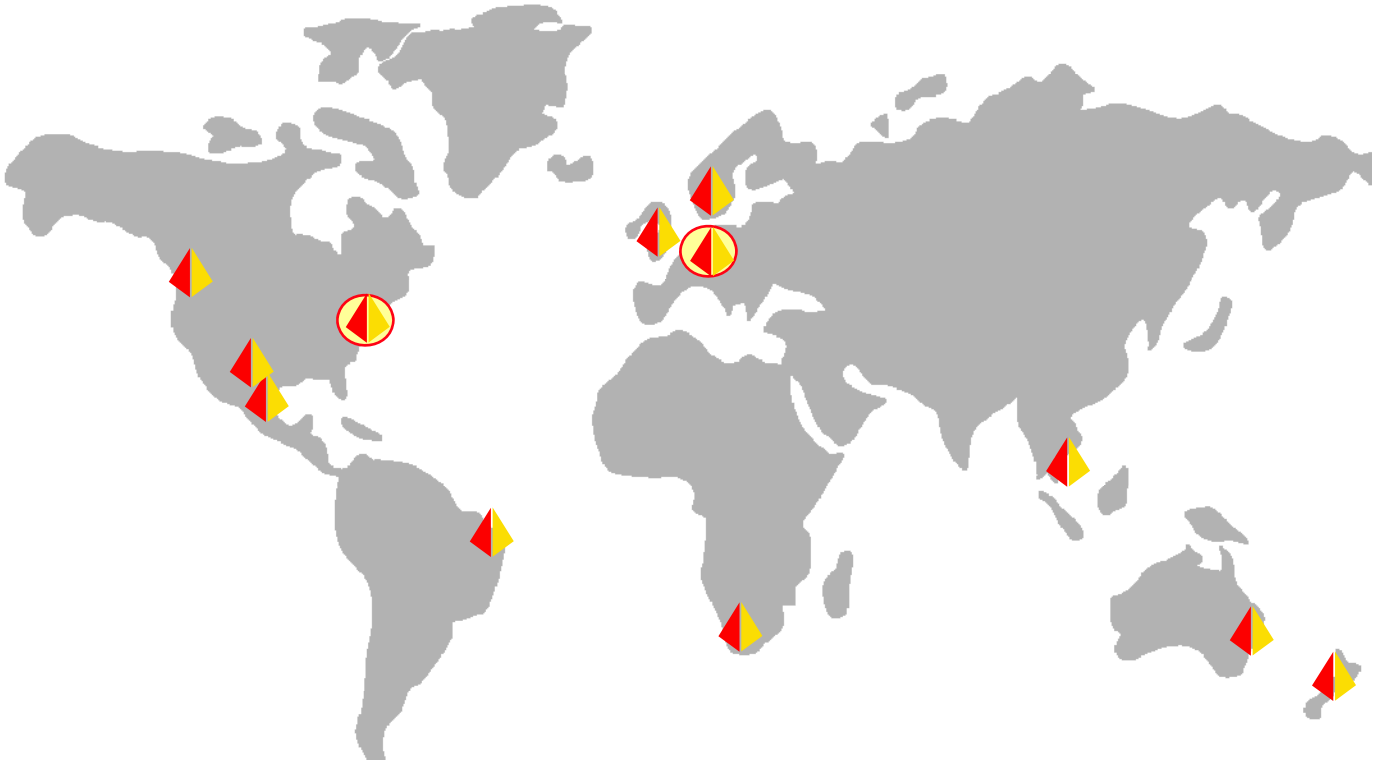
The 7 Things Every Plant Manager Should Know About Control System Security

24 February 2011

John A. Cusimano, CFSE, CISSP

- Director of Security Solutions for exida
- 20+ years experience in industrial automation
- Employment History:
  - Eastman Kodak
  - Moore Products
  - Siemens
- Certifications:
  - CFSE, Certified Functional Safety Expert
  - CISSP, Certified Information Systems Security Professional
- Industry Associations:
  - ISA S99 Committee
  - ISA S84 Committee
  - ISA Security Compliance Institute
  - ICSJWG Workforce Development & Vendor Subgroups

- We help our clients improve the safety, security and availability of their automation systems



Agenda

- Intro to Control System Security
- The 7 Things
- Case Study
- Summary

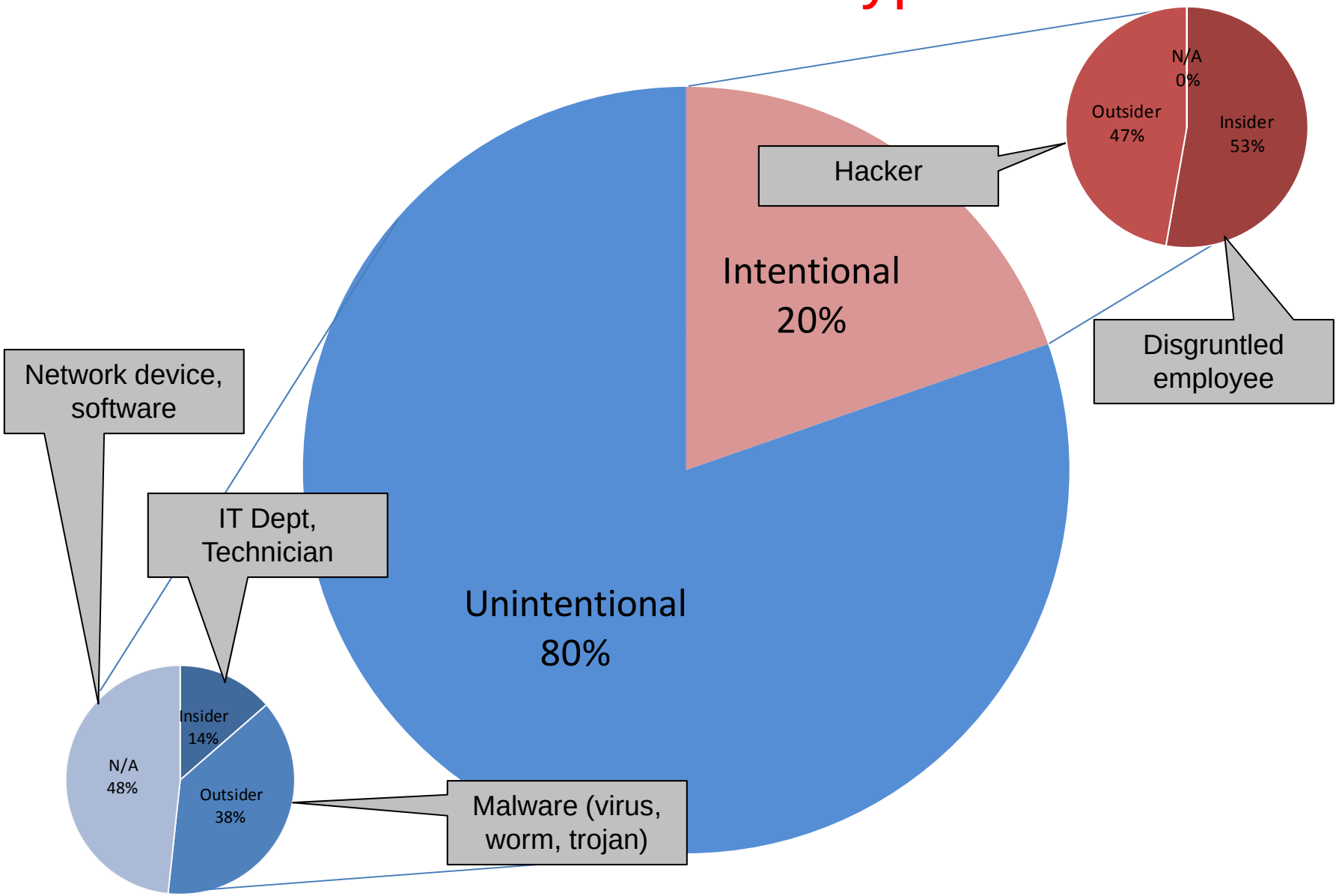
What is Control System Security?

- Prevention of intentional or unintentional interference with the proper operation of industrial automation and control systems through the use of computers, networks, operating systems, applications and other programmable configurable components of the system
- Goes by many names:
  - SCADA Security
  - PCN Security
  - Industrial Automation and Control System Security
  - Control System Cyber Security
  - Industrial Network Security
  - Electronic Security for Industrial Automation and Control Systems

Control Systems are more vulnerable today than ever before

- Heavy use of Commercial Off-the Shelf Technology (COTS) and protocols
  - *Integration of technology such as MS Windows, SQL, and TCP/IP means that process control systems are now vulnerable to the same viruses, worms and trojans that affect IT systems*
- Increased Connectivity
  - *Enterprise integration (using plant, corporate and even public networks) means that process control systems (legacy) are now being subjected to stresses they were not designed for*
- Demand for Remote Access
  - *24/7 access for engineering, operations or technical support means more insecure or rogue connections to control system*
- Public Information
  - *Manuals on how to use control system are publicly available*

Actual Incident Types



Stuxnet Summary

- First malware specifically targeting industrial control systems
- First discovered in June 2010 (in circulation since June 2009)

- Has the ability reprogram Siemens S7 PLCs
- Infects Siemens SIMATIC software running on Win PCs
- Uses SIMATIC software to read S7 PLC memory and overwrite FB with its own code (hidden)
- Spreads via USB memory sticks, local networks and Step 7 project files
- Thousands of PC's infected worldwide (predominantly Iran, India and Indonesia)
- Approximately 22 cases reported on SIMATIC systems

Pathways for Stuxnet Infection

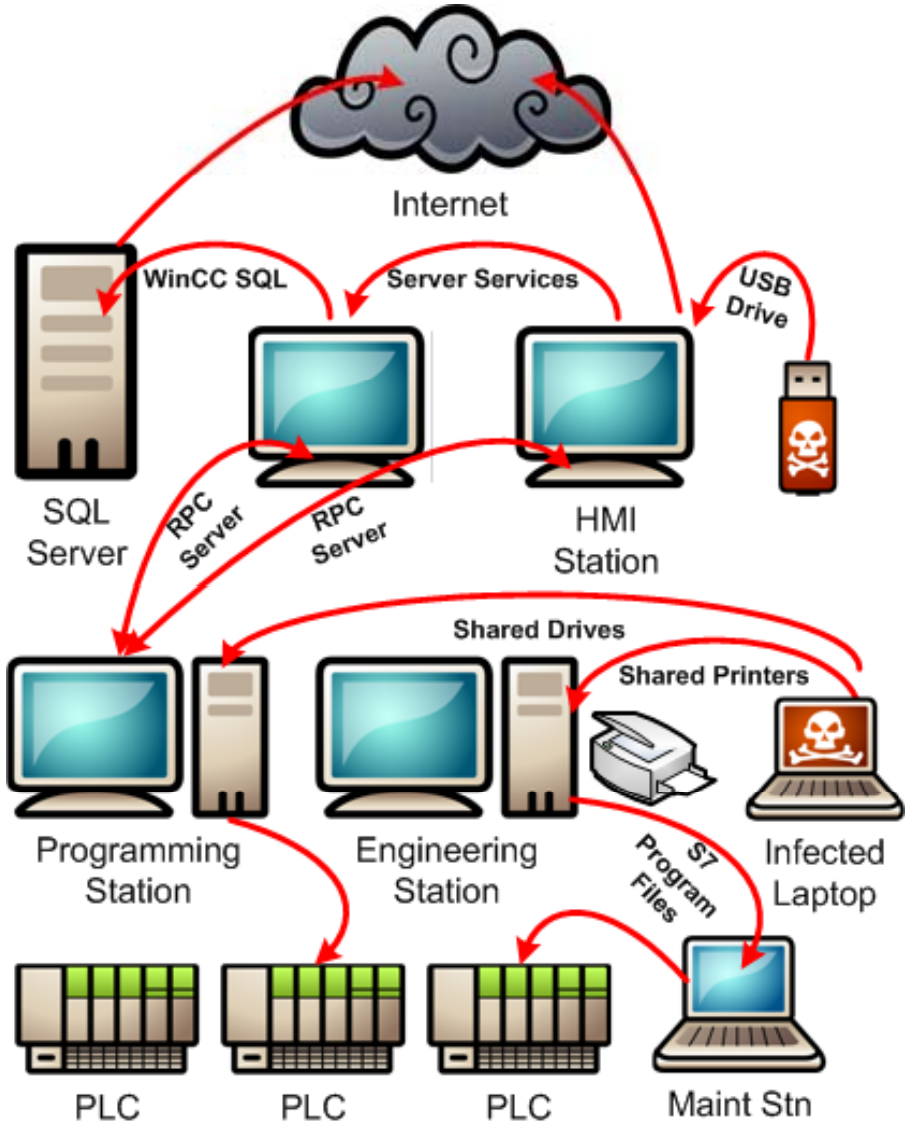


Image courtesy of Byres Security Inc.

