Industrial Security: IT vs OT Deployment Practices

Robert Albach, Product Line Manager IoT Security
BRKIOT-2115
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

Cisco Spark spaces will be available until July 3, 2017.

cs.co/ciscolivebot#BRKIOT-2115
Industrial Networks: Change / Challenge

The average age difference between industrial and non-industrial workers doubled between 2000 and 2012.

The number of TCP/IP connected end-points in industrial environments rose 96% between 2011 and 2015.

The number of vulnerabilities found in industrial systems rose 2400% from 2009 to 2015.

The minimum technology horizon for technology refresh is 5 years in some industries.
2015 Ukraine Utility Attack

Video Capture (with captions)
Goal of this Presentation: Educate and Prepare you to provide security for industrial environments.
Agenda

• Information and Industrial Network Differences
  • Industrial Protocols – their security challenges
  • Standards in Industrial spaces
  • A Phased Approach to Industrial Security
  • Four Common Industrial Security Use Cases
  • 3 Attack Discussions
  • Closing / Question & Answer
What is the OT Thing?

• Operations Technology
  • “Industrial” NW and Compute
    • Intelligent Electronic Devices (IEDs)
    • Autonomous but highly limited

• More than SCADA
  • …and what is that SCADA(Supervisory Control and Data Acquisition) thing?
  • Or is that ICS (Industrial Control Systems)?
  • Same / Different
  • Depends on your POV
Holistic View of Vertical Segments

**Purdue Model**

**Level 5**
- Enterprise Network
  - 100% IT
  - E.g. Virtual Patient, IP Video, Wi-Fi, RFID, Medical Inventory, Trackers, Patient Media Experience

**Level 4**
- Site Business Planning
  - 90% IT
  - E.g. Store-in-a-box, Digital Experience, Electronic Shelf-Edge Labels, Product Tracking Tags

**Level 3.5**
- DMZ Demilitarized Zone
  - 70% OT
  - E.g. Fleet, asset Management

**Level 3**
- Plant Zone
  - 60% IT
  - E.g. Collaborative to Navigation Applications

**Level 2**
- Cell/Area Zone
  - 40% OT
  - E.g. Roadways, Trackside, Onboard, & Mobile Signature Device

**Level 1**
- Basic Control
  - 30% OT
  - E.g. Automotive Subsystems Interior to Safety Sensors

**Level 0**
- Process
  - 10% OT
  - E.g. Asset Tracking

**Note:** IT & OT As Defined by IOT BU

*OT Baseline Features

**Level 0 Process**
- 10% OT
  - E.g. Asset Tracking

**Level 2 Cell/Area Zone**
- 10% OT
  - E.g. Asset Tracking

**Level 3 Plant Zone**
- 10% OT
  - E.g. Remote Cell Towers

**Level 4 Site Business Planning**
- 10% OT
  - E.g. Asset Tracking

**Level 5 Enterprise Network**
- 10% OT
  - E.g. Store-in-a-box, Digital Experience, Electronic Shelf-Edge Labels, Product Tracking Tags

**Level 3.5 DMZ Demilitarized Zone**
- 30% IT
  - E.g. Fleet, asset Management

**Level 3 Plant Zone**
- 30% OT
  - E.g. SCADA, ICS, EMS, AGC, Automation, Robots, Assets Tracking, & RFID Tag Reader

**Level 2 Cell/Area Zone**
- 30% OT
  - E.g. Smart Gas Meter, Power Room, Distribution & Substation, Oilfield, Refinery, & Smart Grid Devices

**Level 1 Basic Control**
- 60% IT
  - E.g. 60% IT Stations, Wi-Fi, Automated Kiosks/Console Traffic & Parking Sensor

**Level 0 Process**
- 70% OT
  - E.g. Backend Offices

**Level 3 Plant Zone**
- 70% IT
  - E.g. Fleet, asset Management

**Level 2 Cell/Area Zone**
- 70% IT
  - E.g. Remote Cell Towers

**Level 1 Basic Control**
- 40% OT
  - E.g. Roadways, Trackside, Onboard, & Mobile Signature Device

**Level 0 Process**
- 40% OT
  - E.g. Automotive Subsystems Interior to Safety Sensors

**Level 3 Plant Zone**
- 60% IT
  - E.g. Collaborative to Navigation Applications

**Level 2 Cell/Area Zone**
- 30% IT
  - E.g. Store-in-a-box, Digital Experience, Electronic Shelf-Edge Labels, Product Tracking Tags

