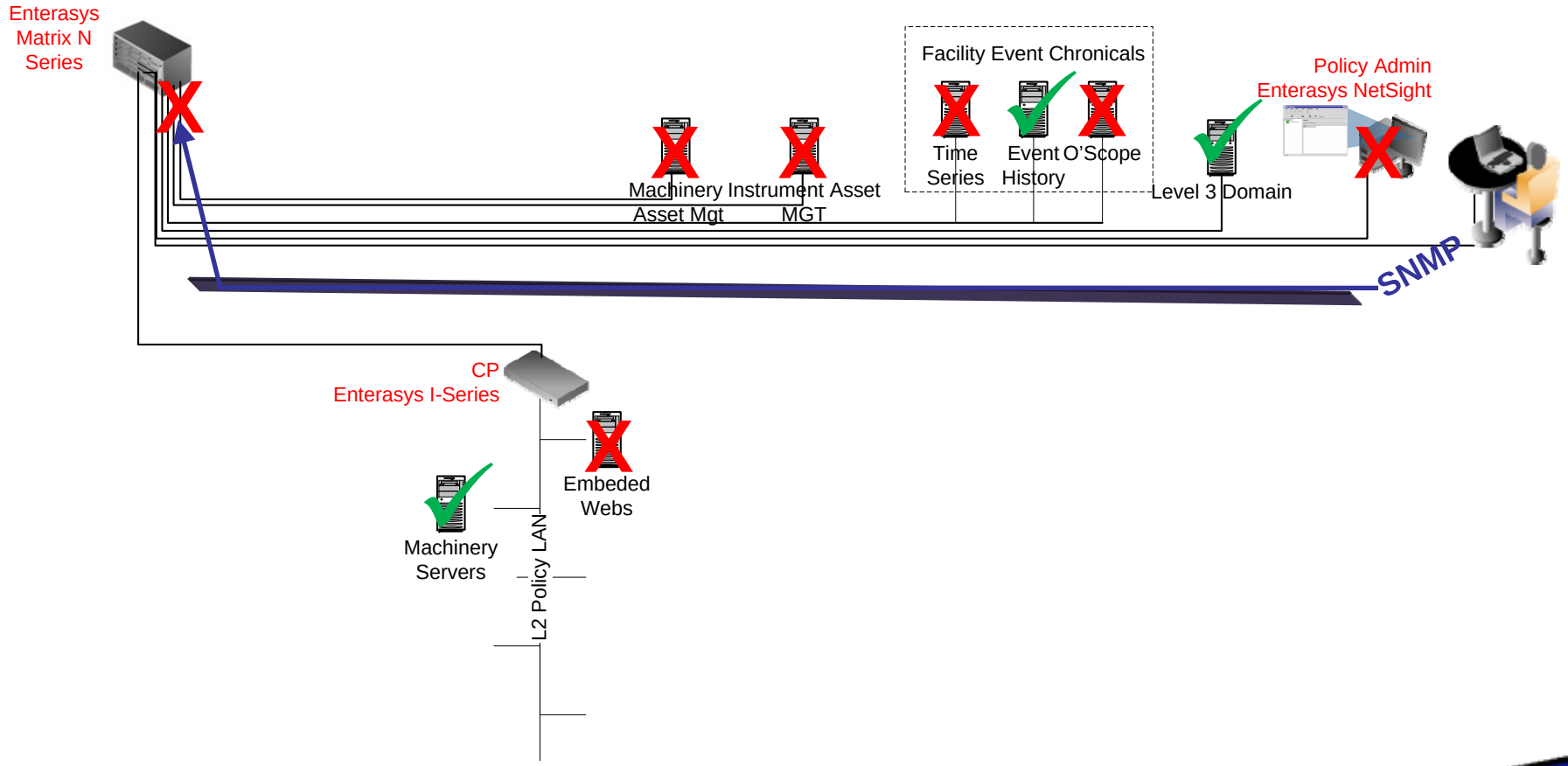
Upstream Facility Control Systems Design