Stuxnet Exploit	Mitigation	Operating System								
		Windows 2000 SP4	Windows XP SP1, SP2	Windows XP SP3	Server 2003 SP1	Server 2003 SP2	Windows Vista	Windows Server 2008	Windows 7	Windows Server 2008 R2
General Malware Infection	General Infection Prevention	Install anti-virus or white listing software in all computers Ensure all signatures September 2010 or newer								
Malware Connection to Internet	Prevent ICS Connections to Internet	Install a firewall to block all outbound communications from control system to Internet								
Shortcut/*.lnk File Vulnerability	Mitigation 1 USB Management	Avoid using USB drives in Control Systems If USB drives must be used, prequalify them								
	Mitigation 2 Windows Patch	Not available		Install patch MS10-046	Not available	Install patch MS10-046				
	Mitigation 3 Disable Icons	Disable the display of icons for shortcuts		Not recommended	Disable the display of icons for shortcuts	Not recommended				
	Mitigation 4 Disable WebClient	Disable the WebClient service		Not recommended	Disable the WebClient service	Not recommended				
Autorun Exploit	Disable Autorun	Disable Autorun for all USB drives								
Windows printer spooler vulnerability	Mitigation 1 Firewall RPC Traffic	Install cell or zone firewall to limit TCP and UDP ports associated with RPC to the minimum required If OPC traffic is present use OPC-aware firewall								
	Mitigation 2 Windows Patch	Not available		Install patch MS10-061	Not available	Install patch MS10-061				
	Mitigation 3 Disable Sharing	Disable printer sharing by all critical servers								
	Mitigation 4 Disable Guest Account	Disable guest account			Guest account disabled by default – no action required if password-based sharing used					
Server service vulnerability	Mitigation 1 Firewall RPC Traffic	Install cell or zone firewall to limit TCP and UDP ports associated with RPC to the minimum required If OPC traffic is present use OPC-aware firewall								
	Mitigation 2 Windows Patch	Install patch MS08-067							Not Required	
Siemens "internal" System Passwords		No confirmed mitigation SIMATIC Security Update may reduce exposure								
Propagation to STEP 7 Files		No known mitigation								
Stuxnet P2P RPC Service	Firewall All RPC Traffic	Install cell or zone firewall to limit TCP and UDP ports associated with RPC to the minimum required If OPC traffic is present use OPC-aware firewall								
Elevation of Privilege 1	Windows Patch	Not available		Install patch MS10-073	Not available	Install patch MS10-073				
Elevation of Privilege 2	Windows Patch	Not Required					Install patch MS10-092			

BYRES SECURITY INC.

TEL: 1 250 390 1333
TOLL FREE: 1 877 297 3799 (N. America)
EMAIL: sales@tofinosecurity.com

TOFINO®

http://www.tofinosecurity.com/stuxnet-central

First Things First

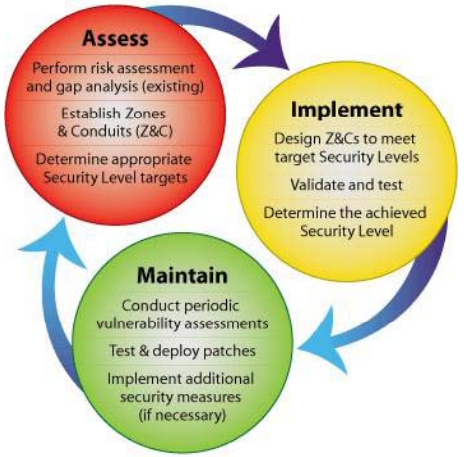
7 things every plant manager should do to secure their facility from unwanted intrusion

THE 7 THINGS

1. Assess Existing Systems
2. Document Policies & Procedures
3. Train Personnel & Contractors
4. Segment the Control System Network
5. Control Access to the System
6. Harden the Components of the System
7. Monitor & Maintain System Security

#1 Assess Existing Systems

- Perform control system security assessments of existing systems
- Compare current control system design, architecture, policies and practices to standards & best practices
- Identify gaps and provide recommendations for closure
- Benefits:
  - Provides management with solid understanding of current situation, gaps and path forward
  - Helps identify and prioritize investments
  - First step in developing a security management program



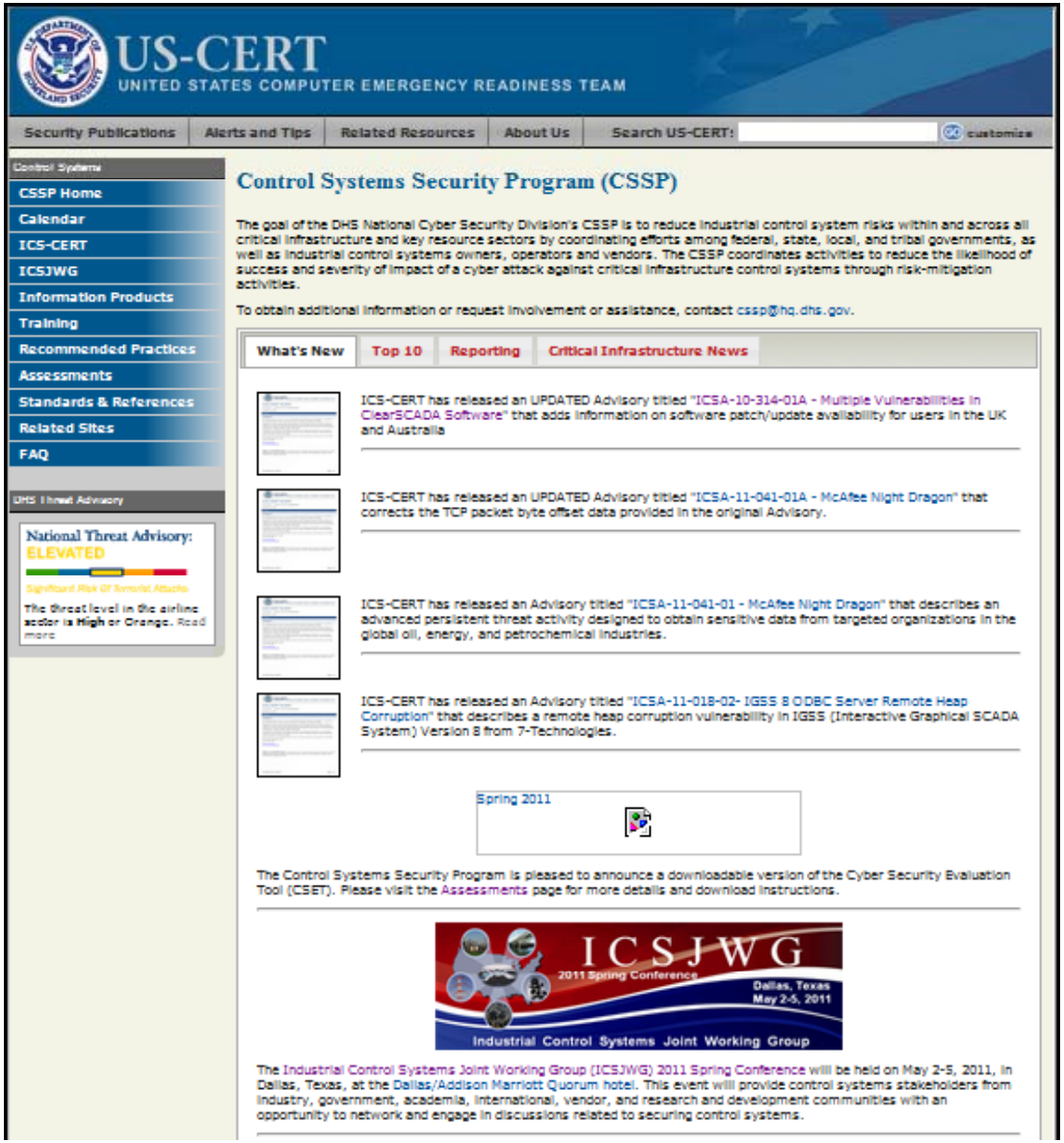
Standards Efforts

- International Society for Automation (ISA)
  - ISA99, Industrial Automation and Control System (IACS) Security
- International Electrotechnical Commission (IEC)
  - IEC 62443 series of standards (equivalent to ISA 99)
- National Institute for Standards and Technology (NIST)
  - SP800-82 Guide to Industrial Control Systems (ICS) Security

Industry Specific Guidance

- American Petroleum Institute
  - API Standard 1164 - SCADA Security
- American Chemistry Council's Chemical Information Technology Council (ChemITC)™ Chemical Sector Cyber Security Program
  - Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0
- North American Electric Reliability Corporation (NERC)
  - Critical Infrastructure Protection (CIP) 002 – 009
- Department of Homeland Security
  - Chemical Facility Anti-terrorism Standards (CFATS)
  - Risk-based Performance Standards (RBPS) (RBPS 8)

DHS Control Systems Security Program

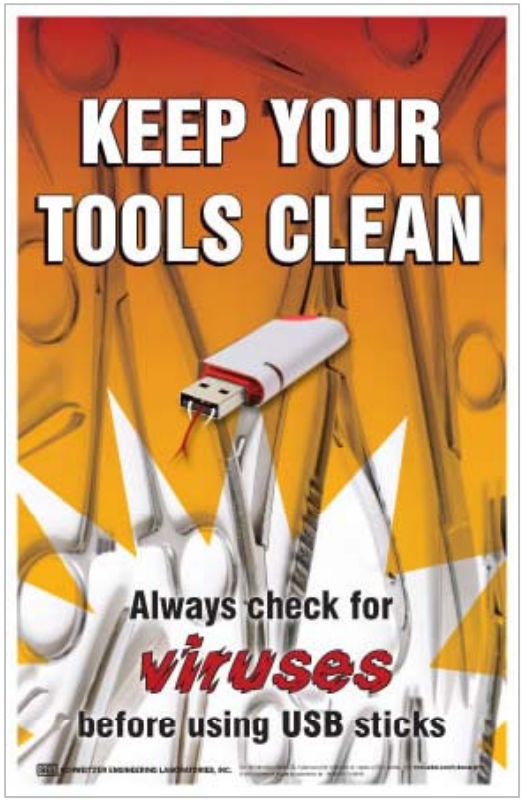


#2 Document Policies & Procedures

- Establish control system security policies & procedures
  - Scope
  - Management Support
  - Roles & Responsibilities
  - Specific Policies
    - Remote access
    - Portable media
    - Patch mgmt
    - Anti-virus management
    - Change Management
    - Backup & Restore
  - References

