

DCS Virus Infection, Investigation and Response

A Case Study



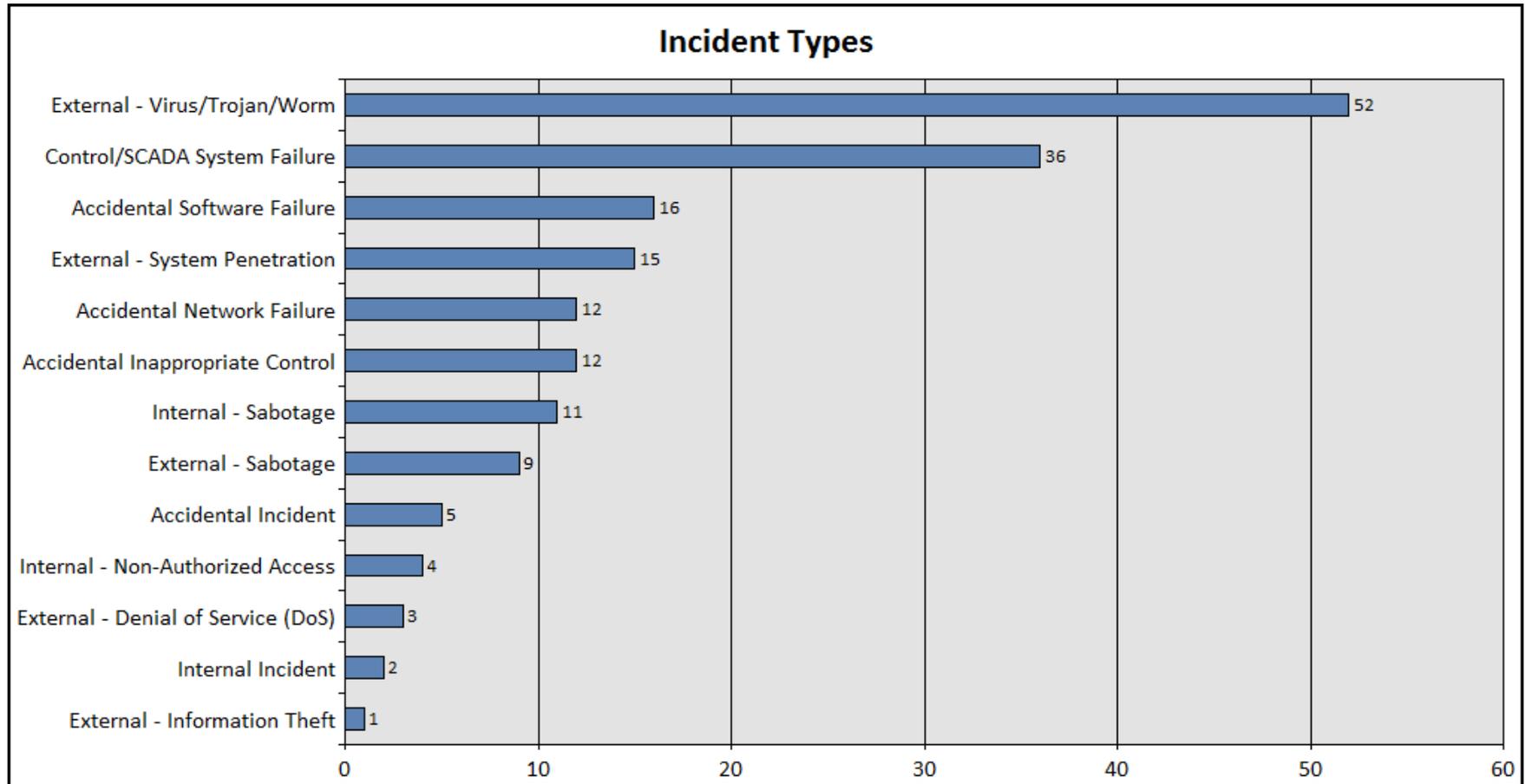
- We help our clients improve the safety, security and availability of their automation systems



