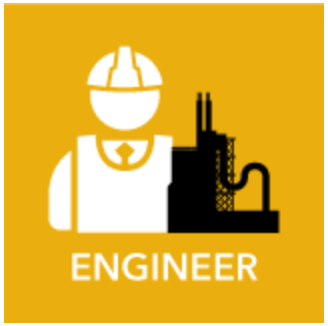
Ensuring Your Plant is Secure

Tim Johnson, Cyber Security Consultant

Schneider Electric

The Foxboro Evo™ Process Automation System

Addressing the needs across your operation today and tomorrow.



Industrial Control Systems

Why Cyber Security

Why Now

Industrial Control System
Cyber Security Headlines

Industrial Control System
Cyber Security

In a "**post-Stuxnet"** world, a lot of attention is being given to the Industrial Control Systems running task for critical infrastructure and important manufacturing processes.

Much of this attention is caused by a new wave of security research being performed on the security vulnerabilities that many of these systems possess.

It is one thing to say that a system has security vulnerabilities, but it is something entirely different to say that the system is insecure,"

http://www.securitybistro.com

Industrial Control System
Cyber Security Impact

- More Corporate/Regulatory Compliance
- Requirements to Reduce Environmental and Financial Risk
- Decreases Plant Safety
- Non-Secure Plant to the Enterprise Network Connections
- Increased Downtime
- Decreased Network Performance

Industrial Control Systems

Protect

Industrial Control System
Cyber Security Basics

Seven Building Blocks Required for Cyber Security

1. Identify what should be protected
   - Identify what is Critical to the Process
2. Electronic Access Controls
   - Firewall Network Segmentation
3. User Access Controls
   - Least Privilege Methodology for Users
4. Patching
   - OS and Software
5. Anti-Virus
   - Advanced Anti-Virus technologies i.e. Device Control
6. Disaster Recovery (Backups)
   - Backup & Recovery Planning
7. Logging & Alerting
   - Failed and Successful Logins