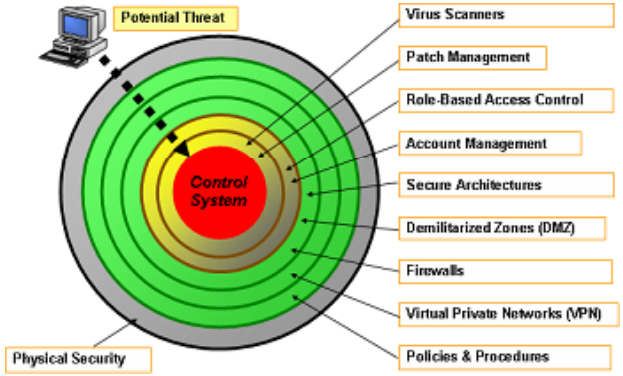
#3 Train Personnel & Contractors

- Make sure personnel are aware of the importance of security and company policies
- Provide role-based training
  - Visitors
  - Contractors
  - New hires
  - Operations
  - Maintenance
  - Engineering
  - Management



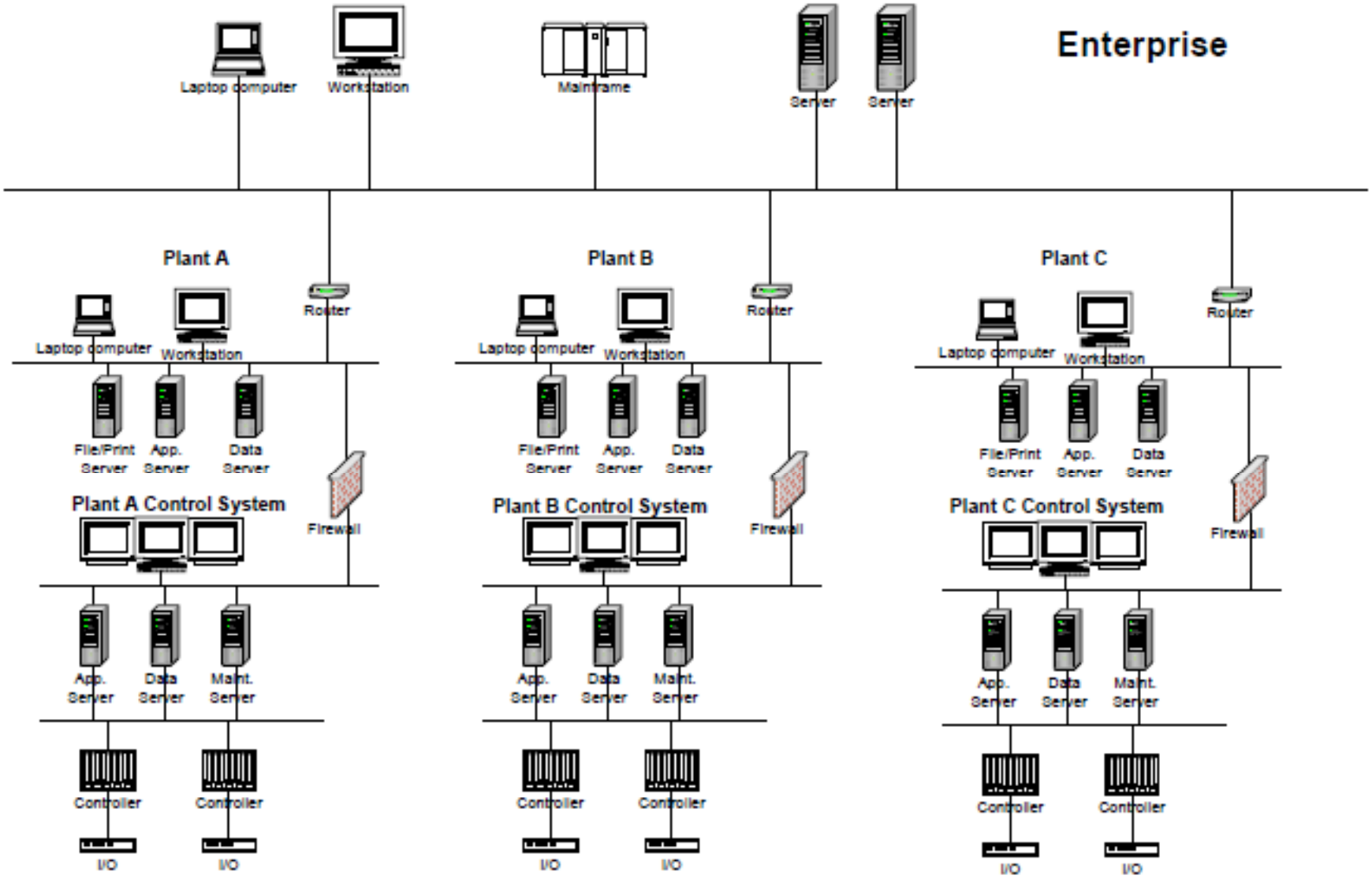
#4 Segment the Network

- Defense-in-Depth strategy
- Partition the system into distinct security zones
  - Logical grouping of assets sharing common security requirements
  - There can be zones within zones, or subzones, that provide layered security
  - Zones can be defined physically and/or logically



- Define security objectives and strategy for each zone
  - Physical
  - Logical
- Create secure conduits for zone-to-zone communications
  - Install boundary or edge devices where communications enter or leave a zone to provide monitoring and control capability over which data flows are permitted or denied between particular zones.

