

Creating a Secure Zone for Control System Data Communications

PCSF 2007 Annual Meeting

Clayton L. Coleman, Invensys
James Bassett, Capgemini Energy



Invensys[®]
Process Systems

Get More from One
Avantis • Foxboro • SimSci-Esscor • Triconex

Objectives

- Understand today's connectivity between the control system and business or plant information networks
- Recognize the need for tighter access controls to protect both the control system and business assets
- Define DMZ, understand it's usage.
- Understand Invensys' solution to address the changing needs to protect the transfer of information between control system and business networks

Today's Environment

- Control systems are connected to the business network via a “second Ethernet” or “admin network”
- Most of these connections grew out of convenience and were not driven by the needs of the business
 - Eventually the need was recognized by the business and these early connections were put to business or enterprise IT-use
- Often, the connection is made by plugging one port of a control station into a switch or hub connected to the business network
- Sometimes a router or firewall is used to control access
- These devices are sometimes managed by corporate IT; most of the time they are unmanaged
- Rarely are these devices ever monitored for security breaches

Example Connection Drivers

- Limited office space within the plant drives the need for a remote view of the plant by the engineers
 - X11 (Exceed and other X-Window applications)
 - Terminal Services
- Corporate management wants to have a “view only” display for presentation purposes
- Long-term historian might be centrally located in the plant or facility’s data center, not within the confines of the operating areas
- Numerous applications requiring OPC communications
- Advanced Control Applications need to talk to the control system, yet these might be managed from a central corporate location

Your examples?

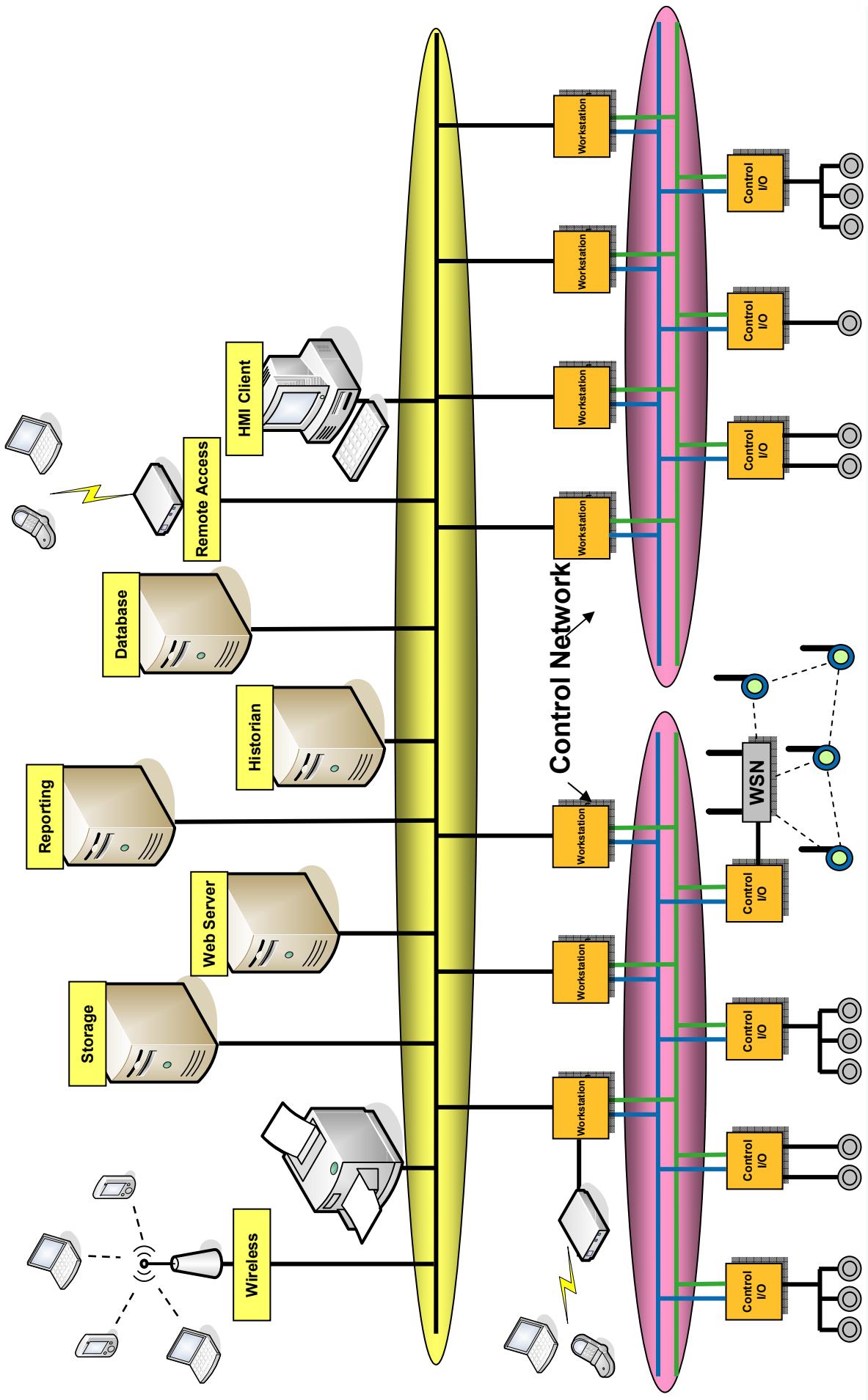
What's the problem?

