Securing Process Control Systems

Bradford H. Hegrat, CISSP, CISM
Sr. Principal Security Consultant
Network & Security Services

Rockwell Automation
Process Solutions User Group (PSUG)
November 14-15, 2011
Chicago, IL - McCormick Place West
Session Abstract

Securing Process Control Networks

This session will share recommendations and generally accepted industry practices for deploying a holistic security program with the intent to secure process manufacturing assets, including FactoryTalk Security and services from Rockwell Automation.

Terms and Definitions

- ICS: Industrial Control System
- PCN: Process Control Network
- IT: Information Technology
- DCS: Distributed Control System
- SCADA: Supervisory Control And Data Acquisition
- EZ, MZ, DMZ: Enterprise, Manufacturing and Demilitarized Zones
- PoLR: Principle of Least Route
Today’s Agenda

1. Definition & Importance of Industrial Security
2. Security Position: An ICS Vendor Perspective
3. Perspective, Background and Theory
4. Going Beyond Defense in Depth
5. Wrap-Up & Summary
6. Five Steps to Enhancing ICS Security

IMPORTANT: Ask Questions throughout!!
This can be a free form discussion.

CONCLUSION: Discussion, Q&A
A Vendor’s Perspective

- Control System lifecycles are long (20+ years)
- Products will have vulnerabilities
- Security is a team sport
  - Vendors & Customers
  - IT & Engineering
  - Pick your teams (point → don’t go it alone)
  - REMEMBER: Human beings are imperfect
- Control System safety and security are closely linked
- Control System security is about managing variables
- Managing the security variables enhances uptime

UPTIME = PROFITABILITY
Trends: Open & Integrated

<table>
<thead>
<tr>
<th>Operating Systems:</th>
<th>Proprietary</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Communication:</td>
<td>Proprietary</td>
<td>Standard Protocols</td>
</tr>
<tr>
<td>Information Flow:</td>
<td>Segmented</td>
<td>Integrated</td>
</tr>
<tr>
<td>Computing Solutions:</td>
<td>Monolithic</td>
<td>Modular &amp; Remote</td>
</tr>
<tr>
<td>Architecture:</td>
<td>Closed</td>
<td>Open</td>
</tr>
<tr>
<td>Users:</td>
<td>Internal</td>
<td>Internal &amp; External</td>
</tr>
</tbody>
</table>

Some key drivers...

- Availability
- Authentication & Authorization (AA)
- Secure Remote Access
- Accounting & Information/IP Protection

Security is a cost of doing business in the 21st century.
in other words...

CONVERGENCE
History: How did we get here?

Manufacturing Network Convergence (as a driver itself)

- Downtime – production control systems
- Lost data – manufacturing, scheduling, tracking and quality
- Theft of intellectual property
- Physical incident
  - Minor personal injury to loss of life
  - Loss of physical assets
- Loss time to market or the loss of public confidence
Theory: Infrastructure Differences

Quite a few...

*Industrial Control System (ICS)*

*vs.*

*Information Technology (IT) Networks*

- Network Detractors
- Open By Default vs. Closed by Configuration
- Data Flows and Intended Use
- Consequences of the negative effects of network anomalies
Network Detractors

Native to IT Networks

• Variability
• Openness
• Quality of End users and administrators

Inherent to ICS Networks

• Typically not the users or operators
• Other than a poor design itself, **latency** is the number one hindrance of control system (more on this later)
• It’s almost never about bandwidth
Open by Default vs. Closed by Configuration

- Typically, office networks are dynamic and will vary greatly based on a number of factors.
- ICS, DCS and SCADA networks are mostly static.
- ICS Mantra = SET IT, FORGET IT, and Forklift Upgrade it in 25 years.

Understanding the static nature of these networks and their data flows is absolutely crucial to their longevity, safety and security.
Both “just pass data” but what is the primary purpose of that Data?

- IT type applications (email, web surfing, SAP, file/print sharing, etc.) are routed off subnet
- Action on/from data is remote
- Data is informational
- Mapping Data flows is easy – it goes “out”

- IT type applications typically have extremely short TCP sessions (3 way handshake – SYN, SYN/ACK, ACK), “PSH - gimme the bits,” FIN under a few seconds, tops)
- PURPOSE: Ubiquitous and unfettered access to every node on the network
- Feature Driven
Data Flows and Intended Use - ICS Networks

• Control oriented applications tend to be tighter in logical distance – many times never leaving one subnet.
• Action on/from data is very localized.
• Data is action.
• Mapping data flow is more difficult.

• Controls type applications tend to have extremely lengthy TCP sessions (3 way handshake, gimme the bits, keep-alive, keep-alive, keep-alive...) lasting hours, days, etc.
• PURPOSE: Secure and stable communications for providing real time access to nodes interacting with physical equipment in the real world (requirements driven).
EPIC FAIL!

• Failure to follow these design principles may have unintended consequences.

• Safety systems may or may not help, depending on the infrastructure.
Consequences: IT Network Issues

Just because you can... doesn’t always mean you should

- Delays, lost packets, viruses/malware or even a hostile network intrusion will cause issues for IT Network administrators.
- Follow incident response plans, stop the event, mitigate the vulnerability and if necessary, restore from backups.

NOTE: This will be painful
Consequences: ICS Network Issues

- ICS Network issues are much more than “data loss” - there are real world, physical consequences
- You cannot fix these “issues” by restoring from backups…

NOTE:
This will be deadly

Just because you can…doesn’t always mean you should
GOING BEYOND DEFENSE IN DEPTH

The Tenets for Designing ICS, DCS and SCADA Networks
To transcend Defense in Depth, one must understand “depth”…

SECURITY IN FOUR DIMENSIONS
Stack Depth: Layers Affect Layers

- Unfortunately this means if one layer is hacked, communications are compromised without the other layers being aware of the problem.
- Security is only as strong as the weakest link.
- Compromise is always bi-directional (vs. network impact model – bottom up).

