Network Security Trends & Fundamentals of Securing EtherNet/IP Networks

Presented by Rockwell Automation
Industrial Network Security Trends

Security Quips

- "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: fast, secure, cheap. (Brett Eldridge.)
Industrial Network Security Trends
Established Industrial Security Standards

- International Society of Automation
  - ISO/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

A secure application depends on multiple layers of protection.
Industrial security must be implemented as a system.
Industrial Network Security Trends
Industrial vs. Enterprise Network Requirements

Convergence of Industrial Automation Technology (IAT) with Information Technology (IT)
Industrial Network Security Trends
Industrial vs. Enterprise Network Requirements

**Industrial Requirements**

- **Switches**
  - Managed and Unmanaged
  - Layer 2 is predominant
- **Traffic types**
  - Information, control, safety, motion, time synchronization, energy management
- **Performance**
  - Low Latency, Low Jitter
  - Data Prioritization – QoS – Layer 2 & 3
- **IP Addressing**
  - Static
- **Security**
  - Industrial security policies are inconsistently deployed
  - Open by default, must close by configuration and architecture

**Enterprise Requirements**

- **Switches**
  - Managed
  - Layer 2 and Layer 3
- **Traffic types**
  - Voice, Video, Data
- **Performance**
  - Low Latency, Low Jitter
  - Data Prioritization – QoS – Layer 3
- **IP Addressing**
  - Dynamic
- **Security**
  - Pervasive
  - Strong policies

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

The Established #1 Industrial Ethernet Physical Layer Network Infrastructure

Reduce Risk  Simplify Design  Speed Deployment
Industrial Network Security Trends
IACS Networking Design Considerations

Recommendations and guidance to help reduce **Latency** and **Jitter**, to help increase data **Availability**, **Integrity** and **Confidentiality**, and to help design and deploy a **Scalable, Robust, Secure and Future-Ready** EtherNet/IP IACS network infrastructure

- Single Industrial Network Technology
- Robust Physical Layer
- Segmentation
- Resiliency Protocols and Redundant Topologies
- Time Synchronization
- Prioritization - Quality of Service (QoS)
- Multicast Management
- Convergence-Ready Solutions
- Security - Defense-in-Depth
- Scalable Secure Remote Access
Industrial Network Security Trends
EtherNet/IP Industrial Automation & Control System Network

- **Open by default** to allow both technology coexistence and device interoperability for Industrial Automation and Control System (IACS) Networks

- **Secured by configuration:**
  - **Protect the network**
    - Electronic Security Perimeter
  - **Defend the edge**
    - Industrial DMZ (IDMZ)
  - **Defense-in-Depth**
    - Multiple layers of security
Industrial Network Security Trends
EtherNet/IP Industrial Automation & Control System Network

Flat and Open
IACS Network Infrastructure

Structured and Hardened
IACS Network Infrastructure
Defense-in-Depth
Multiple Layers to Protect the Network 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.
A balanced Industrial Security Program must address both Technical and Non-Technical Elements

- Non-technical controls - rules for environments: e.g. standards, policies, procedures, and risk management
- Technical controls – technology to provide restrictive measures for non-technical controls: e.g. Firewalls, Group Policy Objects, Layer 3 access control lists (ACLs)

- Security is only as strong as the weakest link
- Vigilance and Attention to Detail are KEY to the long-term security success
Defense-in-Depth
Balanced Industrial Security Program - Example

- When a Technical Control is lacking, the non-technical control will only provide so much protection
  - Example: Policy states operators should not surf the web from an industrial automation and control system HMI; however there is no technical control in place preventing such access or behavior

- When a Non-Technical Control is lacking, the technical control will only provide so much protection
  - Example: Firewalls are in place to prevent operators from surfing the web from an industrial automation and control system HMI; however there is no non-technical control in place stating you shouldn’t change the HMI’s network port access to the other side of the firewall

How much security is enough security?