- No security policy or direction
- Lack of access controls
- No auditing mechanisms
- Regulations become a driving force
- Virus/worm headaches
- Risk of intruders
 - External/internal hackers

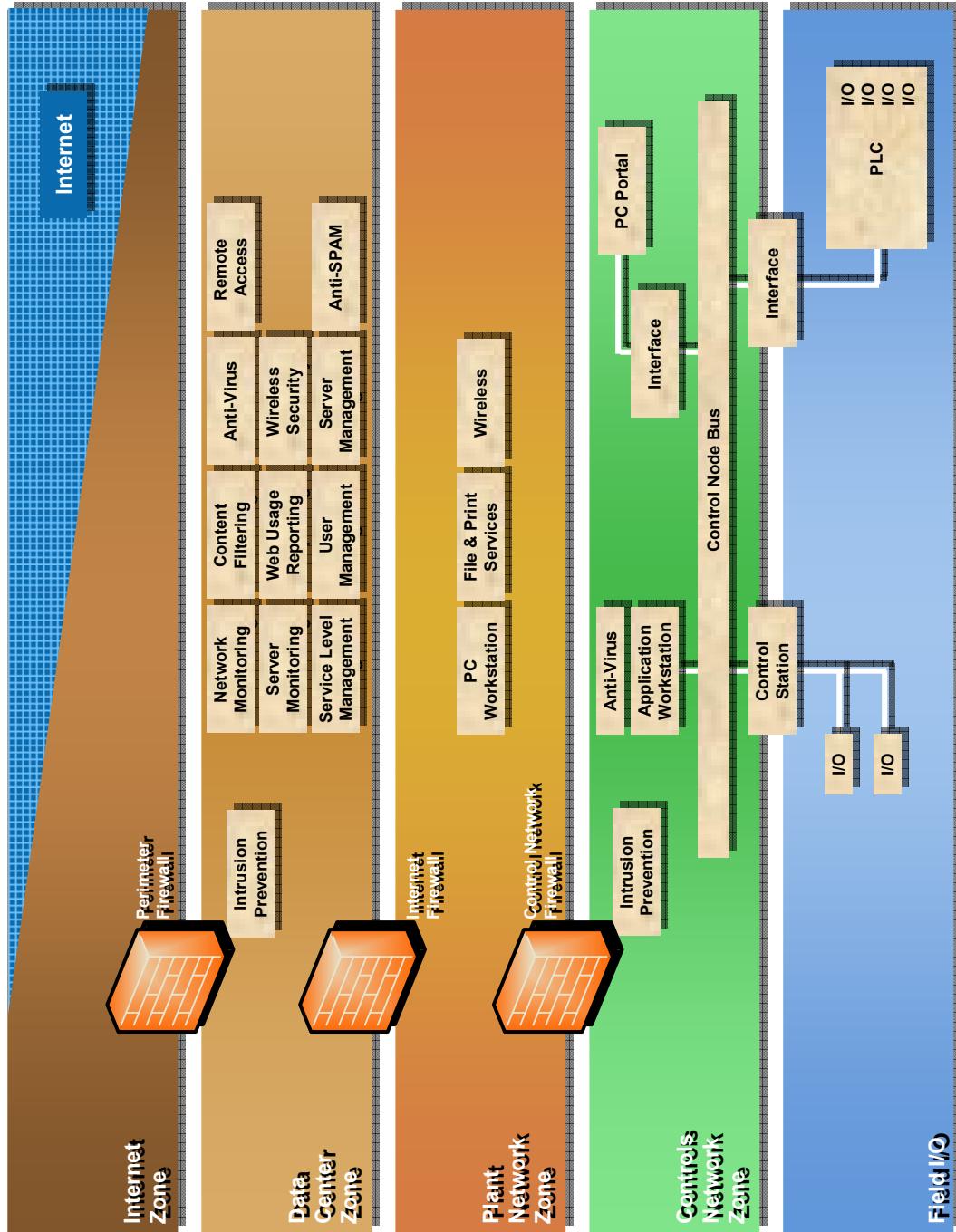
Connectivity Today

Invensys[®]