**Level 1 Basic Control**
- 90% IT
  - E.g. Virtual Patient, IP Video, Wi-Fi, RFID, Medical Inventory, Trackers, Patient Media Experience

**Level 0 Process**
- 100% IT
  - E.g. Virtual Patient, IP Video, Wi-Fi, RFID, Medical Inventory, Trackers, Patient Media Experience
OT / IT Technology Splits – Electric Transmission
How OT Networks were Built

• Manufacturing
  • Ad Hoc – Built by our paint system provider.
  • Multiple sources – Paint sprayer and drier.
  • Assembled - Conveyer belt through paint sprayer into drier.

• Utilities
  • Top Down – “We built this sub-station.”
  • Integrated – “We interface with LCRA here (grid interconnects).”
  • Telecomm groups - <if the utility is large enough>
How OT Networks were Built - 2

• Transport
  • Bus / Train / Plane
  • Ticketing systems / boarding systems / physical security / signaling / control / etc.
  • Each from a different source / different “network”

• Oil and Gas / Mining
  • Upstream – exploration / drilling / production /
  • Midstream – transport: barge / rail / pipeline
  • Downstream – refinery / pipeline / retail
## Assets to Protect

<table>
<thead>
<tr>
<th>Asset</th>
<th>Description</th>
<th>Examples and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IED</td>
<td><strong>Intelligent Electronic Device</strong> – Commonly used within a control system, and is equipped with a small microprocessor to communicate digitally.</td>
<td>Sensor, actuator, motor, transformer, circuit breaker, pump</td>
</tr>
<tr>
<td>RTU</td>
<td><strong>Remote Terminal Unit</strong> – Typically used in a substation or remote location. It monitors field parameters and transmit data back to central station.</td>
<td>Overlap with PLC in terms of capability and functionality</td>
</tr>
<tr>
<td>PLC</td>
<td><strong>Programmable Logic Controller</strong> – A specialized computer used to automate control functions within industrial network.</td>
<td>Most PLCs do not use commercial OS, and use “ladder logic” for control functions</td>
</tr>
<tr>
<td>HMI</td>
<td><strong>Human Machine Interfaces</strong> – Operator’s dashboard or control panel to monitor and control PLCs, RTUs, and IEDs.</td>
<td>HMIs are typically modern control software running on modern operating systems (e.g. Windows).</td>
</tr>
<tr>
<td>Supervisory Workstation</td>
<td>Collect information from industrial assets and present the information for supervisory purposes.</td>
<td>Unlike HMI, a supervisory workstation is primarily read-only.</td>
</tr>
<tr>
<td>Data Historian</td>
<td>Software system that collects point values and other information from industrial devices and store them in specialized database.</td>
<td>Typically with built-in high availability and replicated across the industrial network.</td>
</tr>
<tr>
<td>Other Asset</td>
<td>Many other devices may be connected to an industrial network.</td>
<td>For example, printers can be connected directly to a control loop.</td>
</tr>
</tbody>
</table>
How to Wire a PLC

- This is a PLC
- Input Terminals
- Output Terminals
- Programming Cable
- Power 24 VDC
## IT/OT Differences in Priorities

<table>
<thead>
<tr>
<th>Security Policies</th>
<th>IT Network</th>
<th>IoT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td>Protecting Intellectual Property and Company Assets</td>
<td>24/7 Operations, High OEE, Safety, and Ease of Use</td>
</tr>
<tr>
<td><strong>Priorities</strong></td>
<td>1. Confidentiality</td>
<td>1. Availability</td>
</tr>
<tr>
<td></td>
<td>2. Integrity</td>
<td>2. Integrity</td>
</tr>
<tr>
<td></td>
<td>3. Availability</td>
<td>3. Confidentiality</td>
</tr>
<tr>
<td><strong>Types of Data Traffic</strong></td>
<td>Converged Network of Data, Voice and Video (Hierarchical)</td>
<td>Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P &amp; Hierarchical)</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>Strict Network Authentication and Access Policies</td>
<td>Strict Physical Access</td>
</tr>
<tr>
<td></td>
<td>Simple Network Device Access Access</td>
<td>Simple Network Device Access Access</td>
</tr>
<tr>
<td><strong>Implications of a Device Failure</strong></td>
<td>Continues to Operate</td>
<td>Could Stop Processes, Impact Markets, Physical Harm</td>
</tr>
<tr>
<td><strong>Threat Protection</strong></td>
<td>Shut Down Access to Detected Threat and Remediate</td>
<td>Potentially Keep Operating with a Detected Threat</td>
</tr>
<tr>
<td><strong>Upgrades and Patch Mgmt</strong></td>
<td>ASAP During Uptime</td>
<td>Scheduled During Downtime</td>
</tr>
</tbody>
</table>
Maintenance Windows