System Architecture



Partitioning into Zones

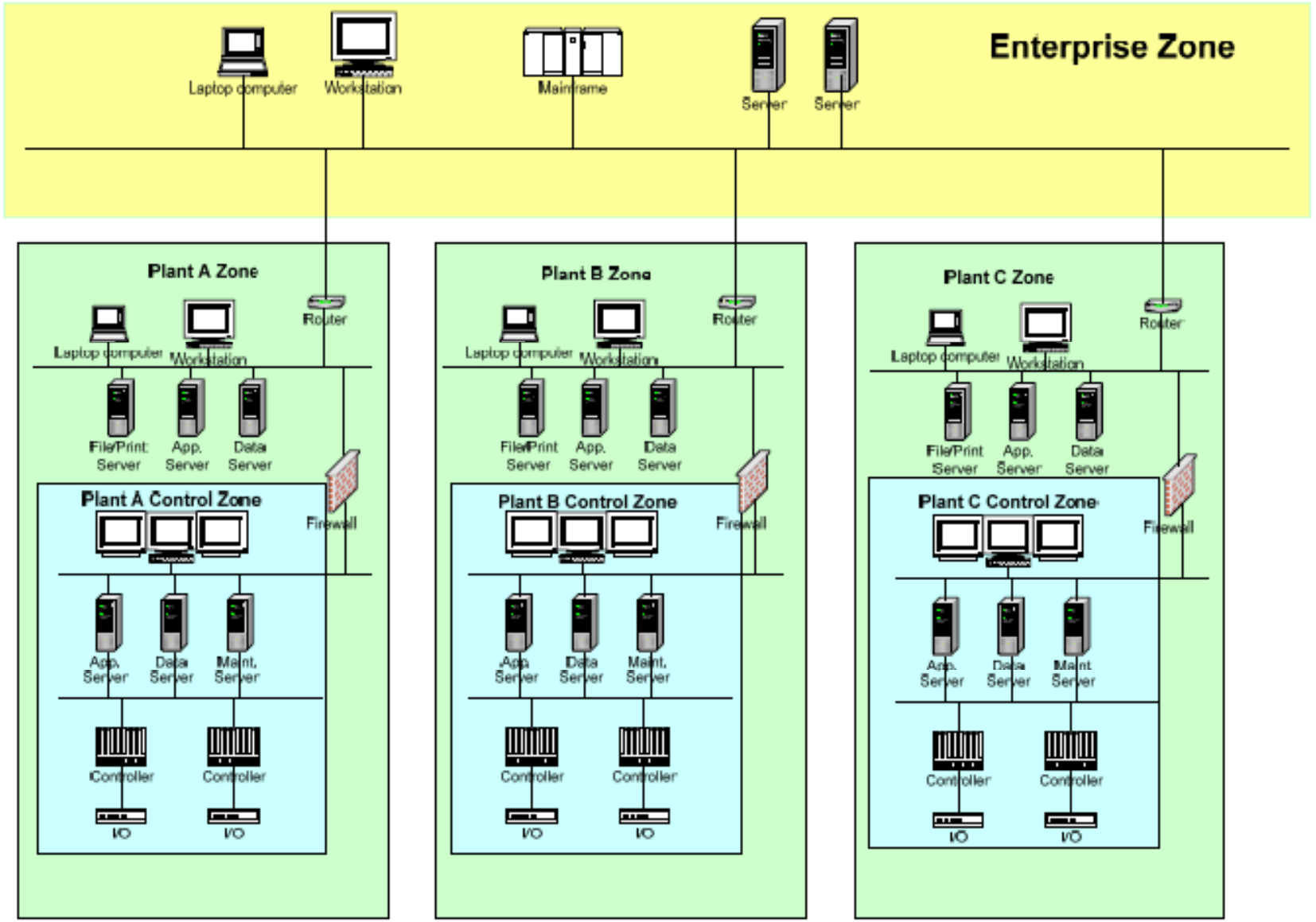


Figure 17 – Multiplant Zone Example

6.5 Zone & Conduit Models

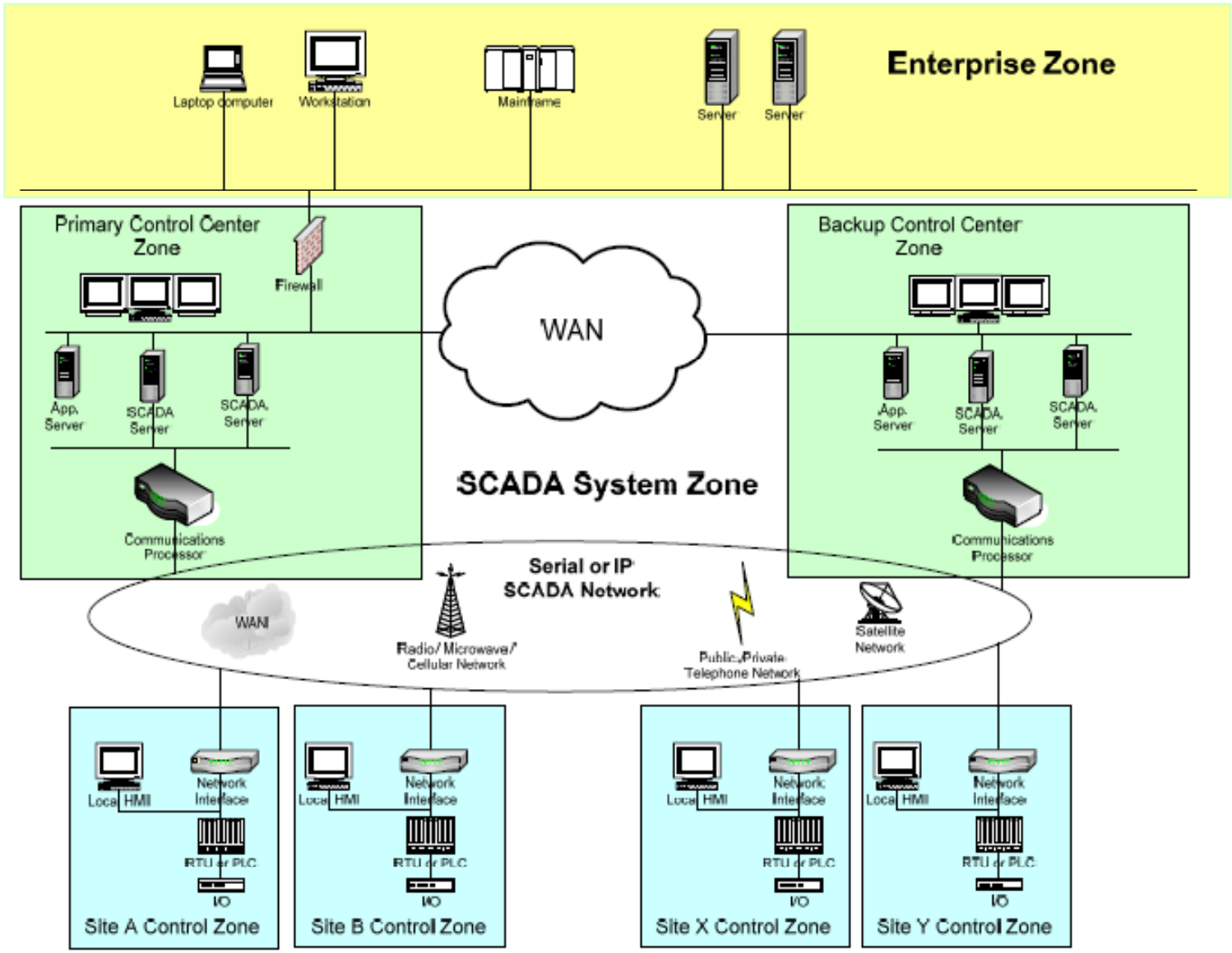


Figure 20 – SCADA Separate Zones Example

Specifying Zones & Conduits

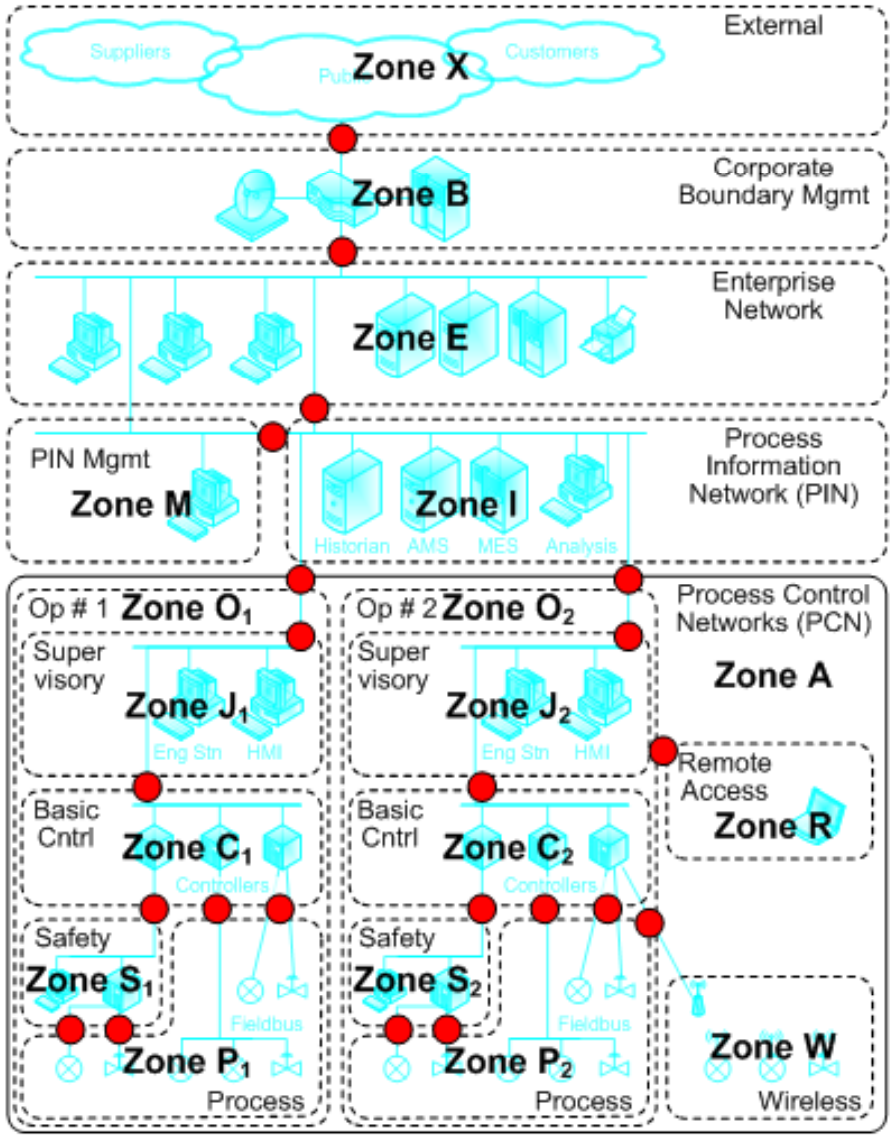


Image courtesy of Byres Security

Honeywell Reference Architecture

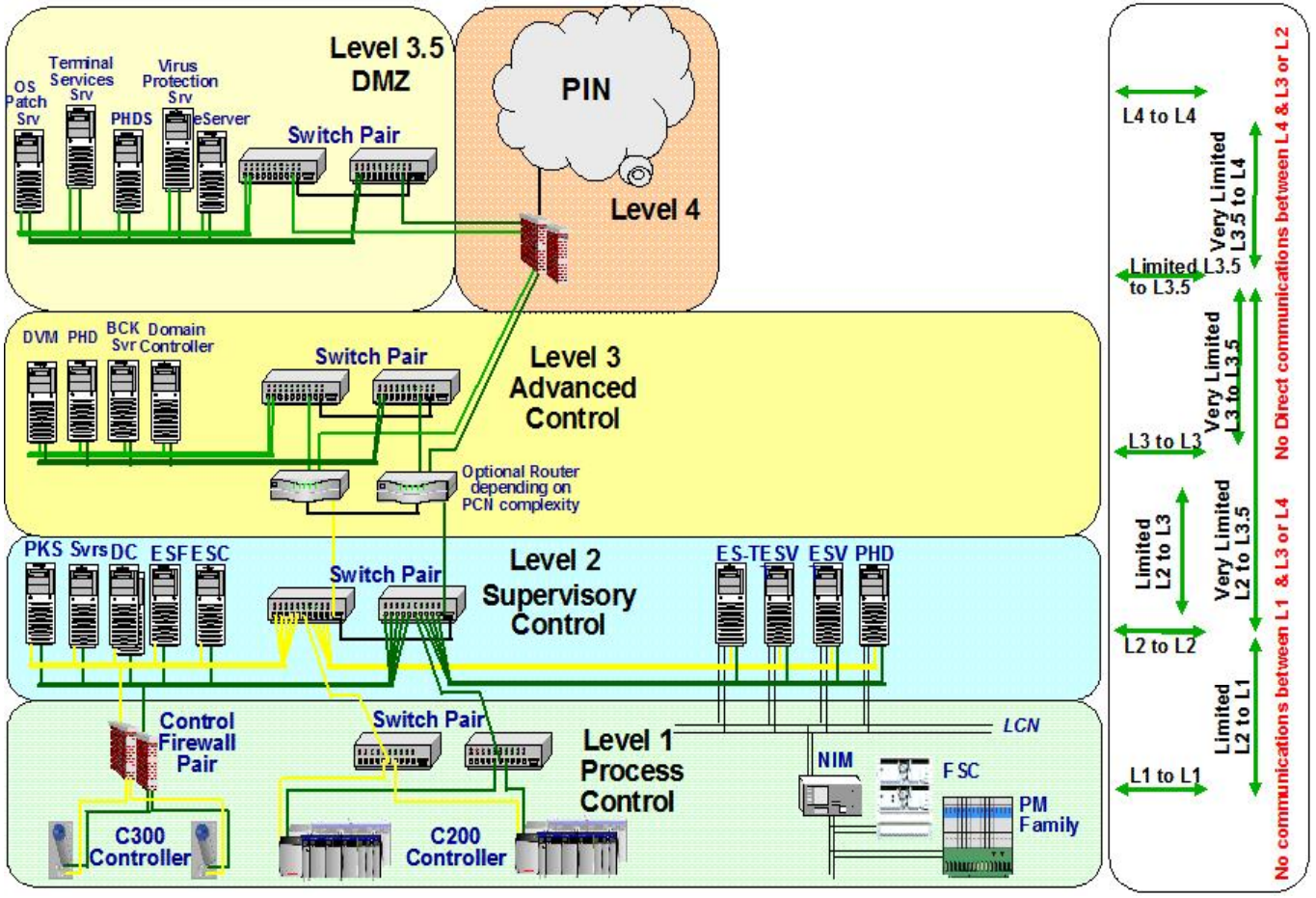
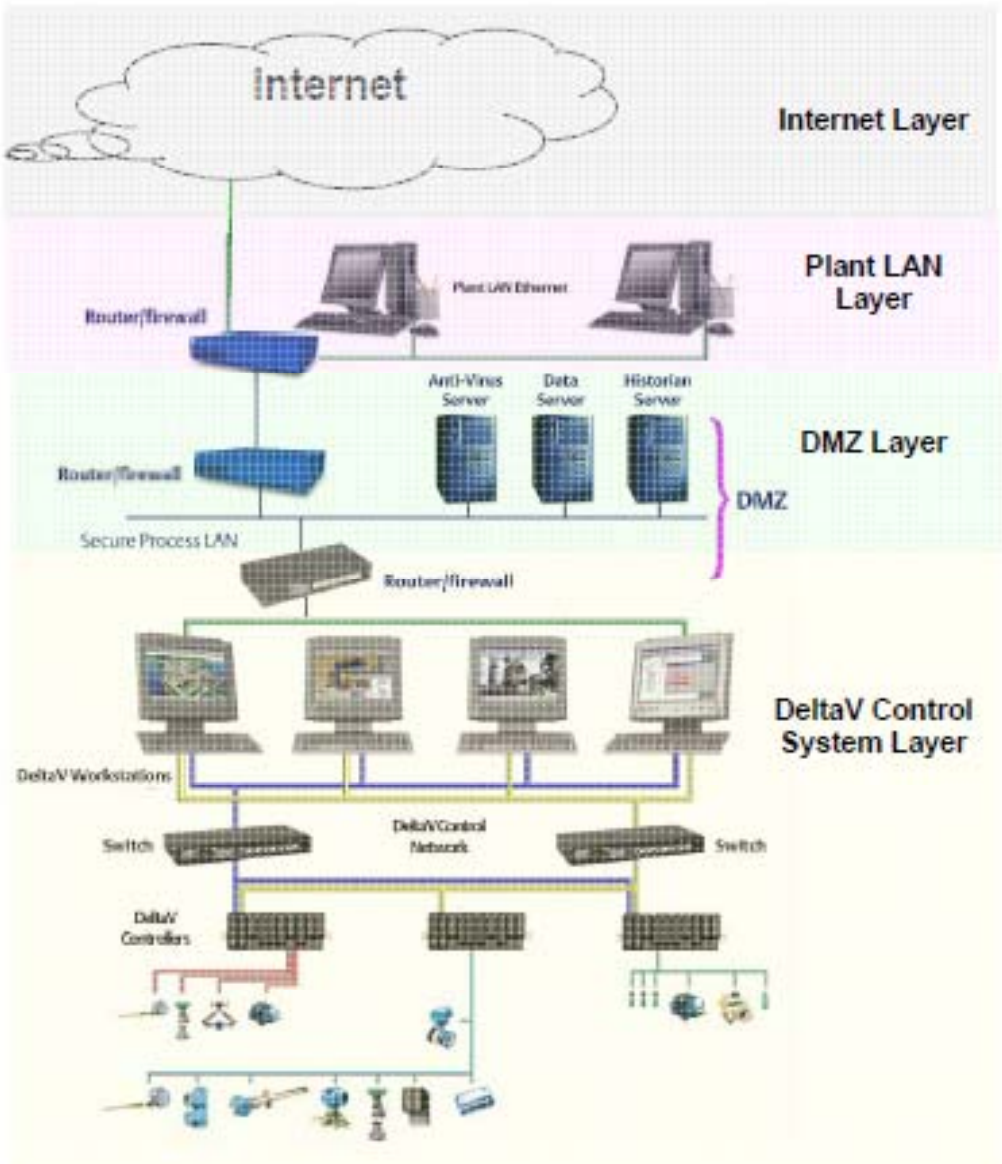