- The amount of security in a system should rise to meet a corporation’s level of risk tolerance.
- In theory, the more security that is properly designed and deployed in a system, the lower the amount of risk that should remain.
Defense-in-Depth
Industrial Security Policies and Procedures

- Security policy - plan of action with procedures (non-technical):
  - Rules for controlling human interactions in automation systems
  - Protect IACS assets, while balancing functional and application requirements such as 24x7 operations, low Mean-Time-To-Repair (MTTR) and high Overall Equipment Effectiveness (OEE).
  - Alignment with applicable industry standards
- Industrial security policy, unique from and in addition to enterprise security policy
- Multi-layer security approach – Defense-in-Depth
  - Procedural, physical and electronic measures
  - Identify Domains of Trust and appropriately apply security to maintain policies
- Risk management:
  - Determination of acceptable risk (tolerance to risk)
  - Assessment - current risk analysis
  - Deployment of risk mitigation techniques

Securing industrial assets requires a comprehensive network security model developed against a defined set of security policies
## 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
- **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) software
- **Device Hardening** – change management, communication encryption, and restrictive access
Network Security Framework
Converged Plant-wide Ethernet (CPwE) Reference Architectures

- Structured and Hardened IACS
- Network Infrastructure
- Industrial security policy
- Pervasive security, not a bolt-on component
- Security framework utilizing defense-in-depth approach
- Industrial DMZ implementation
- Remote partner access policy, with robust & secure implementation

Network Security Services Must Not Compromise Operations of the IACS
Network Security Framework
Controller Hardening

- Physical procedure:
  - Restrict Industrial Automation and Control System (IACS) access to authorized personnel only
    - Control panels, devices, cabling, and control room
    - Locks, gates, key cards
    - Video Surveillance
    - Other Authentication Devices (biometric, keypad, etc.)
  - Switch the Logix Controller key to “RUN”

- Electronic design:
  - Logix Controller Source Protection
  - Logix Controller Data Access Control
  - Trusted Slot Designation
Network Security Framework
Physical Port Security

- Keyed solutions for copper and fiber
- Lock-in, Blockout products secure connections
- Data Access Port (keyed cable and jack)
Network Security Framework
Network Infrastructure Access Control and Hardening

- Cryptographic Image
  - HTTPS (HTTP Secure)
  - Secure Shell (SSH)
  - SNMPv3

- Restrict Access
  - Port Security – Dynamic learning of MAC addresses
  - ACL (Access Control List)
    - Local
    - Authentication through AAA Server

- Quality of Service (QoS)
  - Minimize Impact of DDoS Attacks

- Disable Unnecessary Services
  - MOP (Maintenance Operations Protocol)
  - IP redirects
  - Proxy ARP

- Attack Prevention
  - DHCP Snooping
    - Rogue DHCP Server Protection
    - DHCP Starvation Protection
  - Dynamic ARP Inspection
    - ARP Spoofing, man-in-the-middle attack
  - Storm Control Thresholds
    - Denial-of-service (DoS) attack
Network Security Framework
VLANs, Segmenting Domains of Trust

Flat and Open IACS Network Infrastructure

Structured and Hardened IACS Network Infrastructure
Network Security Framework
Plant Firewall – Unified Threat Management

- Multi-layer packet and traffic analysis
- Advanced application and protocol inspection services
- Network application controls
- Real-time protection from application and OS level attacks
- Network-based worm and virus mitigation
- Spyware, adware, malware detection and control
- On-box event correlation and proactive response
- Flexible user and network based access control services
- Stateful packet inspection
- Integration with popular authentication sources including Microsoft Active Directory, LDAP, Kerberos, and RSA SecurID
- Threat protected SSL and IPSec VPN services
- Zero-touch, automatically updateable IPSec remote access
- Flexible clientless and full tunneling client SSL VPN services
- QoS/routing-enabled site-to-site VPN
- Low latency
- Diverse topologies
- Multicast support
- Services virtualization
- Network segmentation & partitioning
- Routing, resiliency, load-balancing

Modern Firewalls (UTM’s) provide a range of security services
Network Security Framework
Unified Threat Management – Stratix Services Router