Agenda

- Introduction
- Incident
- Response
- Assessment
- Lessons Learned
- Next Steps

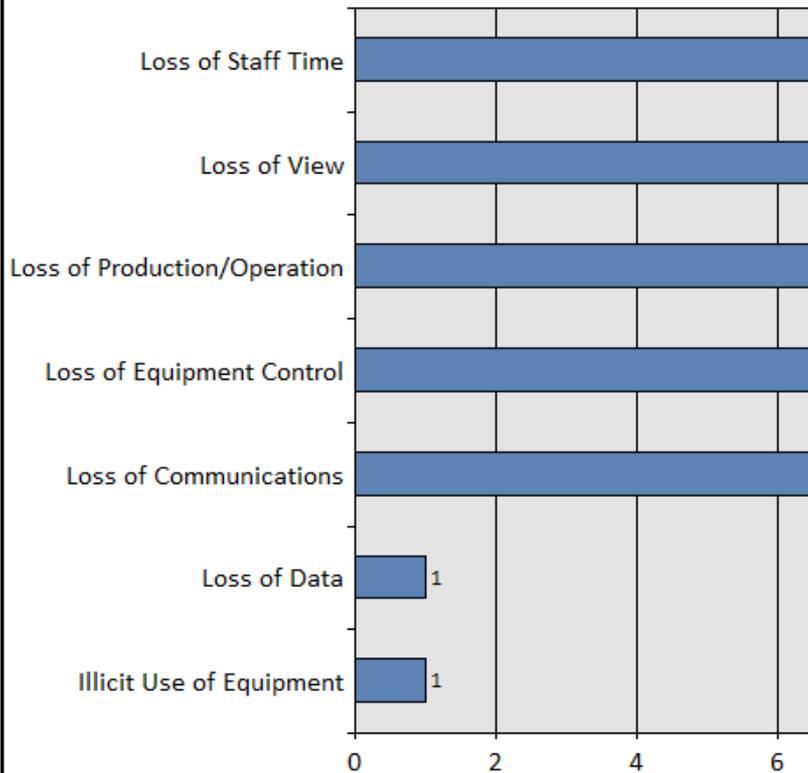
Stuxnet is not the first malware to infect ICS



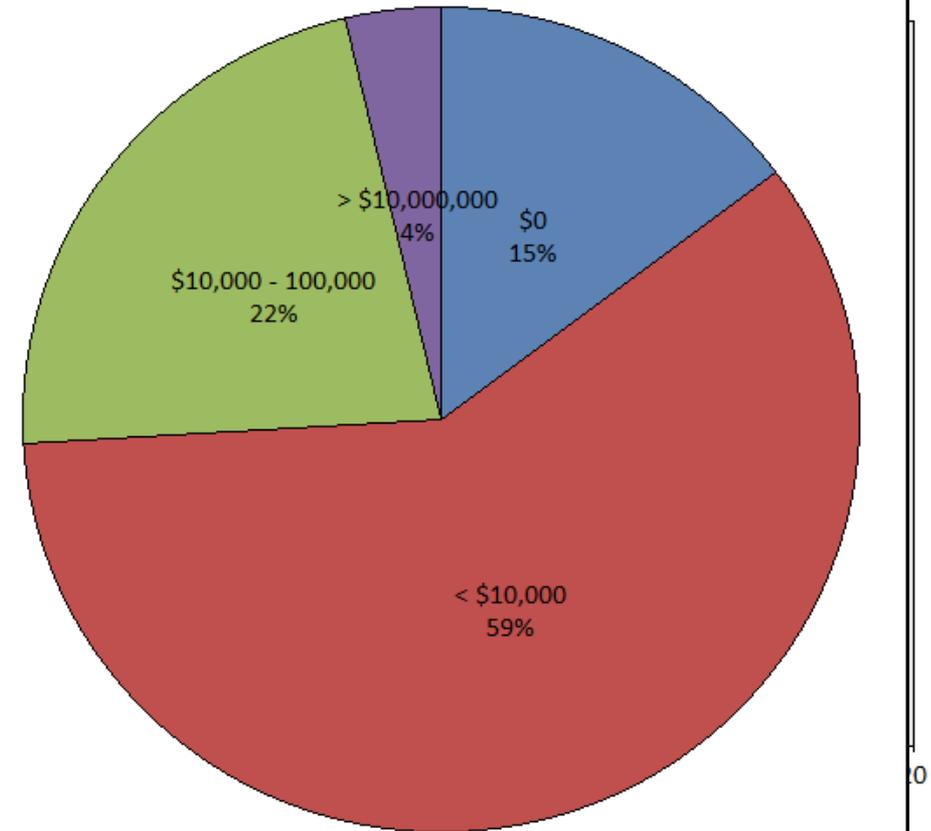
© 2010 Security Incidents Organization, The Repository of Industrial Security Incidents (RISI) database