Process Systems

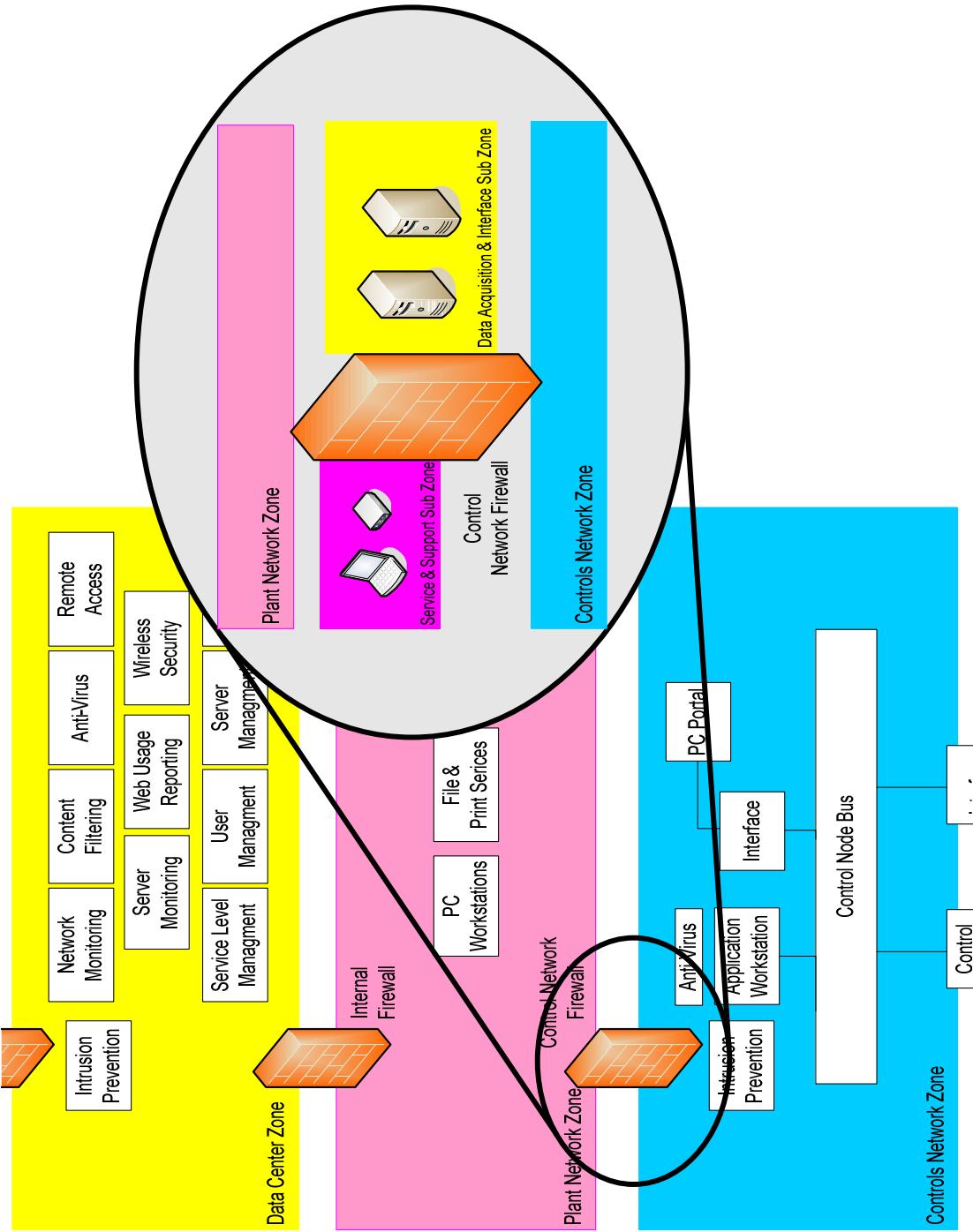


The Layered Approach



Multiple Zone Network

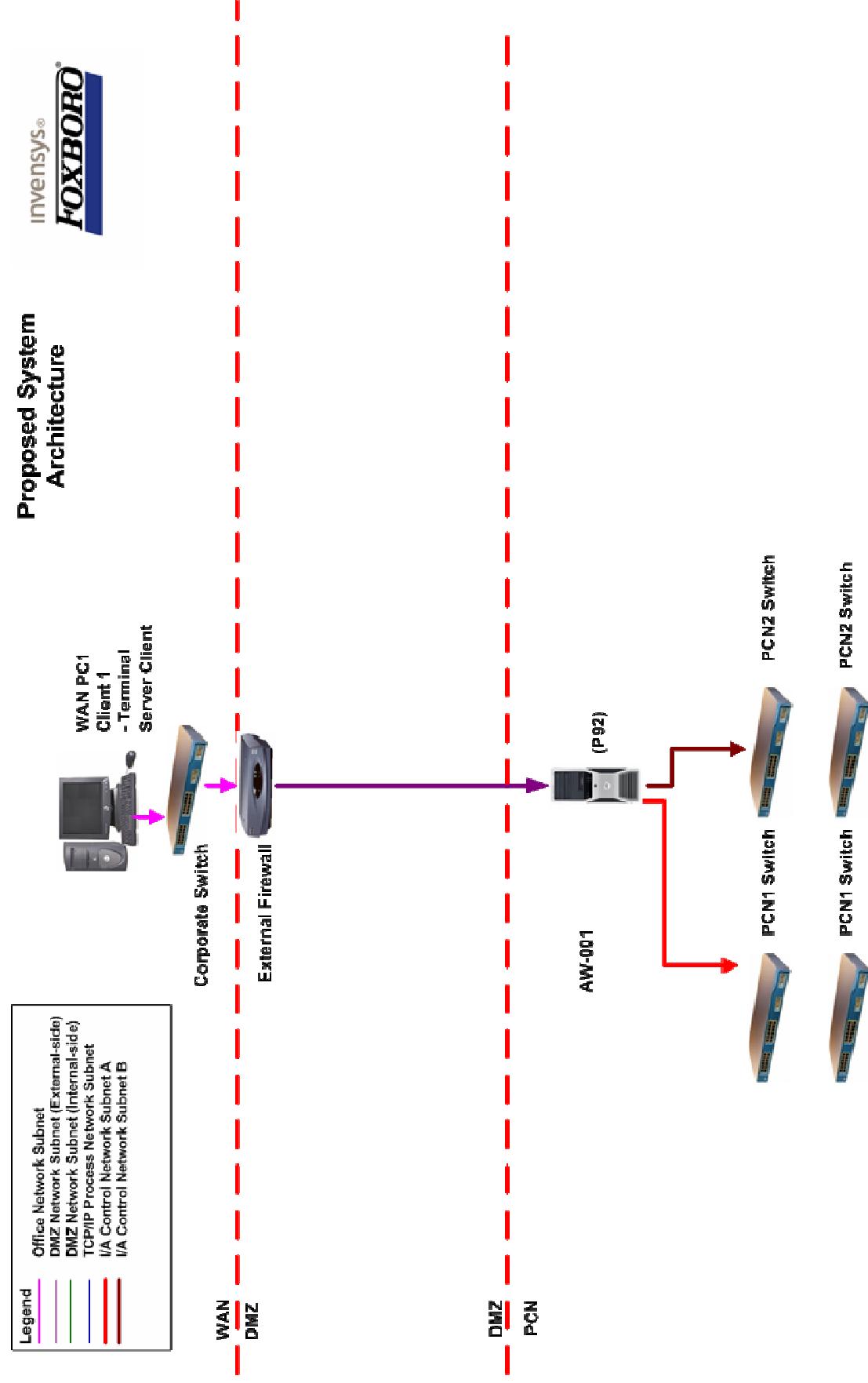
What is a DMZ?