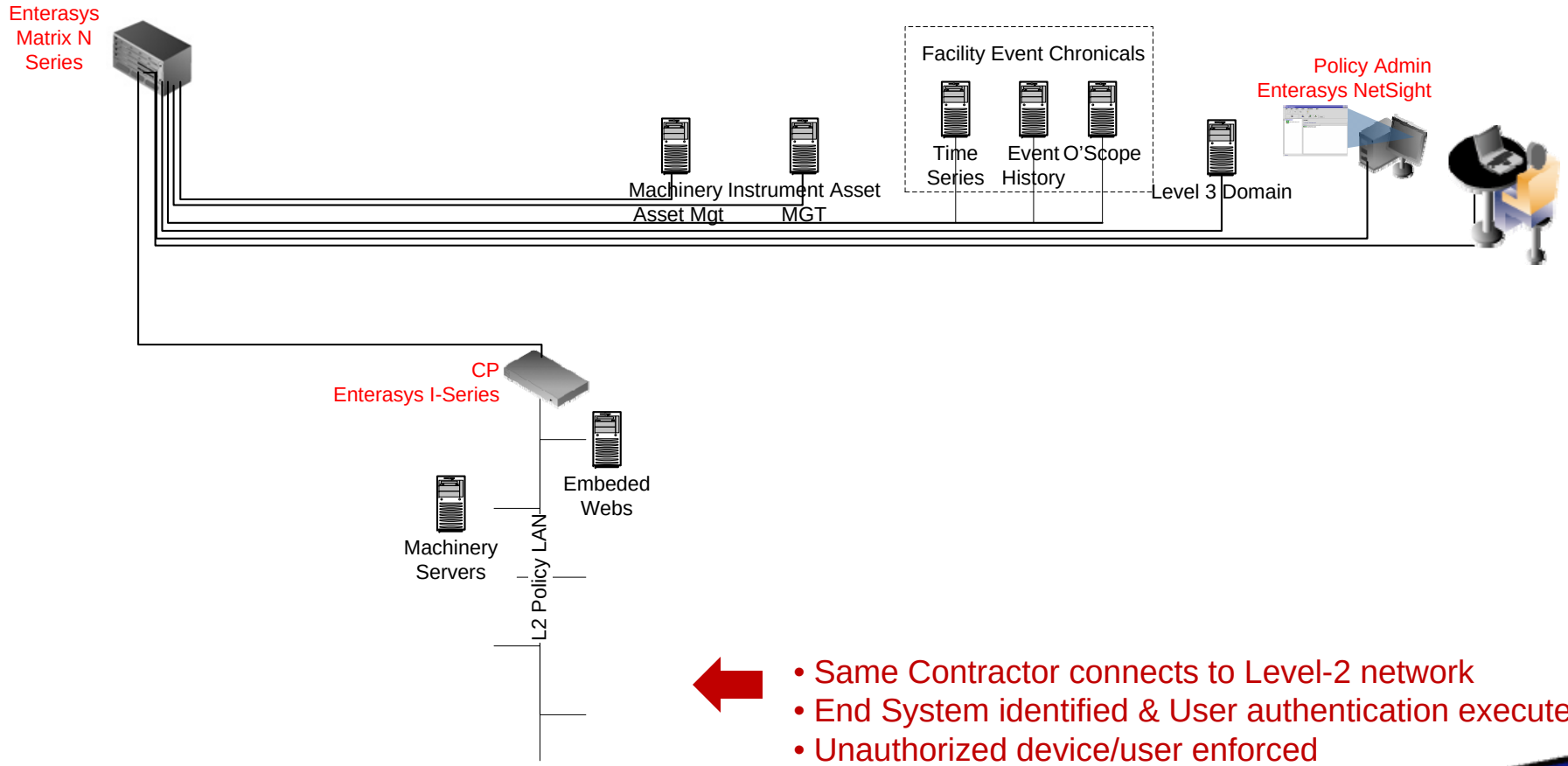


- Contractor connects to Level-3 network
- End System identified & User authentication executed
- Base policy enforced & Specific policy based on device and user Role enforced