- Monthly
- Quarterly
- Yearly
Every Network has its Challenges

IT Networks
   Many Applications
   Dynamic
   Interoperability unconstrained
   Knowledgeable workers in market

OT Networks
   Fixed / Limited Applications
   Stagnant / Stable
   Limited interoperability
IT Networks – Data Flows

End points are smart – human driven.

If data leaves – it goes far…

Web – data center / internet
Email
File / Print shares
Nearby devices largely unrelated

When the end points talk:
Short conversations
Many connections
Short TCP sessions – SYN SYN/ACK ACK – a few secs max
Largely egalitarian – anybody talk to anybody
OT Networks – Data Flows

End points are not smart – repetitive.

If data leaves – it stays close
Interaction is largely local
Movement not very visible
if it does leave – streams out
Not a conversation usually

When the end points talk:
Long conversations
Few connections
Long TCP sessions – lots of keep alives– hours / days!
Principle of Least Route*

- An attribute of discrete / segmented modularly built networks <like manufacturing systems>
- Generally references network span
- Small subnets

- Zone segmentation much more than VLANs

*Rockwell Automation
By Count most of the “things” in IoT: Won’t have an IP Address
How To: Set an IP Address

<table>
<thead>
<tr>
<th>Switch</th>
<th>Position</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address High Byte</td>
<td>0 ~ F</td>
<td>Hexadecimal setting of IP address’ last octet. 192.168.1.xxx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example 1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Byte: “0”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Byte: “1”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hexadecimal value “01” = 1 (decimal)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP Address: 192.168.1.1</td>
</tr>
<tr>
<td>IP Address Low Byte</td>
<td>0 ~ F</td>
<td>Example 2:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Byte: “A”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low Byte: “7”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hexadecimal value “A7” = 167 (decimal)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP Address: 192.168.1.167</td>
</tr>
</tbody>
</table>
...and TIME is different too.

- **NTP** – Network Time Protocol
  - Precision levels - coarse
  - CPU or mother board oscillator

- **PTP** – Precision Timing Protocol
  - Precision levels 100 ns
  - Specialized HW <Phy level>
Some Interesting Industrial Sec Features…

- Run / Remote / Program Switch
- CPU Lock
- Programmable Task Priority
Environmental Needs

- **Obvious** – More strenuous
  - Cold / Heat
  - Vibration / Shock

- **Next Obvious** – Not an Add-On

- **Not so Obvious**
  - Operating Environment
  - Storage Environment

Operating Environment - -40°C to 60°C in a fully enclosed cabinet (no airflow)

Storage Environment - Temperature: -40 to +85 degrees C
Industrial Needs are More than Environmental

• Driven by the IT vs. OT differences discussed
  • Latency over Throughput
  • Application control over Threat control
  • Simplicity over Sophistication

• This equipment *might* get swapped out in a decade.

• …Availability over Security

• Power, alarm connectors, IO connector are often different
Summary: Industrial Network Differences

- Emphasis on Availability and Safety First!
- Continually operating / Infrequently interrupted
- Very different network patterns
- Physical environment drives unique equipment
Agenda

- Information and Industrial Network Differences
- Industrial Protocols – their security challenges
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 3 Attack Discussions
- Closing / Question & Answer
Industrial Protocols and Security Issues
Industrial Networks: Manufacturing +

- Fieldbus: 58%
  - Annual growth: 7%
- PROFINET: 8%
- EtherCAT: 6%
- Modbus-TCP: 4%
- Powerlink: 3%
- Other Ethernet: 8%
- EtherNet/IP: 9%
- Other fieldbuses: 15%
- CAN/CANopen: 5%
- AS-interface: 3%
- Devicenet: 5%
- CC-Link: 6%
- Modbus: 7%
- PROFIBUS: 17%