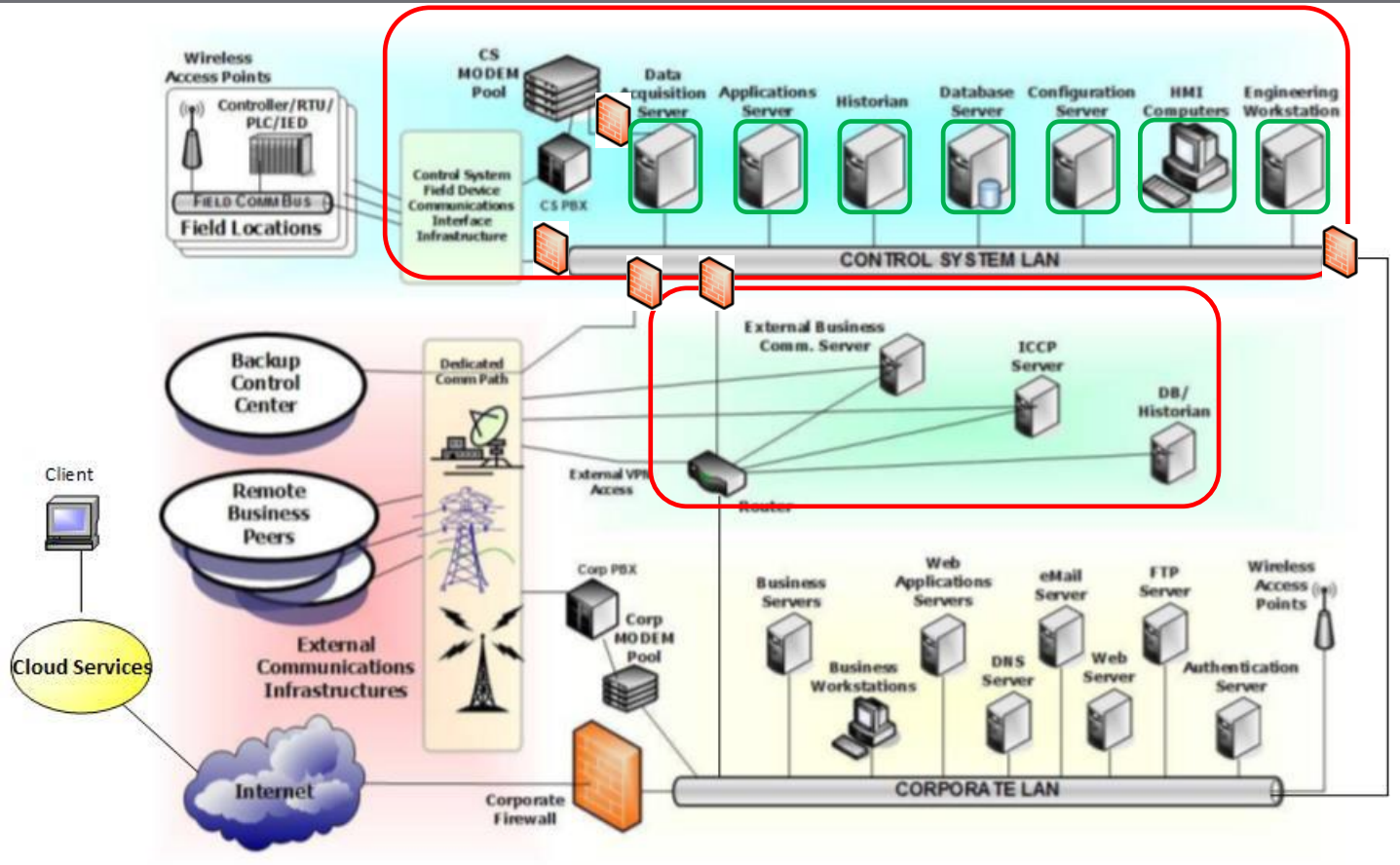
Industrial Control Systems

Best Practices

*Network Segregation

*Electronic Access Point Access Controls

*System Hardening



Industrial Control Systems

Best Practices - Continued