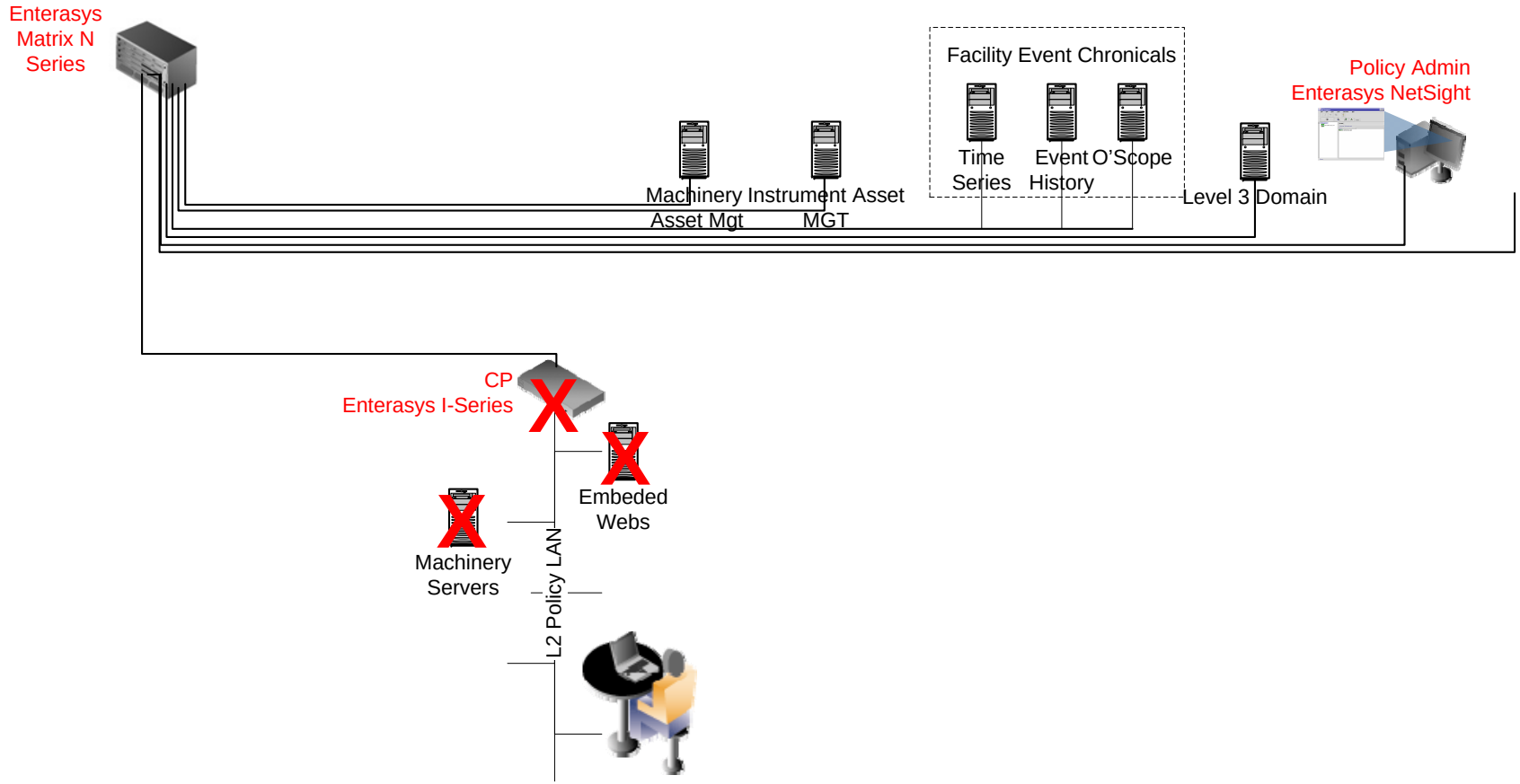
Contractor can only communicate to appropriate services and cannot introduce unauthorized traffic onto the network!





