IT Security and OT Security

Understanding the Challenges
Security Maturity Evolution in Industrial Control

1950s
Security Maturity Evolution in Industrial Control

- **2003**: Firewalls, Business connectivity, Locks on the Door
- **2005**: Intrusion Detection, Network Based, Known Bad, Industrial Protocols, Alarm Sensors
- **2007**: Event Monitor, Central Logging, Monitor and respond, Alert on Events of interest, Log everything and apply forensics, Incident Management, Flight recorder
- **2009**: Intrusion Prevention, Network Based, Host Based, Deep packet inspection, Known Bad signatures, Known Good Signatures, Whitelisting, System hardening, System locked down
- **2012**: Security Management, Automates manual process, Enforces policy, process & procedures, Leverages "baselines", Manages changes, Audit reporting, Continuous assessments, Attestation data, Doing it and Proving you are doing it

Technology Sophistication
IT Drivers vs. OT Drivers

Real-Time Business Intelligence
- End-to-end business convergence
- Consequences of an incident are potentially greater

Enterprise IT

Automation Systems
OT

Consequences of Cyber Incident
- Economic Impact
- Social Impact

Consequences of Cyber Incident
- Physical Impact
- Economic Impact
- Social Impact
Control Systems Have Unique Architectures

What Needs To Be Protected and Monitored?

- Servers
- HMI's
- Control System Networks
- Network Devices
- PLC’s IED’s RTU’s

Device Interfaces and Communications

- Event / log collection
- IDS / IPS
- Configuration and patch data collection
- Remote access controls

Automation Systems Devices

- Servers: PCS, SCADA, ...
- Firewalls
- Work stations
- HMI Stations
- Hardened networking devices
- IEDs, Sensors, Controllers
### Automation Systems Security Really Unique?

<table>
<thead>
<tr>
<th>Corporate IT</th>
<th>Automation Systems IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not life threatening</td>
<td>Safety first</td>
</tr>
<tr>
<td>Availability important</td>
<td>Non-interruption is critical</td>
</tr>
<tr>
<td>Transactional orientation</td>
<td>Real-time focus</td>
</tr>
<tr>
<td>IBM, SAP, Oracle, .....</td>
<td>ABB, Emerson, GE, Honeywell, Siemens...</td>
</tr>
<tr>
<td>People ~ Devices</td>
<td>Few people; Many, many devices</td>
</tr>
<tr>
<td>PCs and Servers</td>
<td>Sensors, Controllers, Servers</td>
</tr>
<tr>
<td>Web services model is dominant</td>
<td>Polled automation control model</td>
</tr>
<tr>
<td>MS Windows is dominant OS</td>
<td>Vendor-embedded operating systems</td>
</tr>
<tr>
<td>Many commercial software products installed on each PC</td>
<td>Purpose-specific devices and application</td>
</tr>
<tr>
<td>Protocol is primarily HTTP/HTTPS over TCP/IP -- widely known</td>
<td>Many industrial protocols, some over TCP/IP – vendor and sector-specific</td>
</tr>
<tr>
<td>Office environment, plus mobile</td>
<td>Harsh operating plant environments</td>
</tr>
<tr>
<td>Cross-industry IT jargon</td>
<td>Industry sector-specific jargon</td>
</tr>
<tr>
<td>Cross-industry regulations (mostly)</td>
<td>Industry-specific regulations</td>
</tr>
</tbody>
</table>
IT/Data Center Environment

• Dedicated Specialists
  - Desktop
  - Database
  - Network
  - Security

• Dedicated Tools
  - Desktop Management
  - Database Management
  - Network Management
  - Security Monitoring
Operations Technology (OT) Environment

- OT Specialists
  - Dedicated Applications Specialists
  - Manage Control Network and Control Systems
  - Generalists, Not Specialists