*Network Segregation

*Electronic Access Point Access Controls

*System Hardening

*User Access Controls

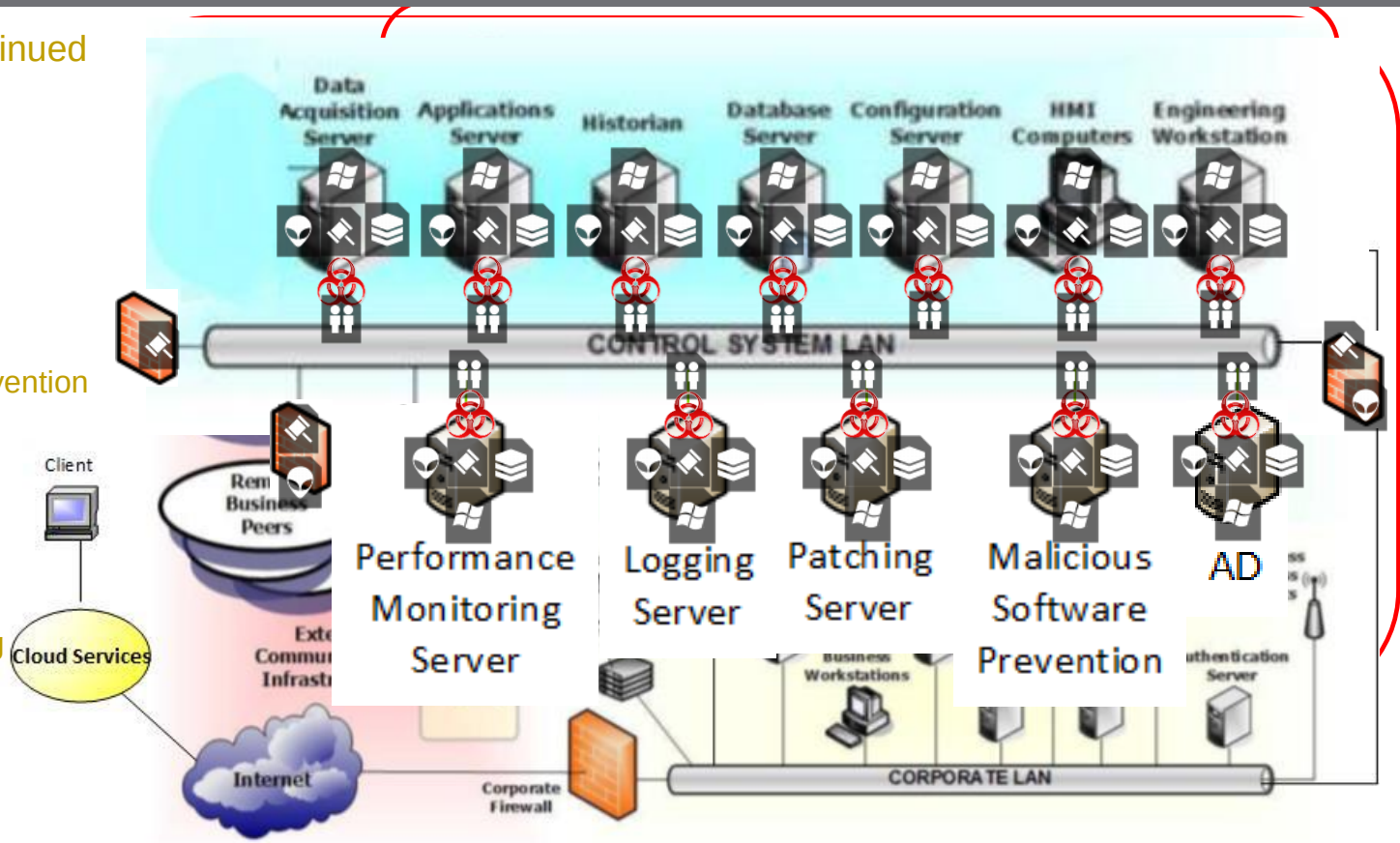
*Malicious Software Prevention
- Antivirus
- Device Control