Image Courtesy of Honeywell Process Control

Emerson Reference Architecture



Siemens Reference Architecture

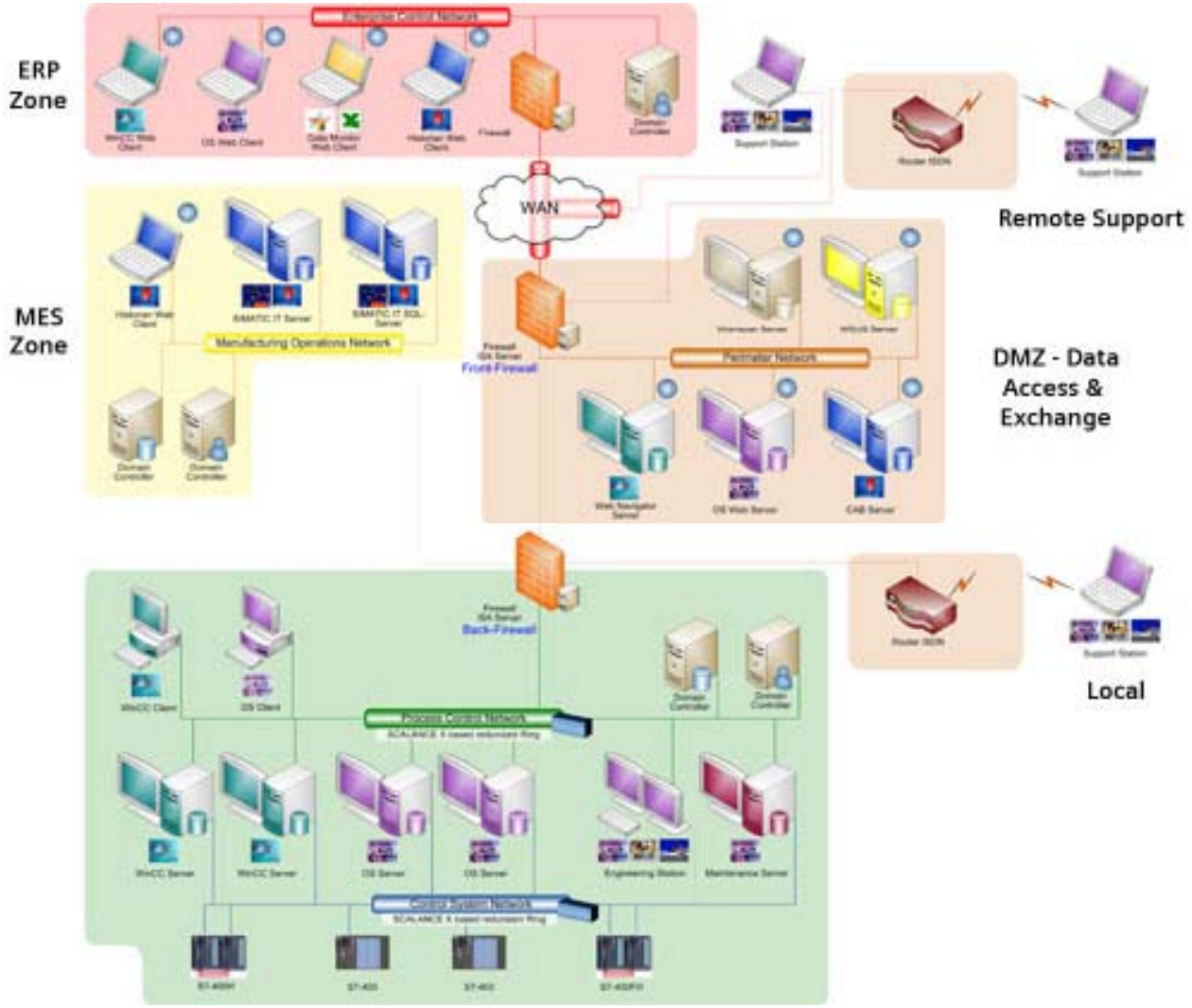


Image Courtesy of Siemens AG

DuPont Reference Architecture

DuPont Reference Architecture

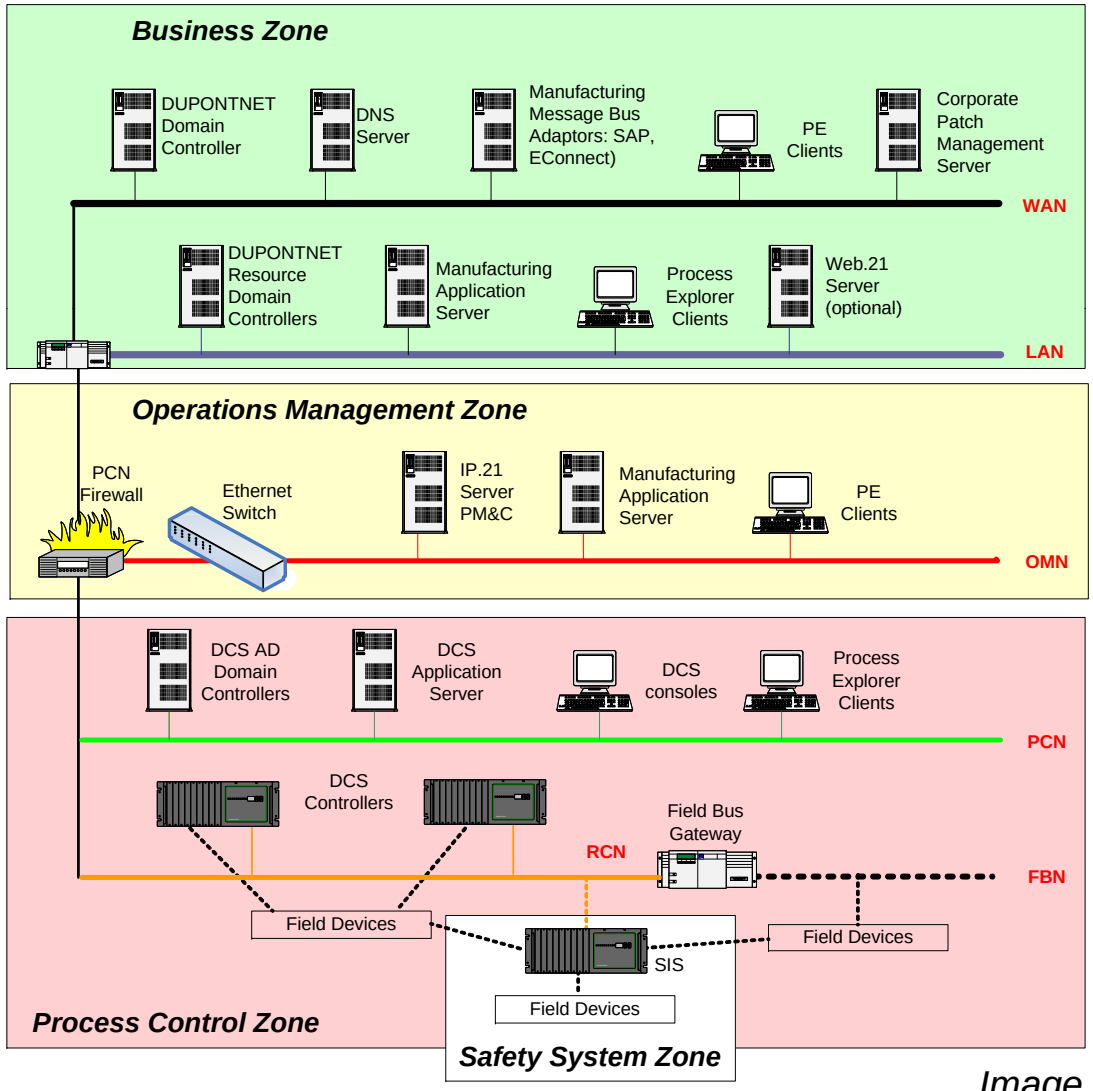


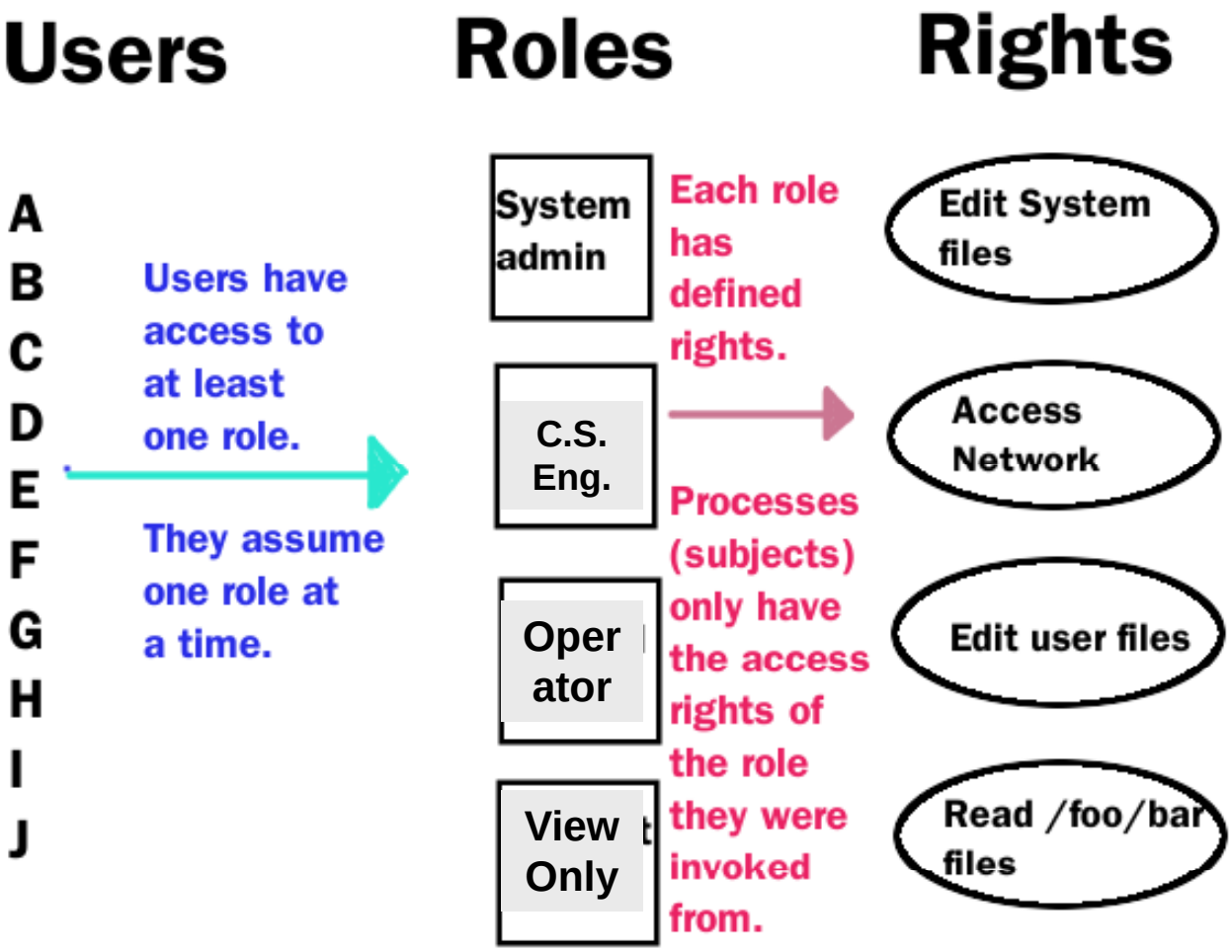
Image Courtesy of DuPont

#5 Control Access to System

- Control and monitor access to control system resources
- Logical & Physical
- AAA
  - Administration
  - Authentication
  - Authorization
- Review
  - Who has access?
  - To what resources?
  - With what privileges?
  - How is it enforced?