Industrial Ethernet: 38%
- Annual growth: 20%

Wireless: 4%
- Annual growth: 30%
- WLAN: 2%
- Other Bluetooth: 1%
- Other Wireless: 1%
Industrial Protocols - General Security Concerns

- Early developments of many protocols made few provisions for security
  - Focus was on interoperability and continuity
  - Master / Slave relationships within serial communications
  - No encryption (but there are reasons not to in some cases)

- Authentication is commonly lacking
  - The most common Ethernet/IP base OT protocol lacked authentication till 2015

- Broadcasting for communications

- Assumption of limited communication complexity
Where are these Protocols Found? Manufacturing Protocols

Manufacturing Protocols
- FieldBus
- TCP/IP
Where are these Protocols Found?

Utility Protocols

- DNP
- ICCP
- BRKIOT

Other Transmission System Operators (TSO)/Distribution System Operators (DSO) and Verticals

Independent Power Producers (IPP)

Inter-Control Center Networks

Utility Tier

Intra-Control/Data Center Tier

Control Center

Applications and Users

Control Center Network

Field Dispatch

Control Center Network
Protocol Awareness:

- Moving beyond simple specification study
- Build stateful analysis of the protocol
- Industrial protocols may have connections that last > 24 hrs.
- Normal reg-ex based rules are more limited
Summary of Industrial Protocol Security

- Industrial Protocols Born from Proprietary Systems
  - Minimal if any interoperability
- Little to no built in security in older systems
  - Growth of security coming for NEW systems
- Visibility challenges
  - Proximity for true view and control
  - Protocol awareness critical
Agenda

- Information and Industrial Network Differences
- Industrial Protocols – their security challenges
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 3 Attack Discussions
- Closing / Question & Answer
2.3 Security Objectives

A critical requirement of IACS security measures is that they must not have the potential to cause impacts to essential services and functions, including emergency procedures. In contrast, IT security measures as often deployed do have this potential. IACS security goals focus on control system availability, plant safety, plant protection, plant operations (even in a degraded mode) and time-critical system response. General IT security goals often do not place the same emphasis on these factors, typically being more concerned with protecting information than physical assets. This difference in emphasis is often referred to as CIA (confidentiality, integrity, and availability) vs. IAC (integrity, availability, confidentiality).
ISA-99 ≈ IEC 62443
Zones

• Design your networks
  • Physical / Logical Organization
  • Mostly Physical

• Remember the OT NW Traffic Profile?
  • Intra-”cell” traffic is dominant
  • Little cell to cell communication
Design of the Assembly Line will drive network and security design:

First – What is the right level of control for:
   - Each Station;
   - Each “Line”;
   - The whole system

Second – What are the applications responsible for each level?
   - Applications that control normal operation;
   - Applications that control safety;
   - Applications that feed operational / business analytics;
   - Applications that provide for maintenance.

Cisco live!
How To Paint a Car – w 90 robots over 4 km

Initial Wash → Treatment → Electrocoat → Oven → Sanding

Seam Seal → Oven → Primer → Oven → Sanding

Base Coat → Oven → Clear Coat → Oven → Polishing

Spot Repair → Body Repair → Wax
How Many Zones? / How Many Vendors?

- Initial Wash → Treatment → Electrocoat → Oven → Sanding
- Seam Seal → Oven → Primer → Oven → Sanding
- Base Coat → Oven → Clear Coat → Oven → Polishing
- Spot Repair → Body Repair → Wax
Conduits

- Controlled Communications
  - ACLs
  - DACLs?
  - Or perhaps Security Group Tags (SGTs)?
  - VLANs

- Secured Communications
  - VPNs
Firewall Rules Recommendations

In summary, the following should be considered as recommended practice for general firewall rule sets:

- **The base rule set should be deny all, permit none.**

- Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.

- All “permit” rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.

- All rules should restrict traffic to a specific IP address or range of addresses.

- Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in the DMZ.

- Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).

- **All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.**

- Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.

- Control network devices should not be allowed to access the Internet.