- Same Contractor connects to Level-2 network
- End System identified & User authentication executed
- Unauthorized device/user enforced

Contractor and device type is not allowed on the Layer-2 network and all traffic is filtered at the network point of connection!



Enterasys Summary

- **Modern process control networks should be policy-enabled**
  - Physical continuity allows for robust communication options – to fully enable emerging process systems
  - Logical segmentation – *through communication policy enforcement* – maintains comprehensive security of critical systems
- **Network infrastructure intelligence and centralized / simple to use administration is critical to success**
- **More detailed information in the PCSF Design Challenge Whitepaper**
- **Thank You!**

A Call to Cross "Sector" Action

- **We the Process Control End-Users can be part of the problem or part of the solution to Secure Industrial Networks**
  - Secure Networks are cross "Sector" and are growing to be **the most** significant and powerful control system and device network infrastructure on the planet
  - All field bus wars end at Ethernet!
  - It is imperative that asset owners work with our industrial secure network suppliers and automation companies to demand use of open standards to increase device & control systems security integrity
- **We can't rely on the automation suppliers to be in the secure network business because they can't be everything to everybody**
- **This is a call to action and we need all "sectors" to collaborate on a common set of End-User open standards based requirements**
- **Secure Network providers working with End-User & automation companies can provide secure solutions to address cross "Sector" asset owners' business requirements**
- **On behalf of our panel, Thank You!**