What is the Isolation Station?

- It is a turn-key solution that can be placed in a DMZ to share process data to remote hosts.
- This data can be in the form of a historian, OPC, or process displays.
- The main components are:
 - A workstation or server connected to the DCS which collects data and “pushes” it to the DMZ
 - A DMZ server that acts as an “offline” copy of the actual control system data objects
- The implementation consists of integrating software, hardware, and engineering services.
- Doesn’t rely on DCOM and is configurable to one TCP port for cross-firewall communications.

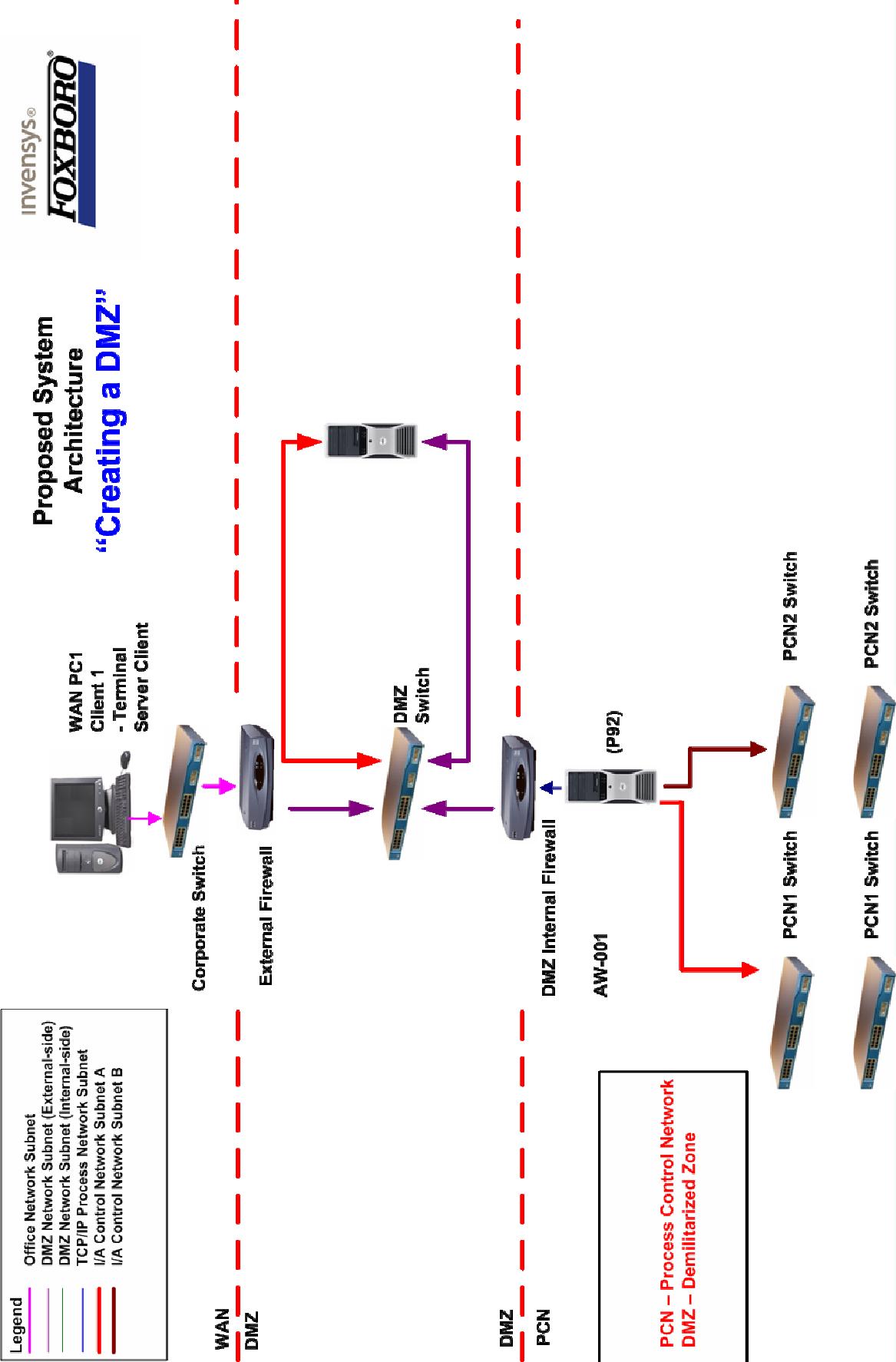
Step 1: Isolating the Control System Network