Impact of Malware in ICS

Impact of



Financial Impact



© 2010 Security Incidents Organization, The Repository of Industrial Security Incidents (RISI) database

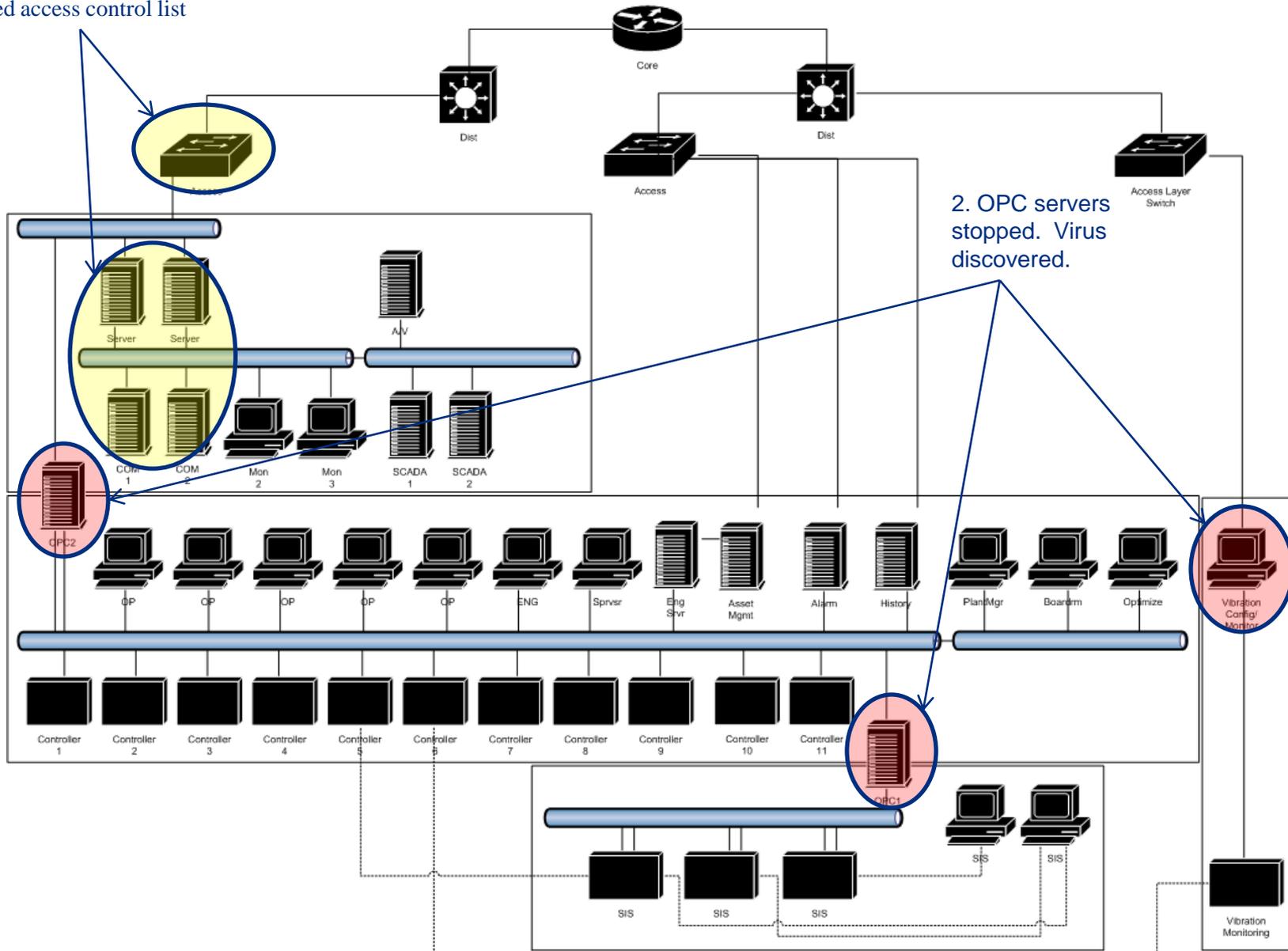
Incident

- 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

2. OPC servers stopped. Virus discovered.



Win32/Sality Virus