- OT Tools
  - Diagnostic Tools Are Usually Supplied by Control Systems Vendor
  - Control Systems Tools Are Application Centric
  - Network, Security, Database, Desktop Support Tools Not Available or Not Present
  - Learning 4-5 IT Tools To Manage Environment Not Practical
Unique Challenge: 15+ Year Duty Cycle on Control Systems

- **Legacy Systems Create Unique Challenges**
  - Operating Systems No Longer Supported by Manufacturer
    - Windows NT
    - Older Unix Systems Such as AIX or Solaris

- **Limited Network Bandwidth**
  - Older Networks Will Be Adversely Affected By Some Standard IT Monitoring Technologies

- **Look For:**
  - Security Technologies That Support Legacy Systems
  - Technologies That Utilize Limited Network Bandwidth For Reporting/Monitoring
Unique Challenge: Industrial Controls Environment

- **Industrial Protocols Within Control System Networks**
  - Modbus
  - DNP3

- **Industrial End Point Devices**
  - Programmable Logic Controllers (PLCs)
  - Intelligent Electronic Devices (IEDs)
  - Remote Terminal Units (RTUs)

- **Look For:**
  - Technologies that support network monitoring of industrial protocols via purpose built signatures for industrial protocols
  - Technologies that can monitor configurations of industrial end point devices
Recommended OT Security Deployment

- Network Segment Monitoring
  - Network Intrusion Monitoring for Including Industrial Protocols

- Monitoring of Servers
  - Syslog
  - Embedded Agents

- Monitoring of Workstations
  - Syslog
  - Embedded Agents

- Perimeter Firewalls

- Anti-Virus Anti Malware
  - Blacklist (signature based)
  - Whitelist (application based)

- Configuration Management
  - Monitoring and Baselines of Configuration Changes
Generation Plant Security Deployment

System 800xA + NERC-CIP Security Solution

Security Management Workplace

WSUS, ePO, ...

RNR Router

CS+AO

AS

PGIM + OPTIMAX®

IEC61850

IEC61850 (GOOSE, MMS)

Plant or Corp. Network

DMZ Network

TAP Network

IEC61850 Network

Client/Server Network

Control Network

© 2012 ABB
Security Components
SCADA

- Cisco Switch WS-C3560-48TS
- RSA Two Factor Appliance
- HMI Workstation w/ 4 Monitors
- Customer RTU
- Customer Provided Modems

SCADA Servers
Oracle Servers UDW
Thin Client Server Proliant DL380R06
Historian / PC Apps Servers w/ MSL2024 Tape Library Proliant DL380R06
Domain Controller Servers Proliant DL380R06

Backup Control System
Routers Provided by RRI

Host Intrusion Detection/Prevention
Example SCADA Management System
Development of Secure Products

• Role-Based Access Control
  – Functions and data
  – Prevent database changes that produce system failures
  – Prevent more than one operator from controlling a single point simultaneously.

• Encryption and Communications

• Audit Trail
  – History of each users access to objects, attributes, data, displays, production areas and controls.

• Vulnerability Testing
  – Independent, un-biased

• Installation Best Practices and Guidelines
Cyber Security Project Execution

Planning
- Functional Design Specification
- Security Policy
- Network Topology Drawings
- Upgrades and Testing

Deployment and Commissioning
- Installation and Hardening Guideline
- Remote Access and File Transfer
- Networks and Interfaces
- Group Policy and Organizational Units

Operation
- Computer and User Administration
- Backup and Recovery
- Patch and Rollup Management

Communicate and agree
Secure the system and make it available
Operation starts on day one
Summary

- OT Has Unique Operating Environments
  - Legacy Systems
  - Industrial Systems And Endpoints

- OT Has Unique Threats

- OT Has Limited Tools and Resources

- Look For:
  - Tools That Are Specialized For OT
  - Tools That Have Been Developed with Security as a Requirement
  - Tools That Have Been Tested By Control System Vendors
  - Are Purpose Built For OT Professionals
  - Proven Methods for Developing and Deploying Secure SCADA Solutions