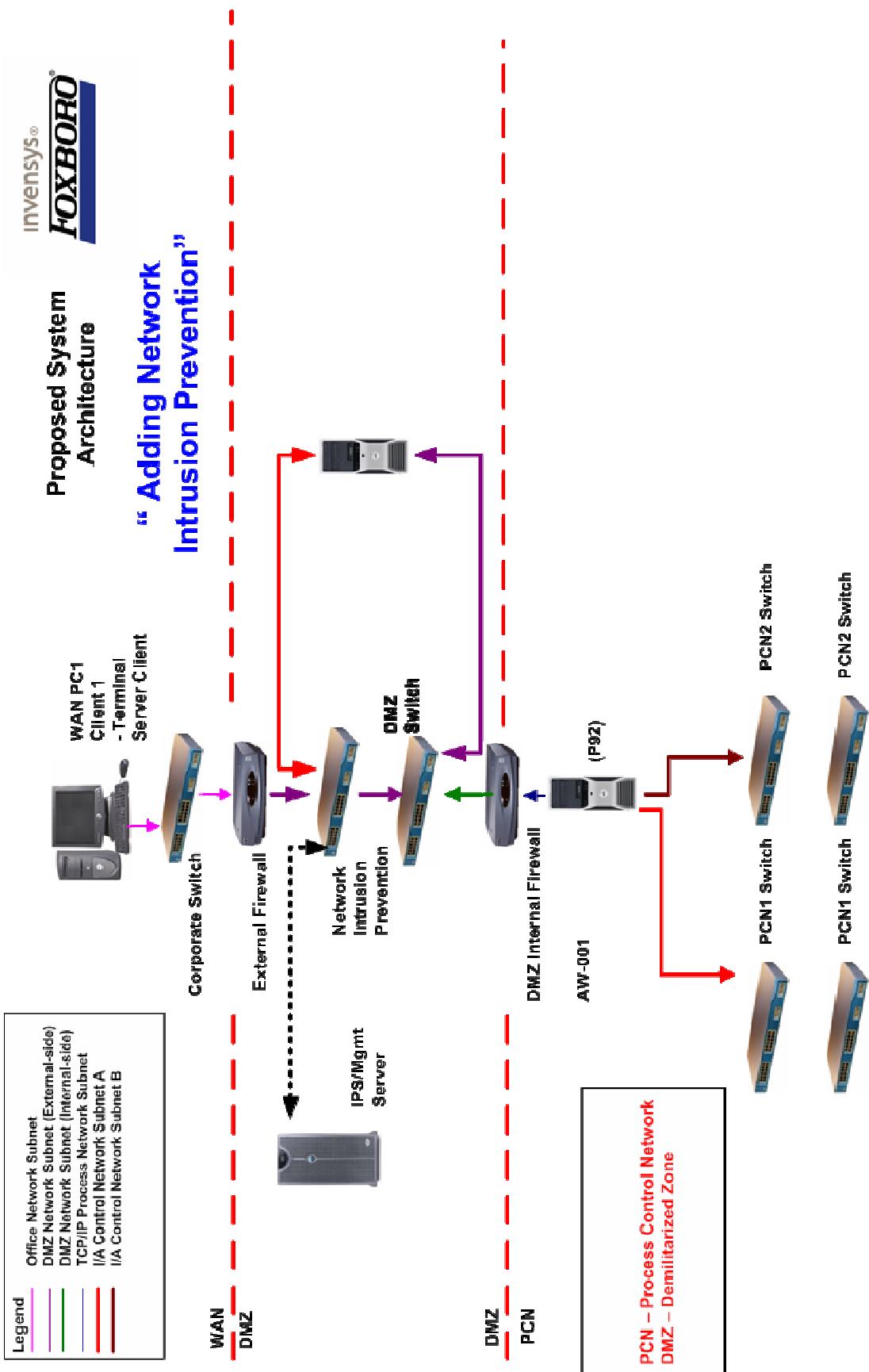
Step 2: Creating a DMZ

Legend
Office Network Subnet
DMZ Network Subnet (External-side)
DMZ Network Subnet (Internal-side)
TCP/IP Process Network Subnet
I/A Control Network Subnet A
I/A Control Network Subnet B