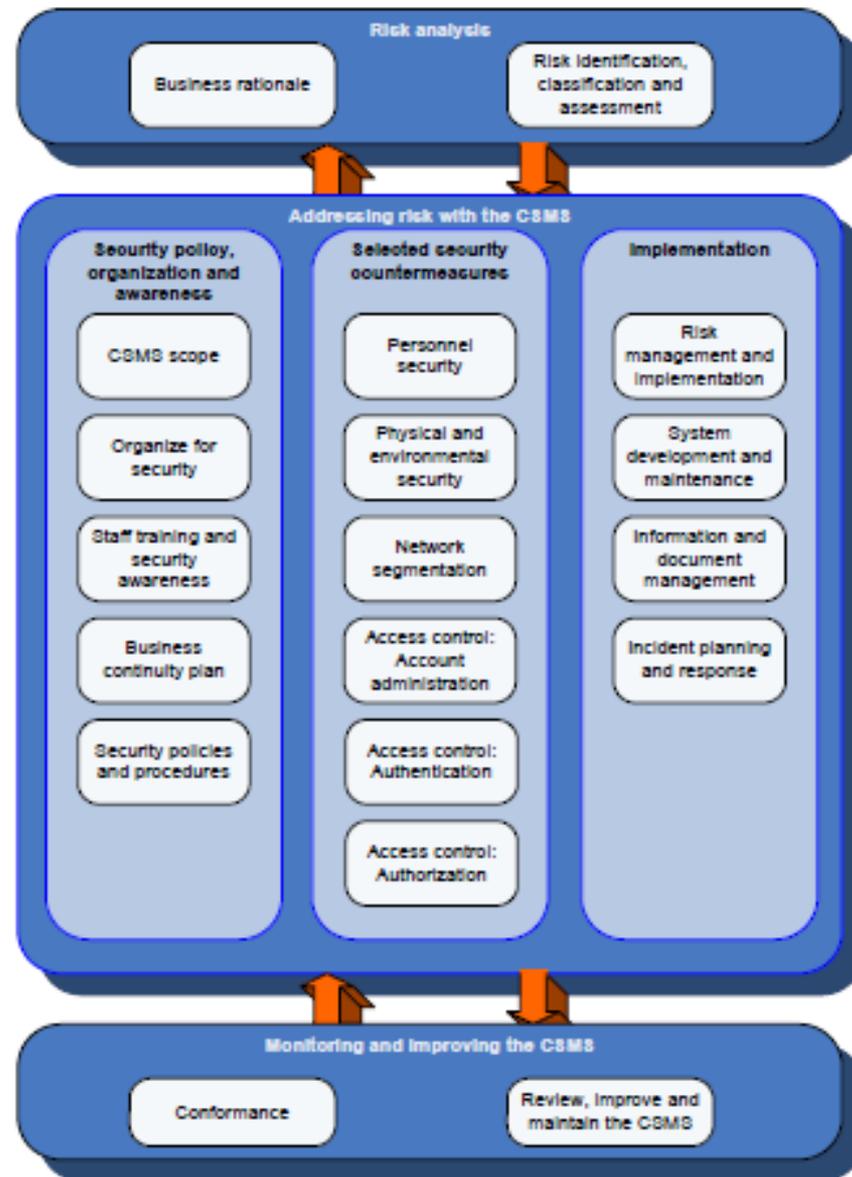
- Discovered: April 18, 2009
- A worm that spreads by infecting executable files and copying itself to removable drives
- Deletes files with .vdb, .avc and .key in the filename and also files listed under certain registry subkeys
- Ends processes and lowers security settings by modifying the registry



