Securing The Connected Enterprise
Pack Expo 2015 – Las Vegas

Chelsea An
Business Development Lead, Network & Security
Connected Enterprise
Control and Information Convergence

THE CONNECTED ENTERPRISE

- Scalable, robust, secure and future-ready infrastructure:
  - Application
  - Software
  - Network

Internet of Things, Internet of Everything
**Transaction information:** orders, supply network, product design …

**Real-time data:** alarms, events, states, energy, diagnostics, …

**IT**
- ERP
- FINANCIALS
- HR
- LOGISTICS
- QUALITY
- WAREHOUSE

**OT**
- INDUSTRIAL “THINGS”
- PLCS & SCANNERS
- MATERIAL & TRANSPORT
- MACHINES & TESTERS
- SHOP FLOOR PERSONNEL
- PRINTERS & LABEL SERVICES

**COMMON SECURE NETWORK INFRASTRUCTURE**
Risks and Threats to Control Systems

Security risks increase potential for disruption to system uptime, safety operation, and a loss of intellectual property.
"Good enough" security now, is better than "perfect" security ... never (Tom West, Data General)

Security ultimately relies - and fails - on the degree to which you are thorough. People don't like to be thorough. It gets in the way of being done (Dave Piscitello)

Your absolute security is only as strong as your weakest link

Concentrate on known, probable threats

Security is not a static end state, it is an interactive process

You only get to pick two of the three: fast, secure, cheap (Brett Eldridge)
Secure Automation & Information
Defending the digital architecture

Tamper Detection
Detect & Record unwanted Activity & Modifications to the application

Secure Network Infrastructure
Control Access to the network, and Detect unwanted access and activity

Content Protection
Protect viewing, editing, and use of specific pieces of control system content

Access Control & Policy Management
Control Who, What, Where & When access is allowed, to which application & device

INDUSTRIAL SECURITY MUST BE IMPLEMENTED AS A SYSTEM
Why is this important?

Industrial Automation and Control System Convergence

Flat and Open IACS Network Infrastructure

Structured and Hardened IACS Network Infrastructure
Industrial Security Trends
Established Industrial Security Standards

- International Society of Automation
  - ISA/IEC-62443 (Formerly ISA-99)
  - Industrial Automation and Control Systems (IACS) Security
    - Defense-in-Depth
    - IDMZ Deployment

- National Institute of Standards and Technology
  - NIST 800-82
  - Industrial Control System (ICS) Security
    - Defense-in-Depth
    - IDMZ Deployment

- Department of Homeland Security / Idaho National Lab
  - DHS INL/EXT-06-11478
    - Defense-in-Depth
    - IDMZ Deployment
Security – Holistic Defense-in-Depth
Multiple Layers to Protect and Defend the Edge

- No single product, technology or methodology can fully secure Industrial Automation and Control System (IACS) applications.
- Protecting IACS assets requires a defense-in-depth security approach, which addresses internal and external security threats.
- This approach utilizes multiple layers of defense (physical, procedural and electronic) at separate IACS levels by applying policies and procedures that address different types of threats.
## Industrial Network Security Trends

### Policies - Industrial vs. Enterprise Network Requirements

<table>
<thead>
<tr>
<th></th>
<th>Industrial (OT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td>24/7 operations, high OEE</td>
<td>Protecting intellectual property and company assets</td>
</tr>
</tbody>
</table>
| **Precedence of Priorities** | Availability  
Integrity  
Confidentiality                                               | Confidentiality  
Integrity  
Availability                                         |
| **Types of Data Traffic** | Converged network of data, control, information, safety and motion | Converged network of data, voice and video                     |
| **Access Control**        | Strict physical access  
Simple network device access                                    | Strict network authentication and access policies             |
| **Implications of a Device Failure** | Production is down  
($$'s/hour … or worse)                        | Work-around or wait                                          |
| **Threat Protection**     | Isolate threat but keep operating                              | Shut down access to detected threat                          |
| **Upgrades**              | Scheduled during downtime                                      | Automatically pushed during uptime                             |
ISC Security Program

Industrial Control System Security Program

Technical Security Controls
- Firewalls, Web Application Firewalls
- Control System Protocol Firewalls
- Traditional SPI/DPPI Firewalls
- Microsoft IPSec Filters
- Microsoft Group Policy Objects
- Intrusion Detection Systems
- Intrusions Prevention Systems
- Layer 3 Network Access Control Lists
- Network Access Control technologies
- Port Security elements
- Principle of Least Privilege

Non-Technical Security Controls
- Governance
  - Lifecycle Management
  - Disaster Recovery/Incident Response

Patch Management
Change & Config Mgmt
EndPoint Protection
Access Control & Authorization

Constant & Enduring Vigilance. No Exceptions.