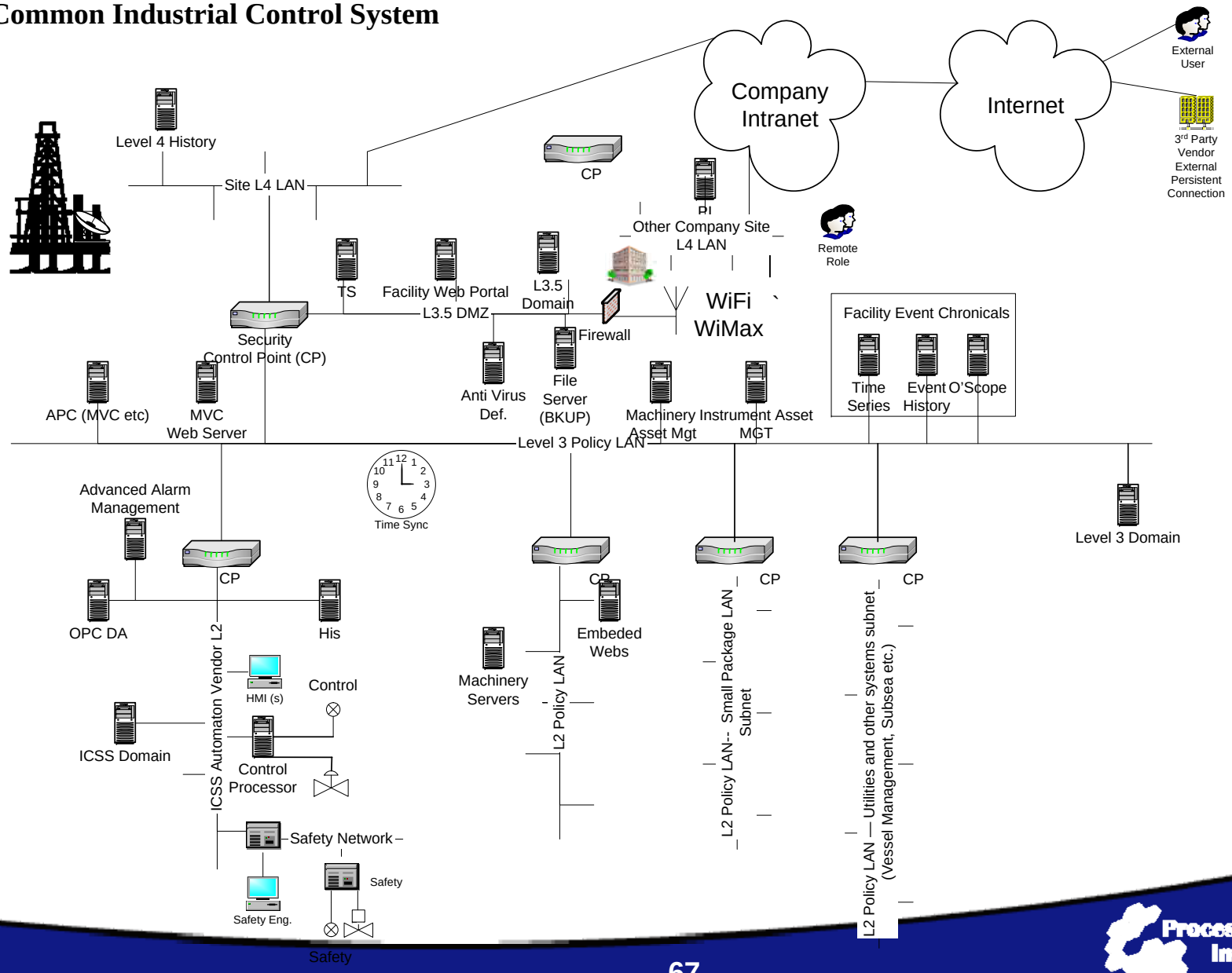
Industry Network Design
Panel Session

Additional Information

Baseline Design Challenge Objectives

- Industrial network design is policy based with only business justified communications allowed. No traffic other than that required to execute the mission.
- Any computer can connect to the network (service company PCs) that is not controlled by the facility operator. They must be remediated and limited to a group of devices and computer(s) the service company PC access.
- Security admin must be easy to administer although a security design admin sets up policy that the admin administers to maintain the site. Graphical management is strongly desired.
- RADIUS and or Active Directory including domains must be addressed by the design
- Central remote site executes the security admin designs local administration within business policy to allow site control within acceptable use policies

Reference Architecture:
Common Industrial Control System



Potential Discussion Topics:

Source: PCS Forum IND Discussion Board

"Layers of protection"

- How can industrial network design contribute as a "layer of protection" to control systems recognizing control devices have demands and lifecycles that are different from common IT technology and refresh cycles?
- What role can diversity plan in secure networks?
- What role can network segregation play? Logical vs. Physical?
- Use of IPS, vulnerability scanners, etc to protect and monitor industry networks

Legacy System protection

- What can we do in the near future to address present and legacy systems as we wait for security "built in" and "not bolted on" or provided by external "appliances"?

Open Security Standards

- How would extending IETF RFCs approach to address control systems security standards benefit industry (Users and vendors) by avoiding proprietary solutions
- How does industry leverage, extend or supporting existing Industrial network protocols like DNP, Modbus, etc. Where are they?
- NAP

Lifecycle Support and Service

- How can we improve vendor patch behavior ?
- How can we improve the interoperability and application of domain controllers and access domains for patch, anti-virus, time sync, access control lists, network & system inventory, equipment health monitoring, IDS, etc.

Potential Discussion Topics:

Source: PCS Forum IND Discussion Board

Local, Remote and External/3rd Party Access Control

- How can we accommodate vendor service laptops coming and going from our networks securely?
- How can we accomplish agent less remediation of laptop systems from many of our service vendors?
- What role can VPN and terminal services play in a secure control system architecture?
- Wireless network protection
- What does network access control really mean in process control networks?
- What are typical compliance guidelines/mandates for end system access and communications in the process control network environment?

Authentication and Authorization

- How can we identify / authorize devices that do not support 802.1X and have them conform to acceptable use electronic policies?
- How can we prevent unauthorized services from establishing themselves in our control system networks?
- What detection, response and remediation methodologies are important for machine centric and human centric end systems connecting to the process control network environment?

System Availability

- Upon network device failure, what technologies exist to allow rapid component replacement without advanced knowledge of network engineering to recover from system failures?
- Auto discovery of services in use on the network and sub networks?
- What detection, response and remediation methodologies are important for machine centric and human centric end systems connecting to the process control network environment?