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

- exida hi
assessr
- Aug 23
- Followe



ecurity

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

1	EXECUTIVE SUMMARY	1
2	PURPOSE AND SCOPE	3
2.1	SCOPE OF STUDY	3
2.2	ITEMS NOT COVERED IN THIS STUDY	3
2.3	ASSUMPTIONS	3
3	PROJECT MANAGEMENT	5
3.1	STANDARDS AND LITERATURE DOCUMENTS	20
3.2	Documentation provided	21
3.2.1	Documentation provided	21
3.2.2	Documentation gaps	22
4	SECURITY RISK ANALYSIS	22
4.1	BUSINESS RATIONALIZATION	24
4.1.1	Importance to Effective Security	24
4.1.2	ANSI/ISA 99.02.01 Req	24
4.1.3	Industry Best Practices	25
4.1.4	Observations	25
4.1.5	Recommendations	26
4.2	RISK IDENTIFICATION, CLASSIFICATION, AND MITIGATION	26
4.2.1	Importance to Effective Security	26
4.2.2	ANSI/ISA 99.02.01 Req	26
4.2.3	Industry Best Practices	26
4.2.4	Observations	26
4.2.5	Recommendations	26
5	SECURITY POLICY	26
5.1	CYBER SECURITY MANAGEMENT	26
5.1.1	Importance to Effective Security	26
5.1.2	ANSI/ISA 99.02.01 Req	26
5.1.3	Industry Best Practices	26
5.1.4	Observations	26
5.1.5	Recommendations	26
5.2	ORGANIZE FOR SECURITY	26
5.2.1	Importance to Effective Security	26
5.2.2	ANSI/ISA 99.02.01 Req	26
5.2.3	Industry Best Practices	26
5.2.4	Observations	26
5.2.5	Recommendations	26
5.3	STAFF TRAINING AND RESOURCES	26
5.3.1	Importance to Effective Security	26
5.3.2	ANSI/ISA 99.02.01 Req	26
5.3.3	Industry Best Practices	26
5.3.4	Observations	26
5.3.5	Recommendations	26
5.4	BUSINESS CONTINUITY	26
5.4.1	Importance to Effective Security	26
5.4.2	ANSI/ISA 99.02.01 Req	26
5.4.3	Industry Best Practices	26
5.4.4	Observations	26
5.4.5	Recommendations	26
5.5	SECURITY PRACTICES AND PROCEDURES	26
5.5.1	Importance to Effective Security	26
5.5.2	ANSI/ISA 99.02.01 Req	26
5.5.3	Industry Best Practices	26
5.5.4	Observations	26
5.5.5	Recommendations	26
6	SELECTED SECURITY COUNTERMEASURES	24
6.1	PERSONNEL SECURITY	24
6.1.1	Importance to Effective Security	24
6.1.2	ANSI/ISA 99.02.01 Req	24
6.1.3	Industry Best Practices	25
6.1.4	Observations	26
6.1.5	Recommendations	26
6.2	PHYSICAL & ENVIRONMENTAL SECURITY	26
6.2.1	Importance to Effective Security	26
6.2.2	ANSI/ISA 99.02.01 Req	26
6.2.3	Industry Best Practices	26
6.2.4	Observations	26
6.2.5	Recommendations	26
6.3	NETWORK SEGMENTATION	26
6.3.1	Importance to Effective Security	26
6.3.2	ANSI/ISA 99.02.01 Req	26
6.3.3	Industry Best Practices	26
6.3.4	Observations	26
6.3.5	Recommendations	26
6.4	ACCESS CONTROL: ACCESS	26
6.4.1	Importance to Effective Security	26
6.4.2	ANSI/ISA 99.02.01 Req	26
6.4.3	Industry Best Practices	26
6.4.4	Observations	26
6.4.5	Recommendations	26
6.5	ACCESS CONTROL: AUTH	26
6.5.1	Importance to Effective Security	26
6.5.2	ANSI/ISA 99.02.01 Req	26
6.5.3	Industry Best Practices	26
6.5.4	Observations	26
6.5.5	Recommendations	26