- Zone-by-zone
  - Asset-by-Asset
    - Role-by-Role
      - Person-by-Person

Role-based Access Control



#6 Harden System Components

- Remove or disable unused communication ports
- Remove unnecessary applications and services
- Apply patches when and where possible
- Consider ‘whitelisting’ tools
- Use ISASecure™ certified products

Port locking devices

Ethernet RJ-45

- Tamper-proof outlet lock and lockable patch cord
- Protects against unauthorized port access in unused outlets
- Deters patch cord removal
- Removable only with a specially designed key

Siemon LockIT™

USB

- USB lock physically locks and blocks the USB Ports.
- Allows secured use of an authorized USB device by capturing the device's cable and locking it into the USB port

Kensington USB Port Lock

Patch Management

- Prioritized and categorize all machines into groups that define when and how they are to be patched. Example:
  - "Early Adopters" receive patches as soon as available and act as Test/Quality Assurance machines.
  - "No Touch" machines require manual intervention and/or detailed vendor consultation.
- Establish a procedure for keeping track of new patches and level of importance to control operations.

Patch Management

- When new vulnerability is announced and/or a patch fix is available, conduct a PDA to evaluate the potential impact on the control system
- This patch is then evaluated and prioritized for adoption based on its risk evaluation.

Reaction Plan	Aggressiveness	Implementation Window	Level of Testing
Alpha	Minimum	Quarterly	High
Bravo	Moderate	By end of following week	Best Effort
Zebra	Maximum	Within 48 hours	Minimal

Application Whitelisting

- Unlike antivirus solutions, that rely on blacklists of known malware, whitelisting enforces a relatively small list of the authorized applications for each computer
- Automatically blocks all unauthorized applications including unknown malware and rogue applications installed by users.
- Minimal performance impact
- Examples:
  - Core Trace Bouncer
  - Industrial Defender HIPS

Stuxnet Response

"Addressing Stuxnet goes beyond using quality security controls. The industry needs to demand higher quality software that is free from defects. Companies who develop products and write code need to continue to mature their development processes to become more secure."

Mark Weatherford

Vice president and Chief Security Officer

NERC

ISASecure
Embedded Device Security Certification

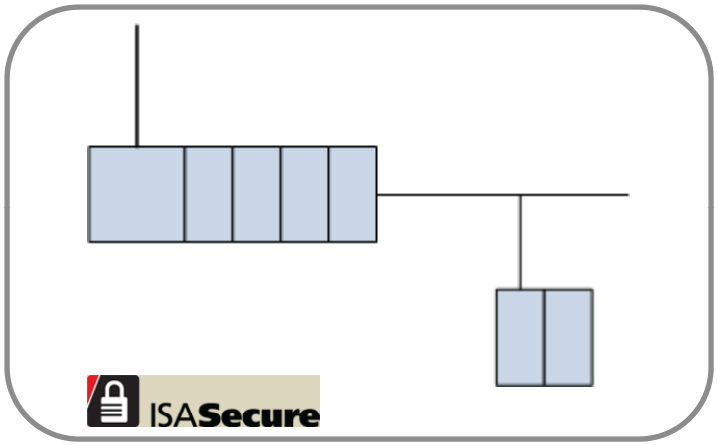
ISA Security Compliance Institute

ISASecure

Software Development Security Assurance (SDSA)

Functional Security Assessment (FSA)

Communications Robustness Testing (CRT)



ISASecure Certification Process

1. CRT test all accessible TCP/IP interfaces
2. Perform FSA on device and all interfaces
3. Audit supplier's software development process
4. Perform integrated threat analysis
5. Issue certification

For more information visit: www.isasecure.org

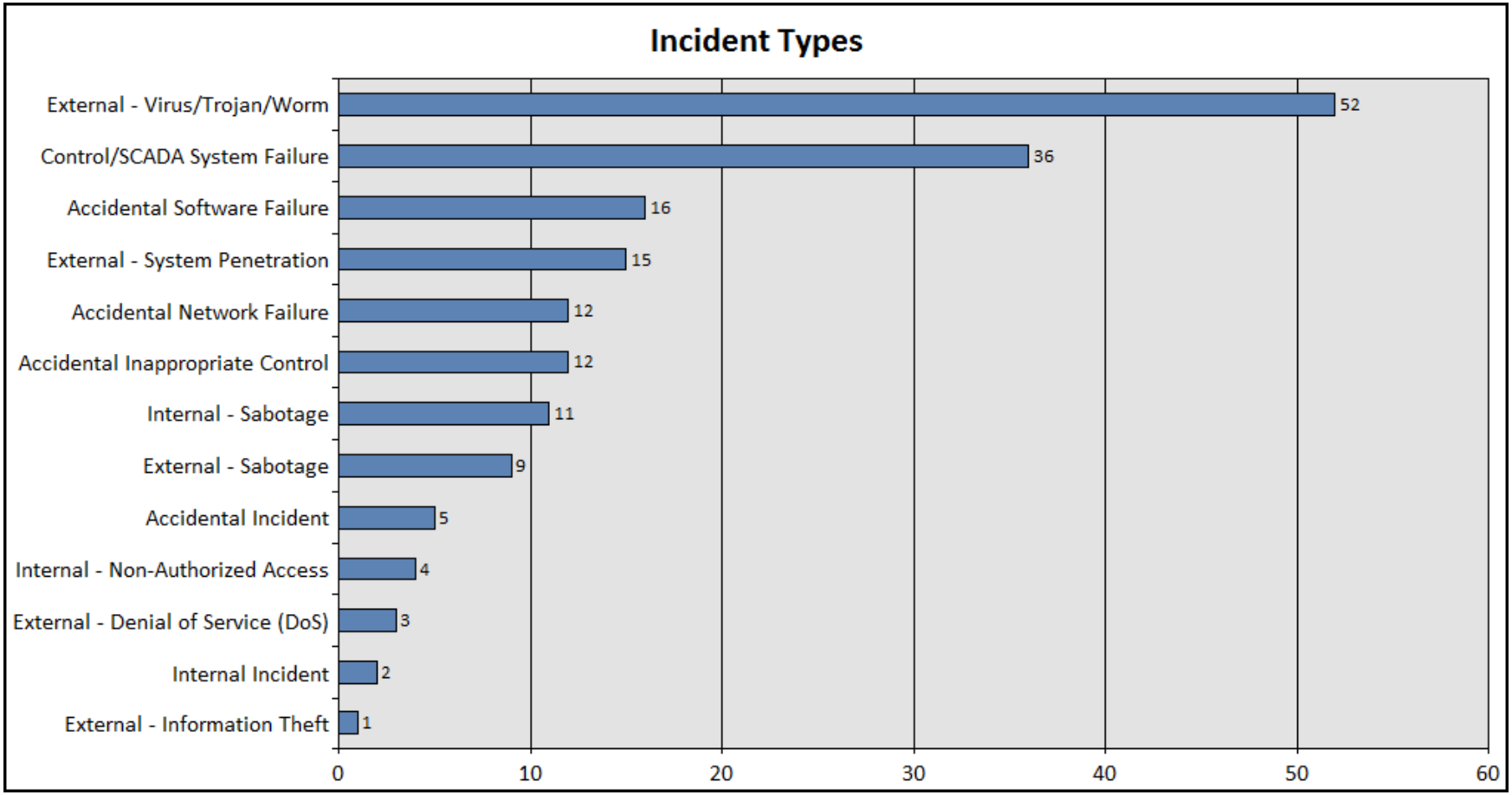
#7 Monitor & Maintain

- Install vendor recommended anti-virus and update signatures regularly
- Review system logs periodically
- Consider Intrusion Detection (IDS) or Host Intrusion Prevention (HIPS)
- Pen testing (offline only)
- Periodic assessments

"I hope I'm not intruding..."

Anti-virus Management

Stuxnet is not the first malware to infect industrial control systems



Malware

The intrusion of malware can result in:

- Performance degradation
- Loss of system availability
- The capture, modification, or deletion of data

…and since Stuxnet

- Loss of control

Mitigation Steps

- Ensure that virus protection and Microsoft security hot fixes are up to date on all nodes in your process control network and the systems connected to it
- Ensure that there are no email clients on any nodes of your process control network
- Use a firewall and DMZ for the business network to process control network interface

THE 7 THINGS

1. Assess Existing Systems
2. Document Policies & Procedures
3. Train Personnel & Contractors
4. Segment the Control System Network
5. Control Access to the System
6. Harden the Components of the System
7. Monitor & Maintain System Security