Levels 4 & 5 – Data Center
Enterprise Zone

Levels 3.5 - IDMZ
Physical or Virtualized Servers
- FactoryTalk Application Servers & Services Platform
- Network Services – e.g. DNS, AD, DHCP, AAA
- Remote Access Server (RAS)
- Call Manager
- Storage Array

Level 3 - Site Operations
Industrial Zone

Levels 0-2
Cell/Area Zones

Enterprise-wide
Business Systems

Enterprise-zone

Plant-wide
Site-wide
Operation Systems

Enterprise-zone

Remote Site #1

Local Cell/Area Zone #1

Local OEM Skid / Machine #1

Stratix 5900
1) Site-to-Site Connection

Stratix 5900
2) Cell/Area Zone Firewall

Stratix 5900
3) OEM Integration

Site-to-Site Connection

Plant-wide
Site-wide
Operation Systems

Remote Site #1

Local Cell/Area Zone #1

Local OEM Skid / Machine #1

Copyright © 2013 Rockwell Automation, Inc. All rights reserved. 25
• Distribution switches typically provide first hop (default gateway) redundancy
  – StackWise (3750X), stack management
  – Hot Standby Router Protocol (HSRP)
  – Virtual Router Redundancy Protocol (VRRP)
  – Gateway Load Balancing Protocol (GLBP)
Network Security Framework
AAA - Network

1. Authentication
   - Keep the Outsiders Out

2. Authorization
   - Keep the Insiders Honest
   - Personalize the IACS Application

3. Accounting
   - Increase Network Visibility
Network Security Framework
AAA - Network

- Cisco - Identity Services Engine (ISE)

- Combines AAA (authentication, authorization, accounting), posture and profiler into one appliance

- Gathers real-time network information to allow administrators to make network access decisions

- Uses network access control to manage what resources users and guests are allowed to access

- Determines what kind of device users are using, and whether it complies with hardware and software policies

- Manages wired and wireless access with 802.1X
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
Scalable Network Security Framework
One Size Does Not Fit All

Not Recommended

Recommended – Depends ... based on customer standards, security policies and procedures, risk tolerance, and alignment with IACS Security Standards
Network Security Framework
Demilitarized Zone (DMZ)

- Sometimes referred to a perimeter network that exposes an organization's external services to an untrusted network.

- The purpose of the DMZ is to add an additional layer of security to the trusted network.
Network Security Framework
Industrial Demilitarized Zone (IDMZ)

- Sometimes referred to as a perimeter network that exposes an organization's external services to an untrusted network. The purpose of the IDMZ is to add an additional layer of security to the trusted network.
Network Security Framework
Industrial Demilitarized Zone (IDMZ)

- All network traffic from either side of the IDMZ terminates in the IDMZ; network traffic does not directly traverse the IDMZ
  - Only path between zones
  - No common protocols in each logical firewall

- No control traffic into the IDMZ, CIP stays home

- No primary services are permanently housed in the IDMZ

- IDMZ shall not permanently house data

- Application data mirror to move data into and out of the Industrial Zone

- Limit outbound connections from the IDMZ

- Be prepared to “turn-off” access via the firewall
Network Security Framework
Industrial Demilitarized Zone (IDMZ)

- Set up functional sub-zones in the IDMZ to segment access to data and services (e.g. Partner zone, Operations, IT)
IACS Network Security
Design and Implementation Considerations

- Align with Industrial Automation and Control System Security Standards
  - DHS External Report # INL/EXT-06-11478, NIST 800-82, ISO/IEC-62443 (Formerly ISA-99)
- Implement Defense-in-Depth approach: no single product, methodology, nor technology fully secures IACS networks
- Establish an open dialog between Industrial Automation and IT groups
- Establish an industrial security policy
- Establish an IDMZ between the Enterprise and Industrial Zones
- Work with trusted partners knowledgeable in automation & security
- "Good enough" security now, is better than "perfect" security ...never.
  (Tom West, Data General)