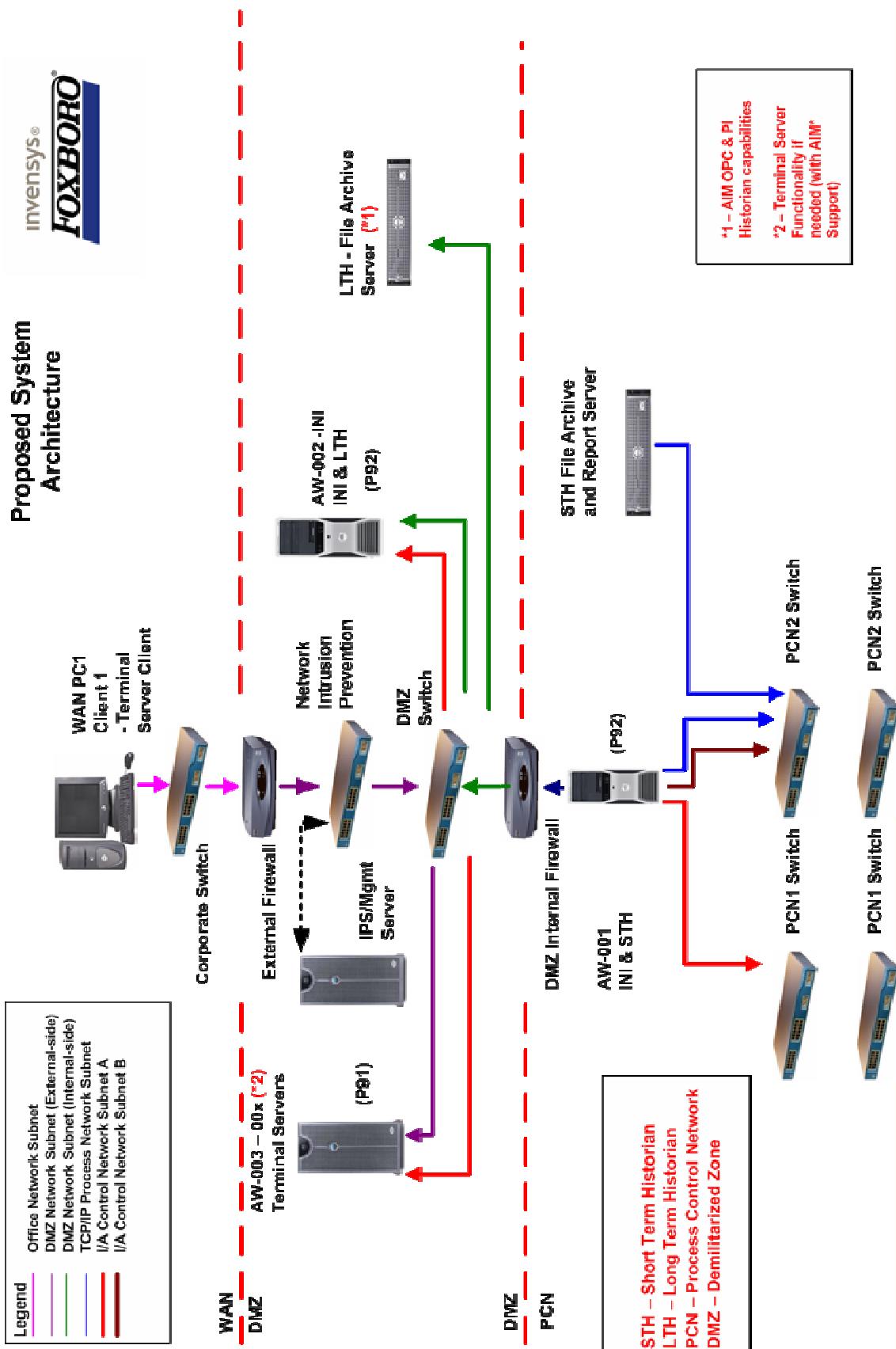
Proposed System Architecture “Creating a DMZ”



Step 3: Adding Intrusion Prevention



Step 4: Introduce “Isolation Station” Functionality



Real World Example



**TXU – Texas-based Generation
Company prepares for the future.**

Challenges

- Secure the control systems of 22 power plants.
- Standardize the security across all plants
- Comply with the up coming NERC standards.
- Maintain the flow of and enhance the value of the data available in the control systems