DCS Virus Infection, Investigation and Response

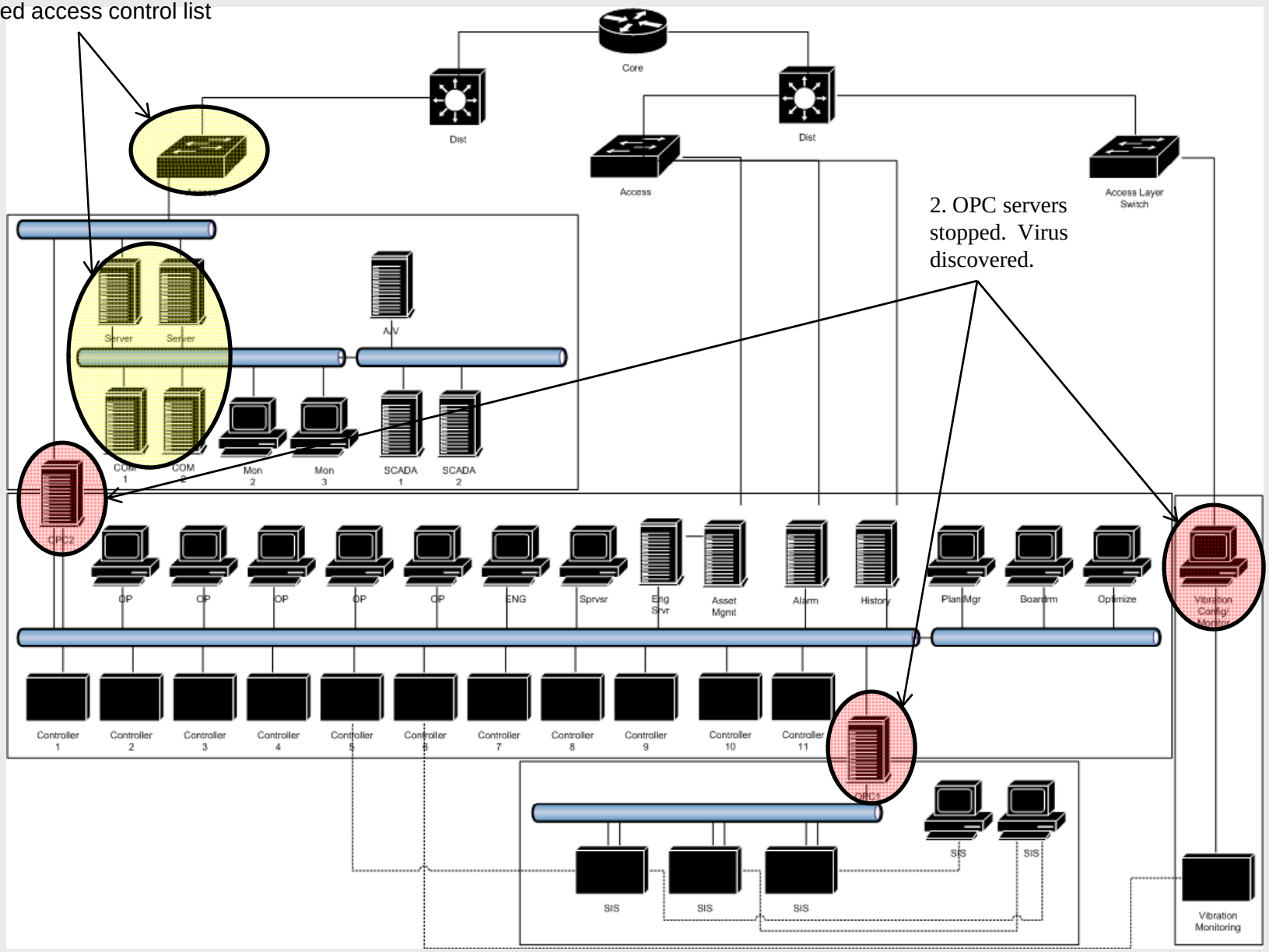
A Case Study

Incident

- December 2009
- Petrochemical company in South Africa
- Virus (Win32/Sality) infected DCS system
- Two OPC servers shutdown
- Operators ran plant partially blind for 8 hours
- Engineers rebuild servers
- Recovered without loss of production

Scenario

1.) Replaced servers and updated access control list



Win32/Sality Virus

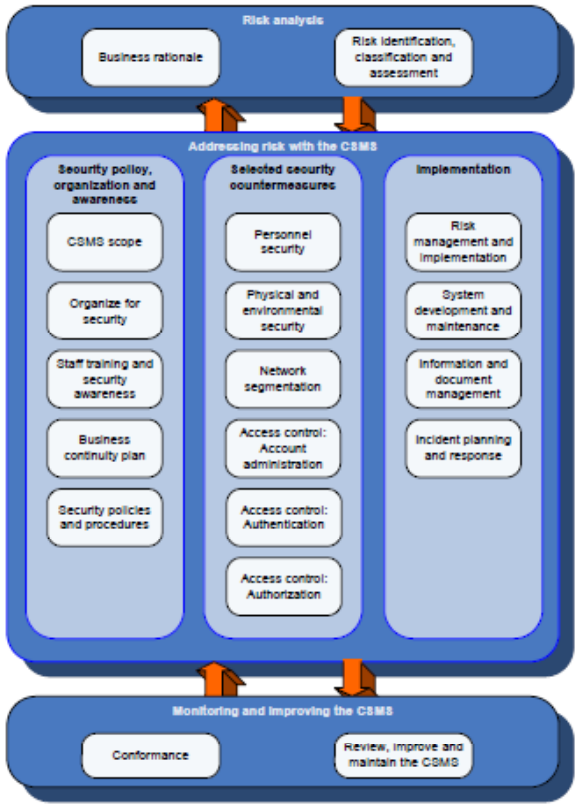
- Discovered: April 18, 2009
- A worm that spreads by infecting executable files and copying itself to removable drives
- Deletes files with .vdb, .avc and .key in the filename and also files listed under certain registry subkeys
- Ends processes and lowers secur modifying the registry

Response

- Conducted a root-cause investigation
- Implemented policy & procedural changes
  - Configuration management policy for IT switches
  - 3rd party software policy
  - Anti-virus management policy
  - Prohibited remote access
  - Portable media policy
- Hired third-party SME to perform a thorough control system security assessment
  - Familiar with DCS, SIS and SCADA systems
  - Knowledgeable of latest standards & technology
  - Experience in similar plants
  - Unbiased

The Project

- exida hired to perform control system security assessment
- Aug 23 – Aug 27, 2010
- Followed ANSI/ISA 99.02.01

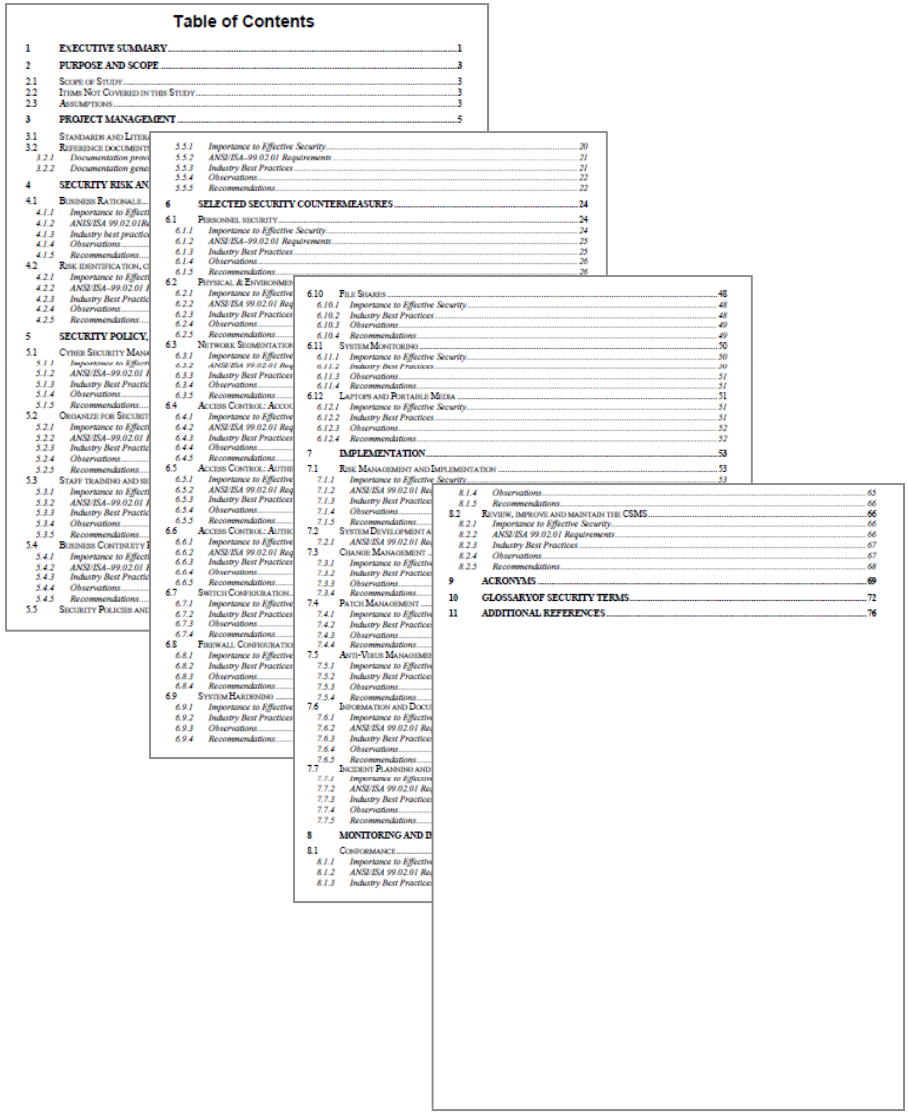


Assessment Process

1. Understand and scope the system under assessment
2. Develop a clear understanding of the network architecture and all traffic flows
3. Develop an inventory of all networked control devices within the boundary of the system
4. Perform device level assessment
5. Interview key employees involved in operations and security of the control networks and equipment
6. Analyze collected data and compare with corporate standards and industry best practices to identify gaps
7. Recommend solutions to close identified gaps

Results

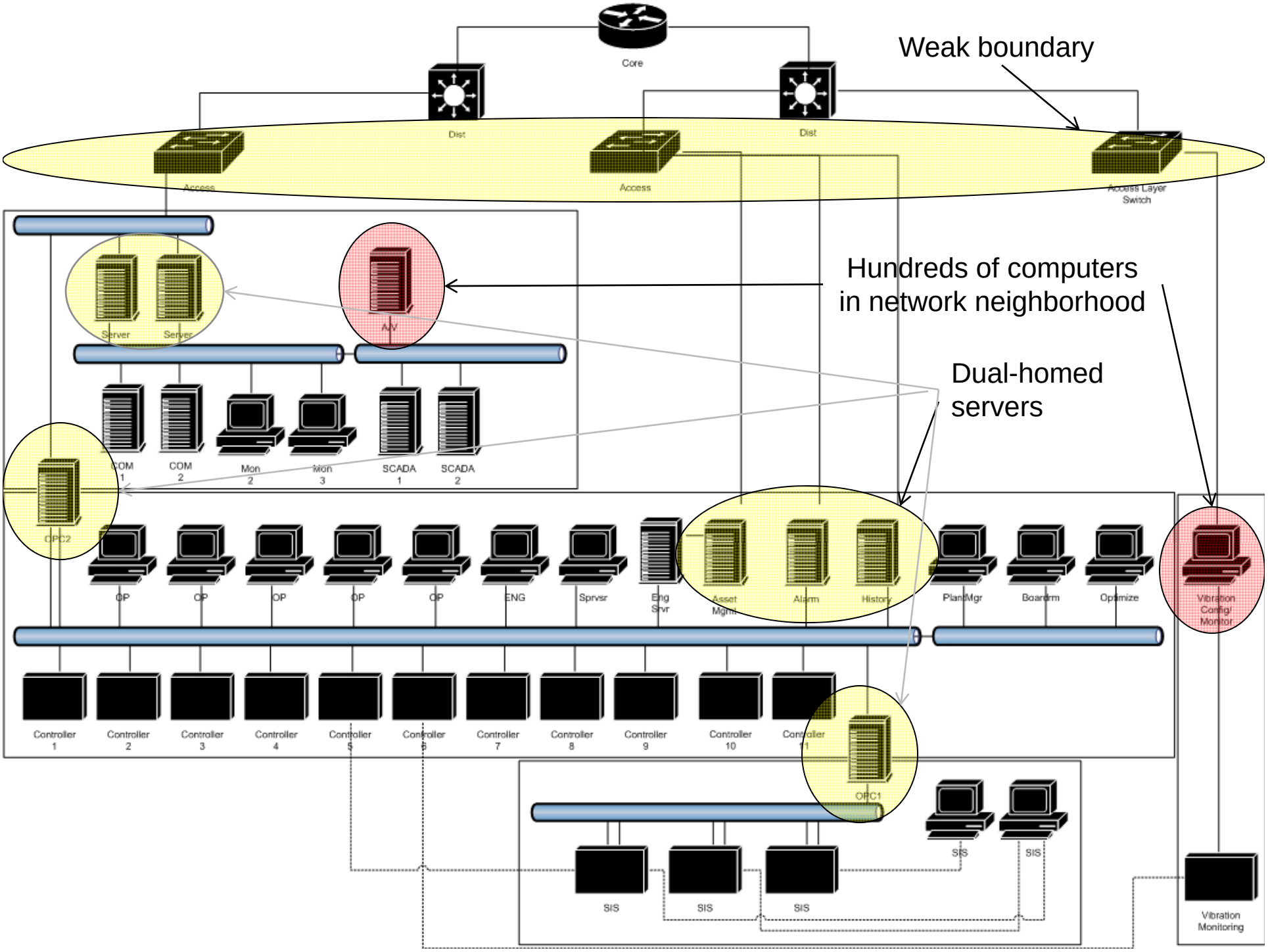
- For each item in ISA 99.02.01
  - Requirements
  - Importance to effective security
  - Industry best practices
  - Observations
  - Recommendations
- 48 recommendations
- 9 critical recommendations