6.6	ACCESS CONTROL: AUTHZ	26
6.6.1	Importance to Effective Security	26
6.6.2	ANSI/ISA 99.02.01 Req	26
6.6.3	Industry Best Practices	26
6.6.4	Observations	26
6.6.5	Recommendations	26
6.7	SWITCH CONFIGURATION	26
6.7.1	Importance to Effective Security	26
6.7.2	Industry Best Practices	26
6.7.3	Observations	26
6.7.4	Recommendations	26
6.8	FIREWALL CONFIGURATION	26
6.8.1	Importance to Effective Security	26
6.8.2	Industry Best Practices	26
6.8.3	Observations	26
6.8.4	Recommendations	26
6.9	SYSTEM HARDENING	26
6.9.1	Importance to Effective Security	26
6.9.2	Industry Best Practices	26
6.9.3	Observations	26
6.9.4	Recommendations	26
6.10	FILE SHARES	48
6.10.1	Importance to Effective Security	48
6.10.2	Industry Best Practices	48
6.10.3	Observations	49
6.10.4	Recommendations	49
6.11	SYSTEM MONITORING	50
6.11.1	Importance to Effective Security	50
6.11.2	Industry Best Practices	50
6.11.3	Observations	51
6.11.4	Recommendations	51
6.12	LAPTOPS AND PORTABLE MEDIA	51
6.12.1	Importance to Effective Security	51
6.12.2	Industry Best Practices	51
6.12.3	Observations	52
6.12.4	Recommendations	52
7	IMPLEMENTATION	53
7.1	RISK MANAGEMENT AND IMPLEMENTATION	53
7.1.1	Importance to Effective Security	53
7.1.2	ANSI/ISA 99.02.01 Req	53
7.1.3	Industry Best Practices	53
7.1.4	Observations	53
7.1.5	Recommendations	53
7.2	SYSTEM DEVELOPMENT	53
7.2.1	Importance to Effective Security	53
7.2.2	ANSI/ISA 99.02.01 Req	53
7.2.3	Industry Best Practices	53
7.2.4	Observations	53
7.2.5	Recommendations	53
7.3	CHANGE MANAGEMENT	53
7.3.1	Importance to Effective Security	53
7.3.2	Industry Best Practices	53
7.3.3	Observations	53
7.3.4	Recommendations	53
7.4	PATCH MANAGEMENT	53
7.4.1	Importance to Effective Security	53
7.4.2	Industry Best Practices	53
7.4.3	Observations	53
7.4.4	Recommendations	53
7.5	ANTI-VIRUS MANAGEMENT	53
7.5.1	Importance to Effective Security	53
7.5.2	Industry Best Practices	53
7.5.3	Observations	53
7.5.4	Recommendations	53
7.6	INFORMATION AND DATA SECURITY	53
7.6.1	Importance to Effective Security	53
7.6.2	ANSI/ISA 99.02.01 Req	53
7.6.3	Industry Best Practices	53
7.6.4	Observations	53
7.6.5	Recommendations	53
7.7	INCIDENT PLANNING AND RESPONSE	53
7.7.1	Importance to Effective Security	53
7.7.2	ANSI/ISA 99.02.01 Req	53
7.7.3	Industry Best Practices	53
7.7.4	Observations	53
7.7.5	Recommendations	53
8	MONITORING AND EVALUATION	53
8.1	CONFORMANCE	53
8.1.1	Importance to Effective Security	53
8.1.2	ANSI/ISA 99.02.01 Req	53
8.1.3	Industry Best Practices	53
8.1.4	Observations	53
8.1.5	Recommendations	53
8.2	REVIEW, IMPROVE AND MAINTAIN THE CSMS	53
8.2.1	Importance to Effective Security	53
8.2.2	ANSI/ISA 99.02.01 Req	53
8.2.3	Industry Best Practices	53
8.2.4	Observations	53
8.2.5	Recommendations	53
9	ACRONYMS	53
10	GLOSSARY OF SECURITY TERMS	72
11	ADDITIONAL REFERENCES	76