- **Control networks should not be directly connected to the Internet, even if protected via a firewall.**

- All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with two-factor authentication. Traffic should also be restricted by IP address to specific management stations.
Summary of Industrial First Principals

• Highly focused on standards

• Network Segmentation is key
  • Zones
  • Conduits
Agenda

- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- Some Industrial Protocols and their Security Issues
- Closing / Question & Answer
# Security Phasing Approaches - Standards

## US Department of Homeland Defense: Continuous Diagnostics and Mitigation

<table>
<thead>
<tr>
<th>CDM – Phase 1</th>
<th>CDM – Phase 2</th>
<th>CDM – Phase 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Control – What is the state of the endpoints I must secure?</td>
<td>Manage People and Services – Who can do what?</td>
<td>Process Planning – What to do and how do we improve?</td>
</tr>
</tbody>
</table>
Evolve to Security: Phased Security Architecture

First Phase – Secured Connectivity

Zone Segmentation Controlled Conduits

Second Phase – Secured Visibility & Control

Application Control Threat Control

Third Phase – Converged Security & Depth

Policy Driven Response Deeper Vision / Control
Cisco IoT System Security

**IoT Network As a Sensor and Enforcer**
- IR Portfolio
- IE Portfolio
- ISE
- Stealthwatch

**OT-Specific Security**
- ISA 3000
- ASA 5506H

**IoT Physical Security**
- 3000 and 6000 Series WDR IP Cameras
- ICPAM
- Physical Access Control

**IoT Security Services**
Cisco IoT Threat Defense Components

- **Stealthwatch** - Visibility of connections and relationships
- **ISE** – Device / User identity
- **NGFW** – App Activity
- **AMP** – End Point Activity

- **AnyConnect** - Secure Connection in/out of OT network
- **ISE** – dynamic access control
- **FirePower** – Observe remote activities
- **DNS** – remote site risk protection

- **FP NGFW** - Segment IT and OT environments
- **TrustSec** - Segment OT devices in the IT network
- **ISE** – Align access with users / device
- **Switches** – Dynamic segmentation enforcement

- **Risk assessment** for baseline
- **Deployment and Migration**
- **Incident response Service** for breach situations
Summary of Phased Security Architecture

- Long – running pre-existing operations

- Introduction of new elements must be done carefully over years

- Phases of introduction
  - Modern networking and networking design
  - Dedicated threat and application visibility
  - Converging with advanced security practices
Agenda

- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- A Phased Approach to Industrial Security
- Standards in Industrial spaces
- Four Common Industrial Security Use Cases
- 3 Attack Discussions
- Closing / Question & Answer
Security Use Case Themes

• Secure Connectivity
• Threat Control
• Safe Environment
• Secure Remote Access

• What can connect
• What can talk to what
• What is vulnerable
• Protect the vulnerable
• Network protection
• Device protections
• What are the controls for access
• How to secure access
Use Case: Transitioning to Secured Connectivity
Protect Critical Infrastructure: Through Network Segmentation – Zone Definition
Wireless Aps: Fully Documented and Controlled
NAT is Everywhere

• Single Vendor Source
  • Identical systems
  • Identical addressing

• Just Dropped In
  • Assembled by Integrator
  • No Re-IP effort

• NAT a security strategy?
Building out Secured Connectivity

• Design the network with Zones / Conduits in mind.

• Build the network with the future in mind – dedicated security appliances / features

• What to deploy:
  • Industrial Switches / Routers / Wireless (combinations)
  • NW Expertise
Protect Critical Infrastructure: Through Network Segmentation – Zone Definition

How to think in terms of the application?

How to ensure ONLY the right protocols are at play?

How to control access to each section?
Use Case: Threat Control – Identification and Actions
Protect Critical Infrastructure – Threat Control

Sinapsis SQL injection attempt
<table>
<thead>
<tr>
<th>2016 ICS Vuln</th>
<th>IT Like Component</th>
<th>Asset</th>
<th>Threat Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13%</td>
<td>NW</td>
<td></td>
<td>Human Error, Failure, Attacks</td>
</tr>
<tr>
<td>2%</td>
<td>Data Historian</td>
<td></td>
<td>Minimal immediate Impact on System</td>
</tr>
<tr>
<td>52%</td>
<td>Supervisory Workstation</td>
<td></td>
<td>Human Error, Failure, Attacks</td>
</tr>
<tr>
<td>4%</td>
<td>HMI</td>
<td></td>
<td>Human Error, Failure, Attacks</td>
</tr>
<tr>
<td>20%</td>
<td>PLC / IO</td>
<td></td>
<td>Command / Program Errors, Failure, Attacks</td>
</tr>
<tr>
<td>7%</td>
<td>RTU / Converters</td>
<td></td>
<td>Valid Inputs and Source, Failure, Attacks</td>
</tr>
<tr>
<td></td>
<td>IED</td>
<td></td>
<td>Failure, Valid Inputs and Source, Physical Security</td>
</tr>
</tbody>
</table>
Use Case: Application Visibility and Control: Safety / Security
Safety Is EVERYTHING
Impact in Ukraine:

Error

20,000 years of radiation
Protect Critical Infrastructure – Safety Enforcement
Stopping Misconfiguration of a Robot Arm
Protocol Parser - Modbus

Parameter Value (Data)  
Function  
Unit

Edit Rule 1:1000025:1
Message: PROTOCOL-SCADA Modbus RTU-2000 cooler power OFF from external s
Classification
Action: alert
Protocol: tcp
Direction: Directional
Source IPs: $EXTERNAL_NET
Destination IPs: $HOME_NET
Source Port: any
Destination Port: 502

Detection Options
flow: Established To Server
metadata
impact_flag: red
reference: url: www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf
modbus_unit: 255
modbus_func: write_single_coil
modbus_data: content: [00 04 00]

Cisco Public
Industrial Protocol Identification

ODVA – CIP / EIP

RA = Rockwell Automation
The OT Control System Application Stack

Enterprise Zone: Levels 4-5
- Industrial Demilitarized Zone (IDMZ)
  - Physical or Virtualized Servers
  - Patch Management
  - AV Server
  - Application Mirror
  - Remote Desktop Gateway Server

Industrial Zone: Levels 0-3
- Authentication, Authorization and Accounting (AAA)
  - Active Directory (AD)
  - Identity Services Engine (ISE)
  - FactoryTalk Security
  - Remote Access Server (RAS)

Level 3 – Site Operations
- OS Hardening
- Application Hardening
- FactoryTalk Client Control

Level 2 – Area Supervisory Control
- VLANs, Segmenting Domains of Trust
- IACS Device Hardening
  - Policies and Procedures
  - Physical Measures
  - Electronic Measures
  - Encrypted Communications

Level 1 – Controller
- Controller Firewall
- Controller LWAP

Network Infrastructure
- Hardening
- Access Control
- Resiliency
- Port Security
- Physical
- Electronic

Wireless LAN (WLAN)
- Access Policy
  - Equipment SSID
  - Plant Personnel SSID
  - Trusted Partners SSID
  - WPA2 with AES Encryption
  - Autonomous WLAN
  - Pre-Shared Key
  - 802.1X - (EAP-FAST)
  - Unified WLAN
  - 802.1X - (EAP-TLS)
  - CAPWAP DTLS

Standard DMZ Design BEST Practices
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Control System Engineers in Collaboration with IT Network Engineers
IT Security Architects in Collaboration with Control Systems Engineers

CiscoLive!
Use Case: Remote Access – A Challenging Necessity
Protect Critical Infrastructure: 
Allow Secured Remote Access
Remote Access in Contracts:

• Ver.10 XXXX Maintenance Support Agreement

• SERVICE AGREEMENT TERMS AND CONDITIONS

• XXXXX, a division of YYYYY North America Corporation ("ZZZZZ") will perform the services ("Services") listed below and on the above pages of this service agreement and any exhibits ("Exhibits") attached to it (together, the "Agreement") under the following terms and conditions:

• 4. Customer’s Responsibility

• Throughout the term of this Service Agreement, Customer agrees to:

  c. provide suitable remote access to the System to enable ZZZZZ to perform its services hereunder, including but not limited to VPN access to the System:

  d) REMOTE SERVICE. For on-site options, if remote Service is available, the Customer will allow NNN to keep diagnostic and maintenance programs resident on Customer's system or site for the exclusive purpose of performing diagnostics and repair. The Customer has no ownership interest in this software provided by NNN. NNN may remove these programs and any NNN loaned equipment upon termination of coverage. Customer's system must be configured to permit access. For NNN to provide remote Service, the Customer must allow NNN remote access to eligible NNN systems using the appropriate protocol and method supported by that system. The Customer must provide the necessary equipment designated for that protocol and method of communication to provide remote access to the eligible NNN system. NNN will advise the Customer what is required at the time of installation.
Configuring and Managing Remote Access for Industrial Control Systems