Network Segmentation

Observations:

- Network connections not well documented
- Insufficient separation between business LAN and control system (VLANS & ACL's)
- Boundaries unclear and no boundary devices
- Several computers were found to have hundreds of established network connections
- Several dual-zoned servers


Weak boundary
Hundreds of computers in network neighborhood
Dual-homed servers
Core
Dist
Dist
Access
Access
Access Layer Switch
Server
Server
AJV
COM 1
COM 2
Mon 2
Mon 3
SCADA 1
SCADA 2
OPC2
OP
OP
OP
OP
OP
ENG
Sprvsr
Eng Srvr
Asset Mgmt
Alarm
History
PlantMgr
Boardrm
Optimize
Vibration Config/ Monitor
Controller 1
Controller 2
Controller 3
Controller 4
Controller 5
Controller 6
Controller 7
Controller 8
Controller 9
Controller 10
Controller 11
OPC1
SIS
SIS
SIS
SIS
SIS
Vibration Monitoring

DuPont Reference Architecture

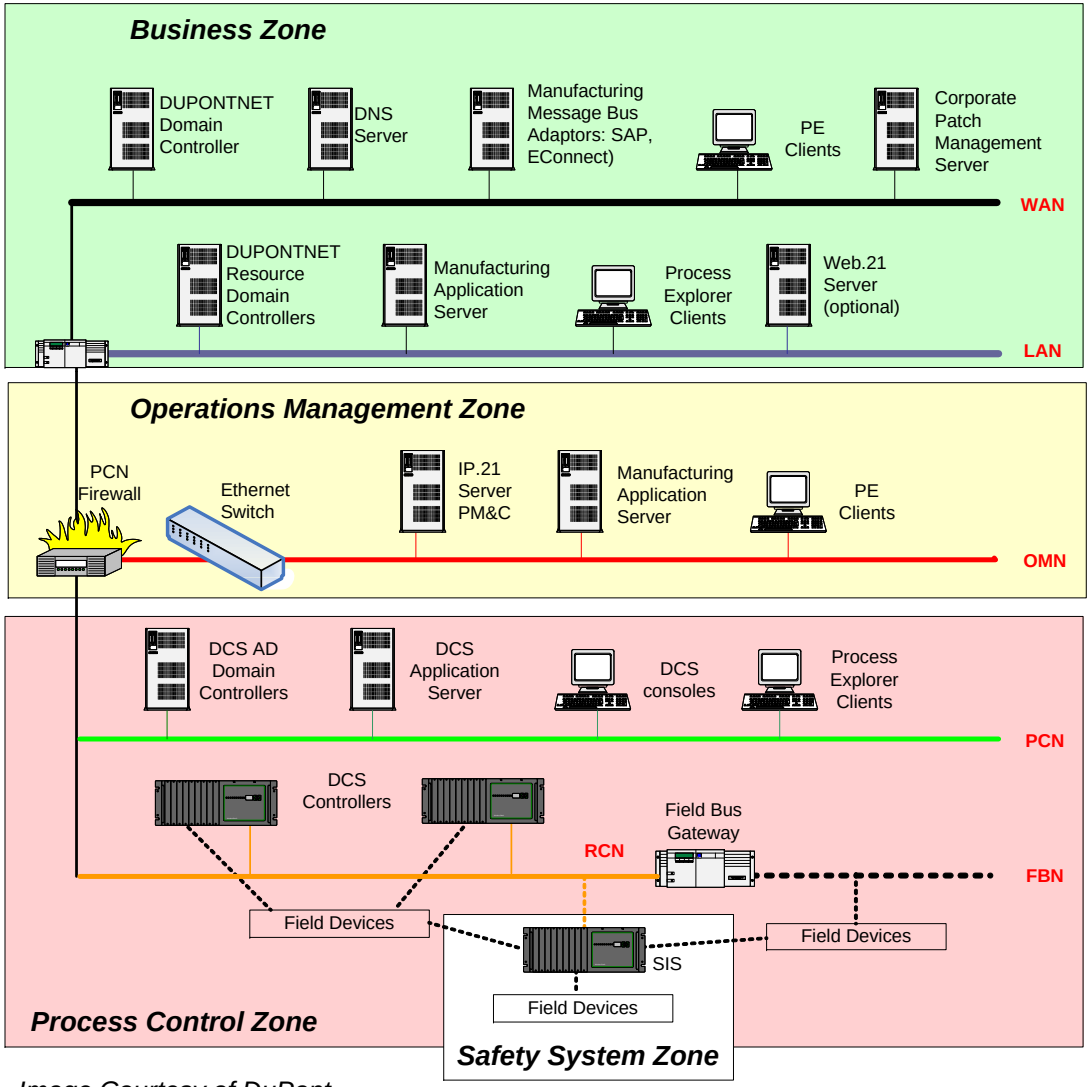
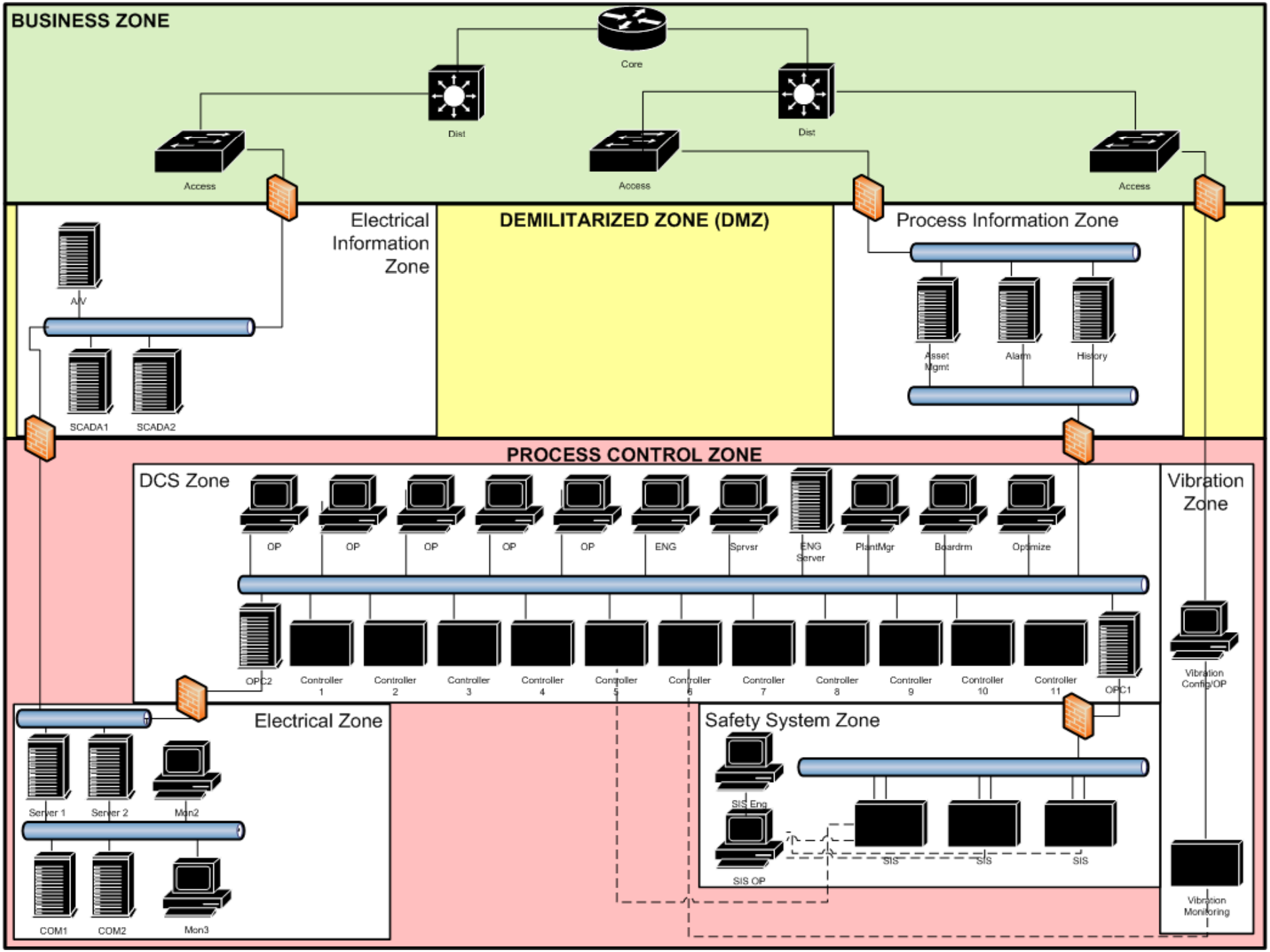


Image Courtesy of DuPont


BUSINESS ZONE
Core
Dist
Dist
Access
Access
Access
Electrical Information Zone
DEMILITARIZED ZONE (DMZ)
Process Information Zone
AMV
SCADA1
SCADA2
Asset Mgmt
Alarm
History
PROCESS CONTROL ZONE
DCS Zone
OP
OP
OP
OP
OP
ENG
Sprvsr
ENG Server
PlantMgr
Boardrm
Optimize
OPC2
Controller 1
Controller 2
Controller 3
Controller 4
Controller 5
Controller 6
Controller 7
Controller 8
Controller 9
Controller 10
Controller 11
OPC1
Vibration Zone
Vibration Config/OP
Vibration Monitoring
Electrical Zone
Server 1
Server 2
Mon2
COM1
COM2
Mon3
Safety System Zone
SIS Eng
SIS OP
SIS
SIS
SIS

System Hardening

Observation

- Workstations extensive number of inappropriate applications
  - UltraVNC
  - Microsoft ActiveSync
  - Internet Explorer
  - Microsoft Outlook / Outlook Express
  - Windows NetMeeting
  - Internet checkers game
  - Remote access phonebook
- Numerous files shares configured

Recommendation

- Remove all unnecessary applications and services
- Apply the vendor recommended or NIST hardening settings to all workstations and servers
- Immediately remove any unnecessary shares

System Hardening

Observation

- Numerous active, unused Ethernet ports
- USB ports disabled by registry setting

Recommendation

- Disable or lock any unused ports
- Use physical devices to lock cables into used ports and block access to unused ports

Lessons Learned

Client

- Network segmentation is critical
- Anti-virus used per supplier recommendations
- Portable media is dangerous
- Awareness/training is important
- Systems should be hardened and patched per supplier recommendations

Assessor

- ANSI/ISA 99.02.01 provides good structure but cannot be used as a checklist
- Zone and conduit modeling works
- Supplier's reference architectures need to be adjusted for "real" applications
- Data collection must be performed very carefully on a live control system

Next Steps

- Client is developing corporate policies and procedures
- Client is preparing to deploy recommended network changes
- Role-based security training is being developed and integrated into existing training program
- Monitoring technology (e.g. IDS, HIPS) being investigated
- Access control (logical and physical) being reviewed
- System hardening being implemented with supplier support
- Additional units and sites will be assessed

Key Takeaways

- ‘Security’ is a key component in control system reliability
- The threats to control system security are real and becoming more sophisticated
- Excellent standards and best practices are available assist users in securing their systems
- Automation equipment suppliers play an important role
- Assessment is the first step

This presentation is available on www.exida.com and www.slideshare.com