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-homed servers

DuPont Reference Architecture

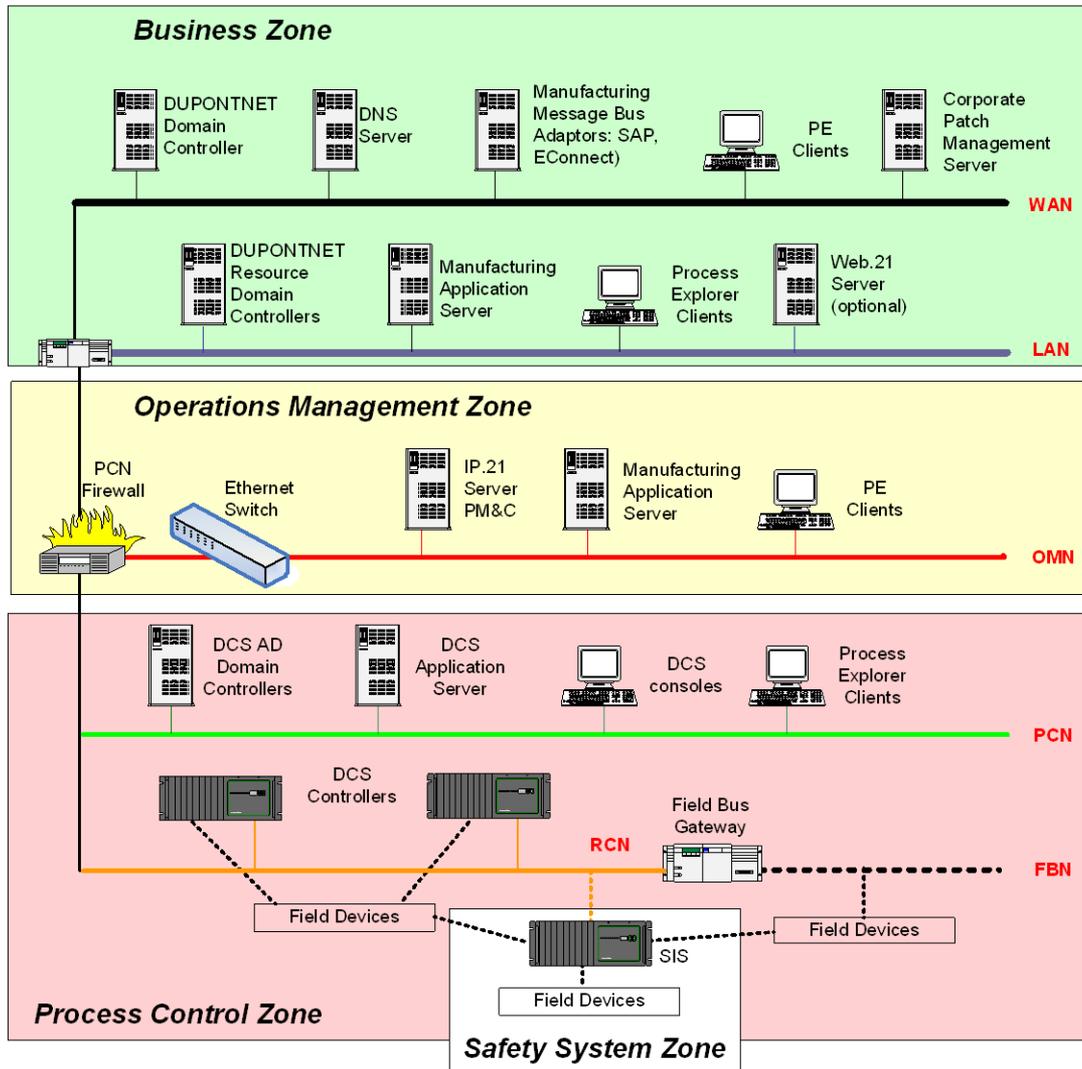
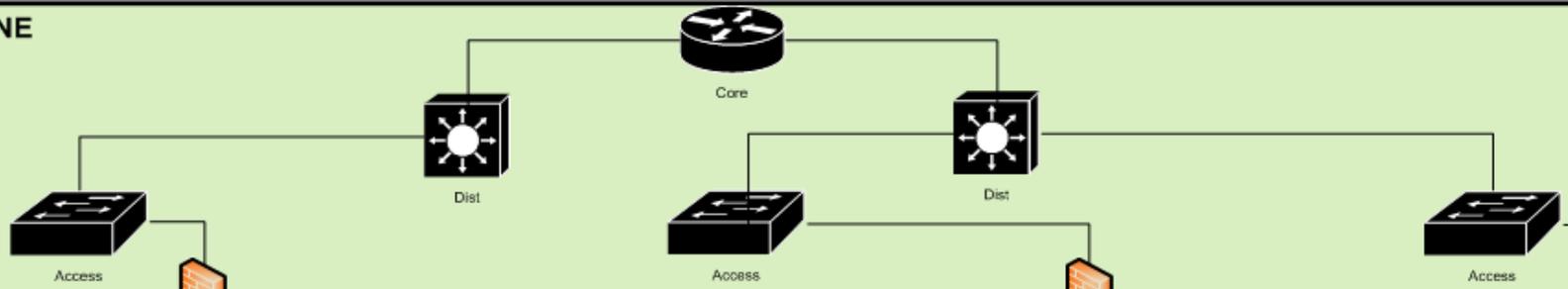
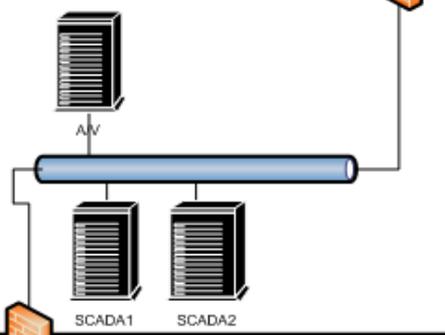