November 2010
If this was a North American Utility: This Approach Would be the Law

<table>
<thead>
<tr>
<th>Part</th>
<th>Applicable Systems</th>
<th>Requirements</th>
<th>Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>High Impact BES Cyber Systems and their associated:</td>
<td>Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.</td>
<td>Examples of evidence may include, but are not limited to, network diagrams or architecture documents.</td>
</tr>
<tr>
<td></td>
<td>• PCA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Medium Impact BES Cyber Systems and their associated:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PCA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Protect Critical Infrastructure: Allow Secured Remote Access

What is security status of vendor device?

What path and QOS through NW needed?

How to coordinate access from IT into OT side?

How to confirm what was done to the device?
Your Plant Floor Workers Don’t Just Do OT Work
Summary of Common Use Cases

- Secured Communications
  - Segmentation and Hierarchical Network Design
- Threat Control
  - Vulnerability identification and mitigation
- Enhanced Safety and Control
  - Securing equipment from unwanted activity
- Remote Access to Industrial Equipment
  - End to End Who, What, When, Where
Agenda

• Information and Industrial Network Differences
• Security First Principals and Industrial Security Concepts
• Standards in Industrial spaces
• A Phased Approach to Industrial Security
• Four Common Industrial Security Use Cases
• 3 Attack Discussions
• Closing / Question & Answer
Discussion of Attacks: Ukraine Utility; German Smelter, LA Transit
**ICS Attacks - When you look at the data on Malware**

<table>
<thead>
<tr>
<th>Incidental Infections</th>
<th>ICS Themed Attacks</th>
<th>ICS Specifically Tailored</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Untargeted Virus, Worms</td>
<td>• Targeted Malware, nothing ICS specific – just named to get OT interest</td>
<td>• Written for ICS systems OR modified for ICS systems</td>
</tr>
<tr>
<td>• <strong>WannaCry</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Renault- Nissan</td>
<td>• Tens</td>
<td>• 3+1</td>
</tr>
<tr>
<td>• Thousands</td>
<td></td>
<td>• Stuxnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Havex</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Black Energy 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>CrashOverride (Industroyer)</strong></td>
</tr>
</tbody>
</table>

**Credit – Dragos Security – Project Mimics**
Attacks Can Break Things…

A cyberattack has caused confirmed physical damage for the second time ever.
Kill Chain – ICS Variant

- Intrusion Phase
  - Reconnaissance
  - Targeting
  - Weaponization
    - Develop / Test
  - Delivery / Exploit / Persist
  - Install
  - Modify Systems
  - Command and Control
  - Attack
  - Anti-Forensics
German Smelter Attack: Reconnaissance / Targeting

- What is known:
  - Phishing Attack
  - Malware
  - Access to ICS System
  - Shutdown commands
  - Damaged smelter

* OT Baseline features
German Smelter Attack: Attack

- What is known:
  - Phishing Attack
  - Malware
  - Access to ICS System
  - Shutdown commands
  - Damaged smelter

* OT Baseline features
Impact in Ukraine:

Attack

3+ hours of lost power

@ month of degradation
2015 Ukraine Utility Attack – Simplified View

2016 Variations

- Spear Fishing into IT
- BlackEnergy Malware Placed
- Credential Theft for Access
- VPN access from outside
- Remote management tools
- DOS of ICS components
- Control protocol commands
- Firmware update / corruption
- UPS system disabled
- KillDisk anti-forensics wipe
- Telephone DDOS
Kill Chain – ICS Variant

• Attacks start on IT side
• Work their way to OT

Sub-Station Attack

- Phishing
- Credential Theft
- Anti-Forensics + Phone DDOS
- Commands
- VPN Access
- Workstation RDP

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
Initial Entry: Reconnaissance / Targeting

Sub-Station Attack

- Phishing
- Credential Theft
- Anti-Forensics + Phone DDOS
- Commands
- VPN Access
- Workstation RDP
Traversal: Credential Theft
Command and Control: VPN Access (OT)
Command and Control: VPN Access (IT)
Attack: Remote Desktop / Control

“The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive. Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel.”