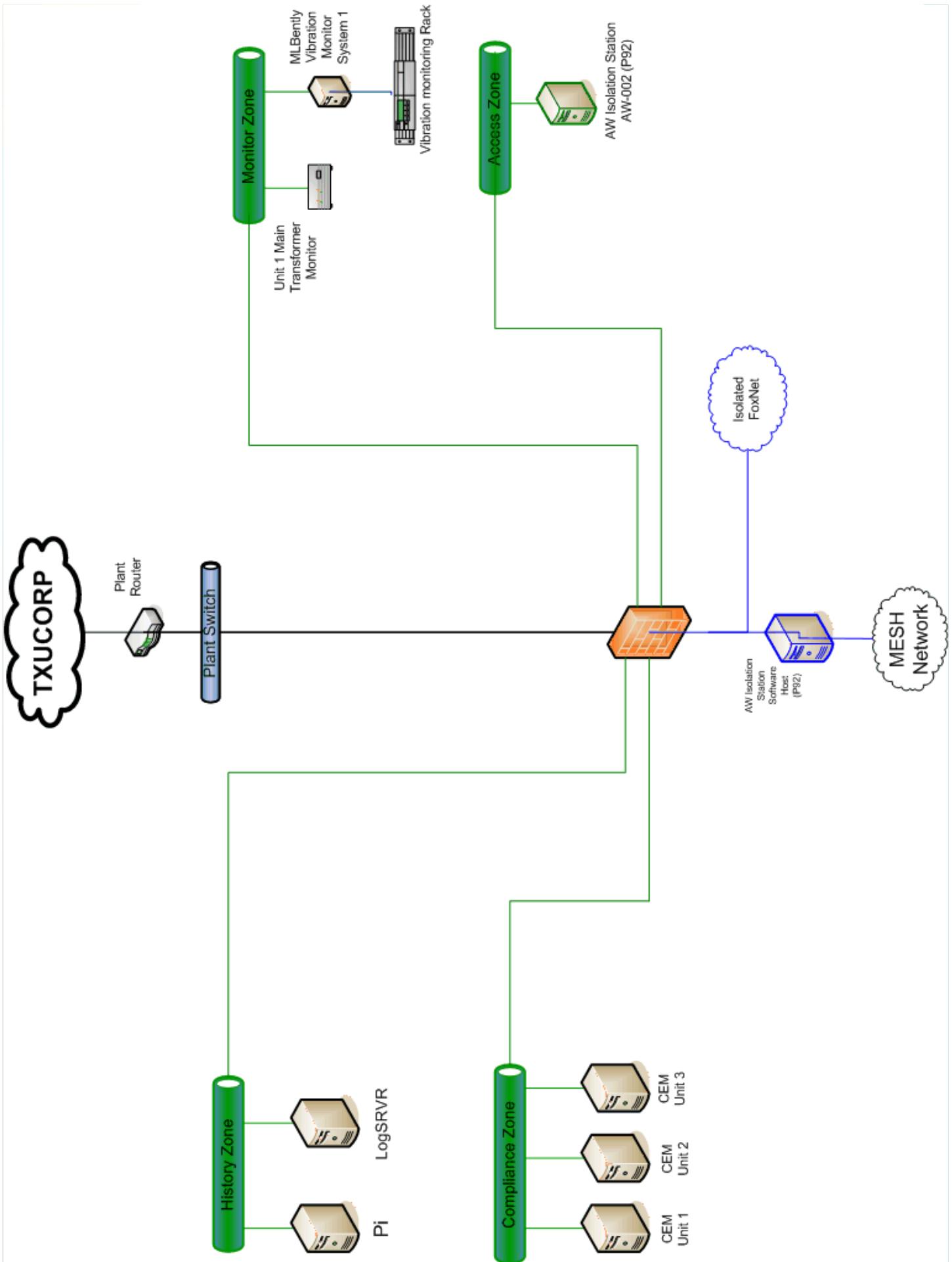
Standard Security Architecture

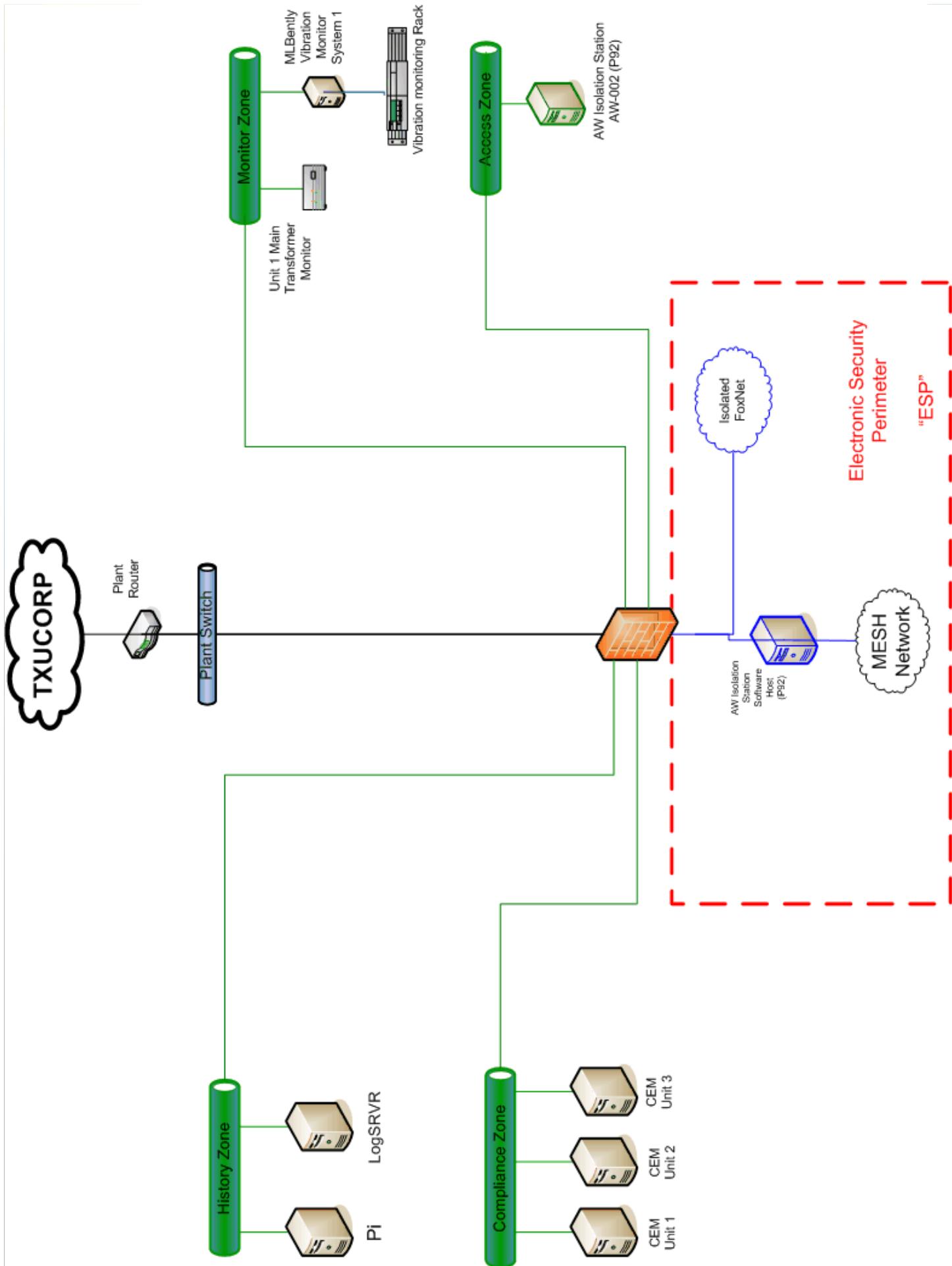
- TXU created a team of experts
- Members were drawn from control system, IT, Corporate Security and management
- SSA Team to standardize and secure all control systems
- Make certain TXU complies with NERC standards