Image Courtesy of DuPont

BUSINESS ZONE

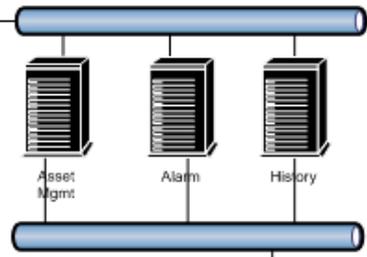


Electrical Information Zone



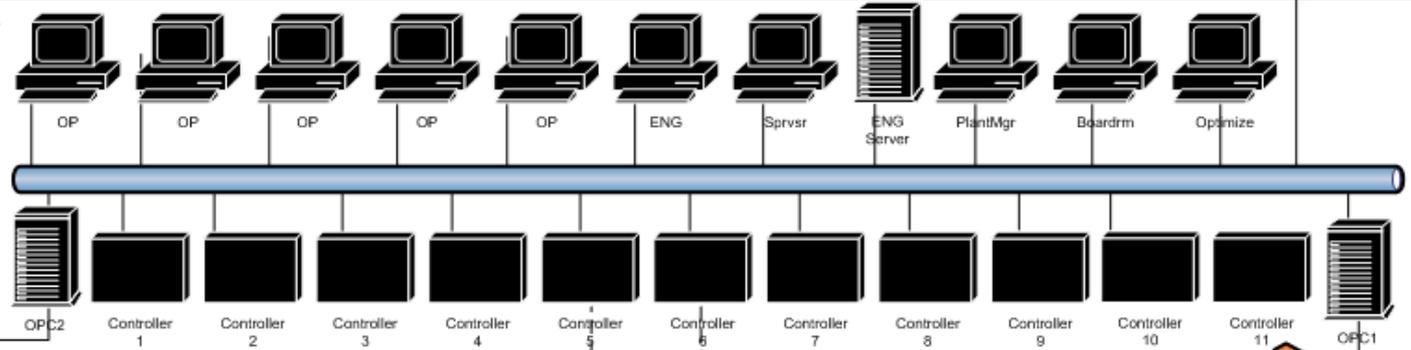
DEMILITARIZED ZONE (DMZ)

Process Information Zone



PROCESS CONTROL ZONE

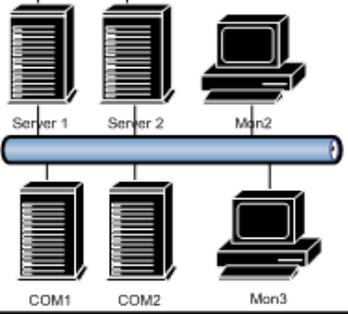
DCS Zone



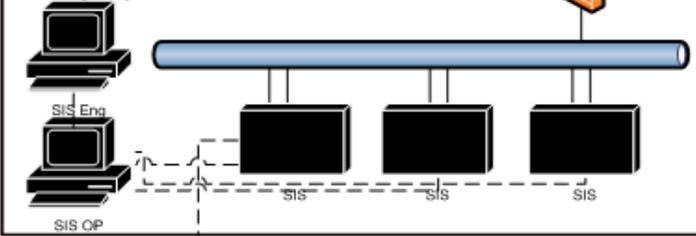
Vibration Zone



Electrical Zone



Safety System Zone



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