Wired Magazine – Inside The Cunning Unprecedented Hack of Ukraine’s Power Grid

2016 Variant:
• DOS of ICS components
• ICS Control protocol commands
ICS Specific Attack: UPS Shutdown
ICS Specific Attack: Bad Firmware Upgrade

Substation Attack

- Phishing
- Credential Theft
- Commands
- VPN Access
- Workstation RDP
- Anti-Forensics + Phone DDOS

Anti-Forensics + Phone DDOS
Attack: Anti-Forensics – Wiper Software
Impact in LA:

Attack

intersections snarled for 4 days

Key signals targeted, officials say

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

January 09, 2007 | Sharon Bernstein and Andrew Blankstein | Times Staff Writers

Back in August, the union representing the city’s traffic engineers vowed that on the day of their work action, "Los Angeles is not going to be a fun place to drive."

City officials took the threat seriously.

Fearful that the strikers could wreak havoc on the surface street system, they temporarily blocked all engineers from access to the computer that controls traffic signals.
Stolen Credentials

Transport

Traffic Management Center

Core and Aggr

Roadside

Vehicle

Yard

Cisco Nexus® Switch
Cisco Nexus Switch
Cisco Nexus Switch
Cisco Nexus Switch

ASR 1000

ASR 901

IP/MPLS Domain

ASR 9000

ASR 9000

ASR 903

TSC/TSP

DSRC RSU

819 ISR

819 ISR

4451X ISR

TSC/TSP

DSRC OBU

819 ISR

CAD/AVL VLU
Agenda

- Information and Industrial Network Differences
- Security First Principals and Industrial Security Concepts
- Standards in Industrial spaces
- A Phased Approach to Industrial Security
- Four Common Industrial Security Use Cases
- 3 Attack Discussions
- Closing / Question & Answer
Summary

Industrial networks are very different. Industrial security must be treated differently.

Operational teams prioritize safety, stability. Operational teams move slowly, cautiously.
Tasks for your OT Security Journey

First
- Update your network
- Gain a view of the network and applications
- Establish access control that reflects the networks

Second
- Understand your applications
  - Who is talking to who
  - What are they saying
  - Establish base lines
  - Determine what is truly necessary

Third
- Get Help
  - IT has done security for years
  - Look at design guides
  - Consider external services
- Act
  - Commit to making change
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 gift card.

• Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.
Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions
# Internet of Things (IoT) Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW! Managing Industrial Networks for Manufacturing (IMINS2 v1.3)</td>
<td>An associate level instructor led lab based training focuses on common industrial application protocols, security, wireless and troubleshooting designed to prepare you for the CCNA Industrial certification</td>
<td>CCNA® Industrial</td>
</tr>
<tr>
<td>Managing Industrial Networks with Cisco Networking Technologies (IMINS)</td>
<td>This instructor led lab based training addresses foundational skills needed to manage and administer networked industrial control systems for today's connected plants and enterprises. It helps prepare plant administrators, control system engineers and traditional network engineers for the Cisco Industrial Networking Specialist certification.</td>
<td>Cisco Industrial Networking Specialist</td>
</tr>
<tr>
<td>Control Systems Fundamentals for Industrial Networking (ICINS)</td>
<td>For IT and Network Engineers, provides an introduction to industry IoT verticals, automation environment and an overview of industrial control networks (E-Learning)</td>
<td>Pre-learning for IMINS, IMINS2 training &amp; certifications</td>
</tr>
<tr>
<td>Networking Fundamentals for Industrial Control Systems (INICS)</td>
<td>For Industrial Engineers and Control System Technicians, covers basic IP and networking concepts, and introductory overview of Automation industry Protocols.</td>
<td>Pre-learning for IMINS, IMINS2 training &amp; certifications</td>
</tr>
</tbody>
</table>

For more details, please visit: [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)
Thank you
Please join us for the Service Provider Innovation Talk featuring:

Yvette Kanouff | Senior Vice President and General Manager, SP Business
Joe Cozzolino | Senior Vice President, Cisco Services

Thursday, July 14th, 2016
11:30 am - 12:30 pm, In the Oceanside A room

What to expect from this innovation talk

• Insights on market trends and forecasts
• Preview of key technologies and capabilities
• Innovative demonstrations of the latest and greatest products
• Better understanding of how Cisco can help you succeed

Register to attend the session live now or watch the broadcast on cisco.com