*Patching Server

*Backups

*Performance Monitoring & Alerting

*Logging Server



Industrial Control Systems

Maintain

Industrial Control Systems

Centralized Cyber Management

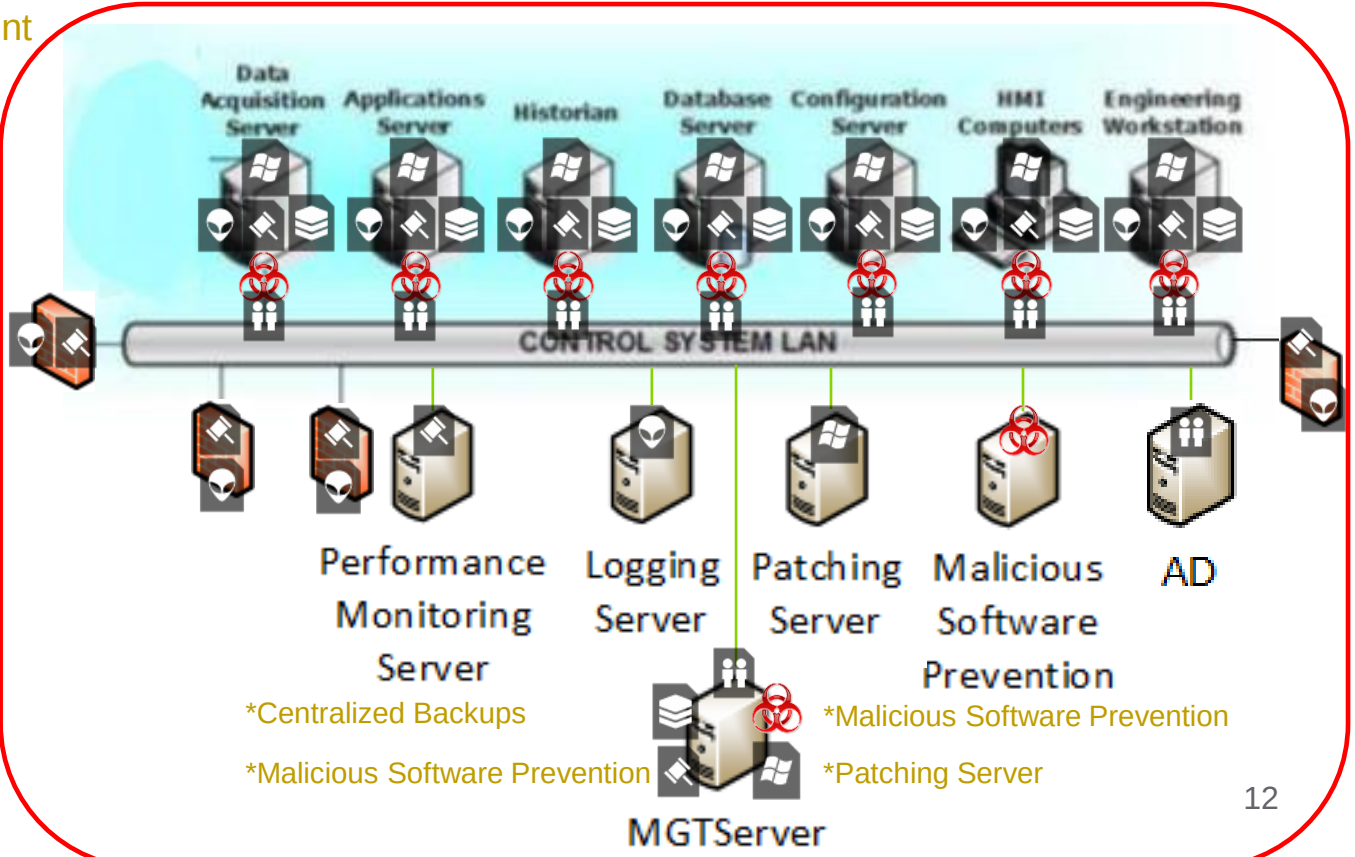
Management Server

*Malicious Software Prevention
- Antivirus
- Device Control

*Patching Server

*Backups

*Performance Monitoring & Alerting



Foxboro Evo™

Process Automation System Cyber Security

Foxboro Evo™
Enabling Cyber Security

Product Features for Secure Deployments:

- McAfee ePO Centralized Management and configuration for:
  - Anti-Virus Settings and DAT updates based on Computer memberships
  - Advanced protections based on users, security groups and computer memberships
  - Data Loss Prevention (Removable Media/USB device controls)
  - Whitelisting
- Centralized Account Management for Operating System (Active Directory)
  - Ability to utilize single or shared user account methodologies
  - Operating System GUI set based on user login
  - Computer Security Settings set by simple drag and drop methodogy
- System Access Controls for Users and Computers Management (Active Directory GPOs)
  - Locked Windows GUI
  - Preliminary Operating System Hardening
- System configuration Baseline and Reports (Station Assessment Tool “SAT”)
- Backup and Recovery (BESR)

Foxboro Evo™
Looking to the Future

Adopting New Technologies:

- Virtualization for Foxboro Stations:
  - Helps lower cost for maintain cyber security programs
    - Less hardware to track, maintain and warrantee
    - Snapshot recovery facilitates patching programs
    - Snapshot recovery reduces dependence on similar hardware and reduces system recovery times
- Single Active Directory Deployment Methodologies
  - Off MESH and Existing Active Directory Integration support as standard product feature
    - Leverage existing DCS Active Directory Installations
    - Create new Active Directory deployments for managing user access controls across your whole plant
- McAfee ePO Advanced Threat Management Mitigitations
  - Application Whitelisting
  - File Integrity Control

Industrial Control Systems

Critical Infrastructure Security Practice (CISP)

CISP
Operation Technology

- Experienced with IT technologies but with a Industrial Control System mindset
  - Bridge technology gap for today's heavily technology based Process Automation Systems
- Providing Cyber Security and Technology services for Industrial Control Systems since 2001
  - CISP Consultants are focused on Critical Infrastructure Market
- Cyber Security implementations across varying industries
- Cyber Security and Technology solutions covering your whole Plant
  - Vendor Independent Cyber Security Solutions

CISP
Services & Solutions

- Expanding Cyber Security for Foxboro Evo™
  - Foxboro Evo™ Cyber Security integration into Non-Foxboro systems
  - Advanced Active Directory integration
  - Network Alarming and Event Management
  - Patching solutions for Foxboro and Non-Foxboro systems
- Technology Assessments and Remediation
- Cyber Security Assessments and Remediation
- NERC CIP Workshops
- Services and Solutions for meeting Corporate Cyber Security requirements placed on Industrial Control Systems