NOTE: This is different than an Enterprise Security Program.
Network Security Framework

Industrial Demilitarized Zone

Logical Model – Industrial Automation and Control System (IACS)
Converged Multi-discipline Industrial Network
No Direct Traffic Flow between Enterprise and Industrial Zone
Security – Holistic Defense-in-Depth
Industrial Security Policies Drive Technical Controls

- **Physical** – limit physical access to authorized personnel: cells/areas, control panels, devices, cabling, and control room…. locks, gates, key cards, biometrics. This may also include policies, procedures and technology to escort and track visitors
- **Network** – security framework – e.g., firewall policies, access control list (ACL) policies for switches and routers, AAA, intrusion detection and prevention systems (IDS/IPS)
- **Computer Hardening** – patch management, anti-x software, removal of unused applications/protocols/services, closing unnecessary logical ports, protecting physical ports
- **Application** – authentication, authorization, and accounting (AAA)
- **Device Hardening** – change management, communication encryption, and restrictive access
Networking Design Considerations
CPwE Reference Architectures

Education, design considerations and guidance to help reduce network **Latency** and **Jitter**, to help increase the **Availability**, **Integrity** and **Confidentiality** of data, and to help design and deploy a **Scalable**, **Robust**, **Secure** and **Future-Ready** EtherNet/IP™ network infrastructure:

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation / Structure (modular & scalable building blocks)
- Prioritization - Quality of Service (QoS)
- Redundant Path Topologies with Resiliency Protocols
- Time Synchronization – PTP, CIP Sync, Integrated Motion on the EtherNet/IP network
- Multicast Management
- Convergence-ready Solutions
- Security – Holistic Defense-in-Depth
- Scalable Secure Remote Access
- Wireless LAN – 802.11 - Autonomous, Unified
Security – Holistic Defense-in-Depth
CPwE Reference Architectures - Architectural Security Framework

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

Level 3 – Site Operations:
- OS Hardening
- FactoryTalk Client
- VLANs, Segmenting Domains of Trust

Level 2 – Area Supervisory Control
- Device Hardening
  - Policies and Procedures
  - Physical
  - Electronic
  - Encrypted Communications

Level 1 - Controller
- Zone-based Policy Firewall (ZFW)
- I/O Soft Starter
- MCC

Level 0 - Process
- Plant Firewalls
  - Active/Standby Inter-zone traffic segmentation
  - ACLs, IPS and IDS
  - VPN Services
  - Portal and Remote Desktop Services proxy

Standard DMZ Design BEST Practices
- 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

Core switches
- Distribution Switch Stack
- Port Security
- Network Status and Monitoring
- Standard DMZ Design BEST Practices

Network Infrastructure
- Hardening
- Access Control
- Resiliency

Wireless LAN Controller (WLC)
- Active
- Standby

Enterprise
- Internet
- External DMZ/Firewall
Additional Material
Training & Certifications

- **Cisco® Industrial Networking Specialist Training and Certification**
  - E-learning modules (pre-learning courses)
    - Control Systems Fundamentals for Industrial Networking (ICINS)
    - Networking Fundamentals for Industrial Control Systems (INICS)
  - Classroom training
    - Managing Industrial Networks with Cisco Networking Technologies (IMINS)
  - Exam
    - 200-401 IMINS

- **CCNA Industrial Training and Certification**
  - Classroom training
    - Managing Industrial Networks for Manufacturing with Cisco Technologies (IMINS2)
  - Exam
    - 200-601 IMINS2

- **Industrial IP Advantage**
  - E-learning modules
  - CPwE Design Considerations and Best Practices
A good place to start the journey is with a security assessment.
Key Takeaways

- Education and awareness:
  - Within your organization, for your customers or trusted partners
- Establish an open dialog between Industrial Automation and IT groups
- Establish an Industrial security policy, unique from and in addition to the Enterprise security policy
- Holistic Defense-in-Depth approach: no single product, methodology, nor technology fully secures IACS networks
- Be aware of Industrial Automation and Control System Security Standards
  - ISA/IEC-62443 (Formerly ISA99), NIST 800-82, DHS External Report # INL/EXT-06-11478
- Utilize standards, reference models and reference architectures
- Work with trusted partners knowledgeable in industrial automation and security
- "Good enough" security now, is better than "perfect" security ... never. (Tom West, Data General)
Securing The Connected Enterprise

PUBLIC

Connect with us.

www.rockwellautomation.com