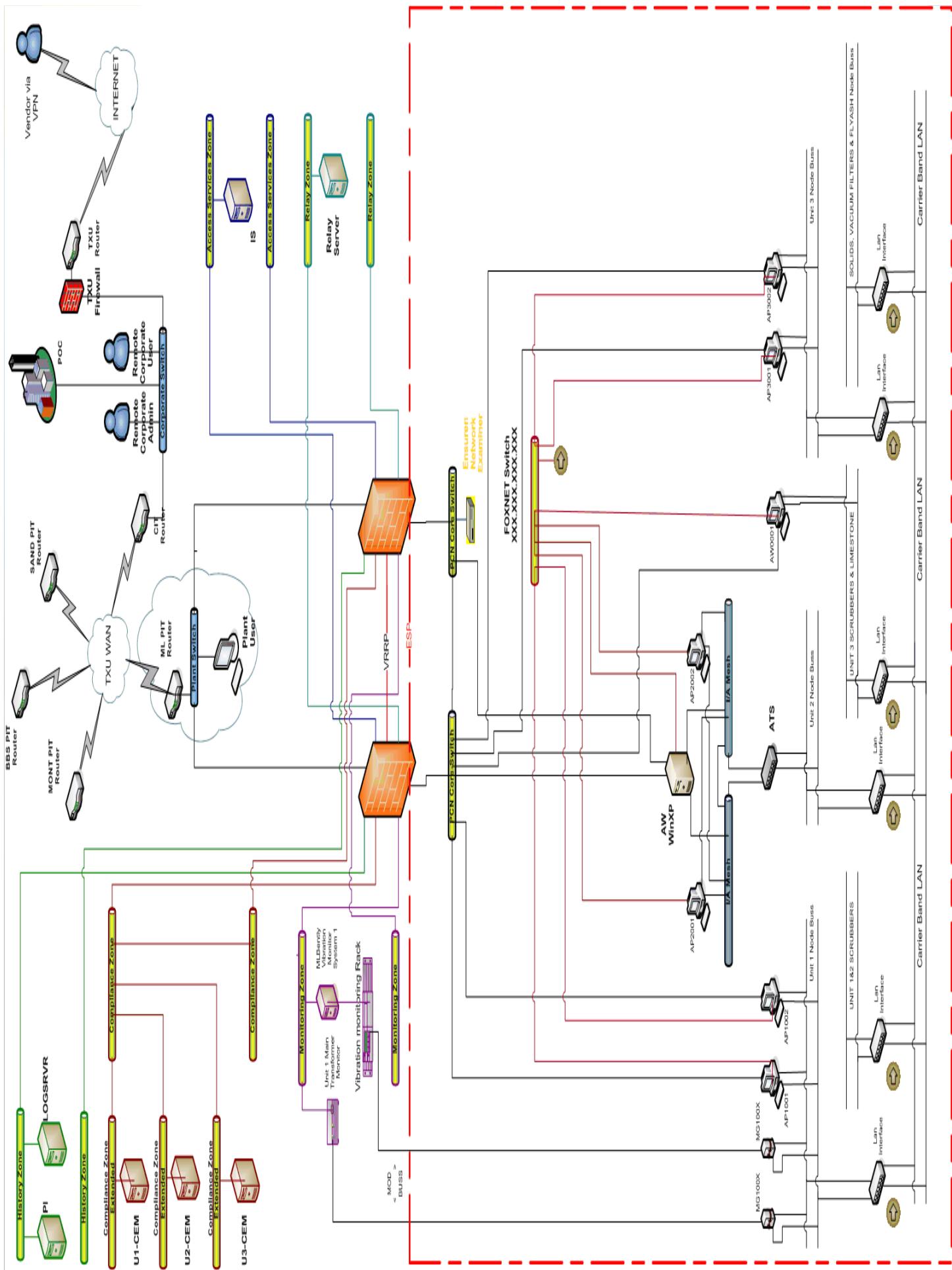
Implementation Plan for Cyber Security Standards
CIP-002-1 through **CIP-009-1**
(Continued)

Table 3
Compliance Schedule for Standards CIP-002-1 through CIP-009-1
Interchange Authorities, Transmission Owners, Generator Owners, Generator Operators,
and Load-Serving Entities

Requirement	December 31, 2006		December 31, 2008		December 31, 2009		December 31, 2010	
	All Facilities	All Facilities						
Standard CIP-002-1 — Critical Cyber Assets								
R1	BW	SC	SC	SC	C	C	AC	AC
R2	BW	SC	SC	SC	C	C	AC	AC
R3	BW	SC	SC	SC	C	C	AC	AC
R4	BW	SC	SC	SC	C	C	AC	AC
Standard CIP-003-1 — Security Management Controls								
R1	BW	SC	SC	SC	C	C	AC	AC
R2	SC	C	C	AC	AC	AC	AC	AC
R3	BW	SC	SC	SC	C	C	AC	AC
R4	BW	SC	SC	SC	C	C	AC	AC
R5	BW	SC	SC	SC	C	C	AC	AC
R6	BW	SC	SC	SC	C	C	AC	AC
Standard CIP-004-1 — Personnel & Training								
R1	BW	SC	SC	SC	C	C	AC	AC
R2	BW	SC	SC	SC	C	C	AC	AC
R3	BW	SC	SC	SC	C	C	AC	AC
R4	BW	SC	SC	SC	C	C	AC	AC
Standard CIP-005-1 — Electronic Security								
R1	BW	SC	SC	SC	C	C	AC	AC
R2	BW	SC	SC	SC	C	C	AC	AC
R3	BW	SC	SC	SC	C	C	AC	AC
R4	BW	SC	SC	SC	C	C	AC	AC
R5	BW	SC	SC	SC	C	C	AC	AC







Creating a Secure Zone for Control System Communications



Thank you.

Clayton L. Coleman
Clayton.Coleman@ips.invensys.com

James Basset
jbasset1@capgeminienergy.com
James.Basset@TXU.com