Ensuring Your Plant is Secure

Putting it all together

Ensuring Your Plant is Secure

*Cyber Security implementation capable of supporting other Vendors

*Ability to Integrate Active Directory (Plant Wide Active Directory Solution)

*Network Segmentation

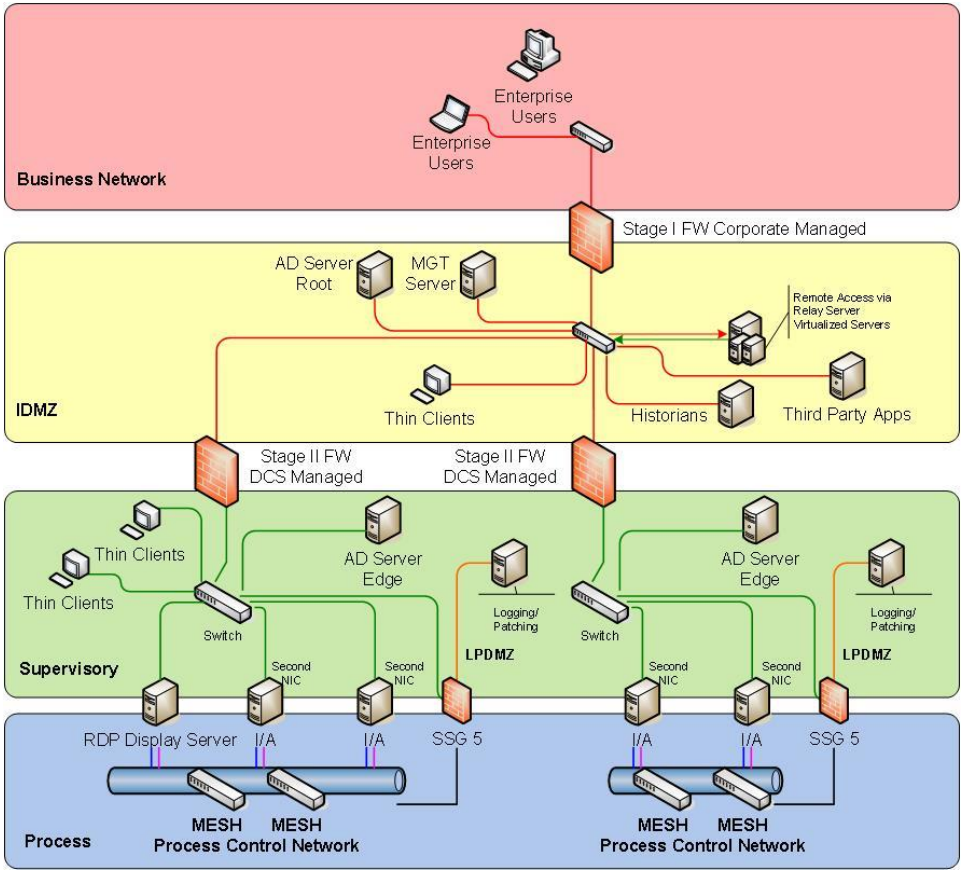
*MGT Server for Centralized Server Dedicated to Cyber Security Task (Plant Wide Solution)

- ePO Server, Patching Server, Logging Server, Centralized Backup Repository, Performance Monitoring and Alerting

*Thin Clients lowering Management and Maintenance cost

*Relay Zone Server Creates a Bastion Host limiting Direct Access from Un-Trusted Networks to DCS Trusted Networks

- Dedicated to RDP access only
- View only or Engineering Server Options
- Additional Active Directory security measure may be implemented



Ensuring Your Plant is Secure
Schneider Electric Cyber Security

CISP Cyber Solutions

- Asset Identification
- User Access Controls
- Electronic Access Controls
- Logging
- Network Design & Management
- Backup and Restoration
- Anti Malware
- Patching
- Platform Hardening

Foxboro Evo™ + **Cyber Security** = Your Plant is Secure

Thank you!