SECURITY SHOULD BE APPLIED AT EVERY LEVEL!!!

![Diagram showing the stack depth and layers affecting each other.](Image)
Physical Depth: Onion model

- **Physical Security** – limit physical access to authorized personnel: areas, control panels, devices, cabling, and control room – escort and track visitors

- **Network Security** – infrastructure framework – e.g. firewalls with intrusion detection and intrusion prevention systems (IDS/IPS), and integrated protection of networking equipment such as switches and routers

- **Computer Hardening** – patch management, antivirus software as well as removal of unused applications, protocols, and services

- **Application Security** – authentication, authorization, and audit software

- **Device Hardening** – change management, vendor specific security bits and restrictive access

SECURITY SHOULD BE APPLIED AT EVERY LEVEL!!!
Implementation Depth: Products

- **Anti-tamper capabilities**
  - Physical security (controller key switch)
  - CPU Lock (unauthorized access)
  - Read/Write Tags
  - Defined Constants (Persistent Tags)
  - Main Controller Function Blocks are not user accessible

- **Firmware signing**
  - Authenticity

- **Authorization & Authentication**
  - FactoryTalk Security (User Access Control)
  - Integration with Microsoft Active Directory (AD)

- **IP & Know-how Protection**
  - Source code
  - Custom routines
Persistence Depth: People

- **People as a design element:** Who owns the network? Who maintains the network?
- Problem of people, not technology. Understanding/backgrounds, mindsets and roles – key to security design principles

- Protocols that “think” for you don’t belong in the ICS/DCS/SCADA realm, such as auto negotiation and DHCP. There are a few exceptions such as routing.
- Defaults are just THAT. Defaults. They beg to be changed.

The good guys need to track ALL variables (including people).
On to the bits... infusing

SECURITY DNA

for inherently defensible architectures
Security Design - the Attributes

- **Principle of Least Route (PoLR)**
  - Principle of Least Privilege applies to Applications/User level system access
  - PoLR applies to network “reachability.”
  - This means small subnets and ACLs (subnet = /29 or /28)

- Zone Segmentation is required (i.e. DMZs). The ‘VLAN for Security Zone Separation’ model is **BROKEN, ANTIQUATED, and RISKY**.

- Monitoring is REQUIRED
  - Revisits the IDS/IPS argument
  - Is IDS dead?
  - Is IPS appropriate for the ICS environment? Interior? Fringe?

Don’t forget Microsoft:
IPsec Filters via GPO, netsh, WF/ICS, WMIC, PowerShell, etc...
• Functional Security Sub-zones in the DMZs
• All traffic traverses the Firewall for DMZ communications
• Control-specific protocols should NEVER route to/through the DMZ
Security Design - the Infrastructure

- Security is **not** a bolt-on
- **Lead with a comprehensive ICS Security Program**
- Implement an Automation DMZ for:
  - Remote Engineering Access
  - Remote 3rd Party Access
  - Secure MZ ↔ EZ programmatic data transfer
  - Secure EZ ↔ MZ management data transfer
  - A means to buffer inter-zone data in the event DMZ connectivity is disrupted
  - Wireless Integration

**Network Security Services Must Not Compromise Operations of the Cell/Area Zone**
Why the PoLR Methodology?!?
The answer: Latency & Security

- In a typical command execution in the ICS, DCS and SCADA environment, there are a number of serialized communications.
- From the point of command execution, the bits must flow all the way down to the IO devices (which could be Ethernet based).
- Each TCP session is a point where data is in motion.
- Network transmissions introduce the potential for latency.
- EVERY point in this path has a significant attack footprint and represents risk to the process.
Latency & Compromise Potential

- Potential for many points of latency
- Presents the case for architectural improvements (small subnets, Layer 3 switching, etc)
- This example ONLY focuses on the Transport Layer and down (OSI model)
- Does not take into account Session and Application layer issues:
  - DNS
  - Microsoft Active Directory
  - OPC
Concept: Applying the Scientific Method to Network Security Design

- Collection of data (user and process requirements)
- Through observation and experimentation (specification and design generation)
- Formulation and testing of hypotheses (design documentation, network build out/testing, functional testing, FAT/SAT, etc)
- While reducing variables and variability in the systems (system hardening)
Reviewing the lessons, application to the future and verification of success

SECURITY IN SUMMARY
Qualification

How do I KNOW my infrastructure is good?

- Verify all physical media installations are up to specification
- Operationally measure and document utilization and throughput across every:
  - End node
  - Uplink and Access ports
  - Switch backplane
- **STRESS TEST THE NETWORK**
  - Use the same base, size, type protocols used in the Control System
  - If the network was designed to X capacity, test performance at 2X, 3X or 5X traffic
  - Probe “Principle of Least Route” deployment (i.e. “lets see what we can get to…”)
  - Test “worse case” scenarios to ensure Control System continued performance. Self Induced DoS is never a good thing...
    - i.e. every alarm, event and trend kicks off at the same time during a network impacting event.
Steps to Increasing Security

1. Create a Program

NOTE: This is different than an Enterprise Security Program.

Industrial Control System Security Program

Technical Security Controls
- Firewalls, Web Application Firewalls
- Control System Protocol Firewalls
- Traditional SPI/DPI 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 Route

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

Constant & Enduring Vigilance. No Exceptions.

“Programs” drive accountability, action and responsibility.
2. Know what you have in your process

- Every control system event must be coded. EVERY ONE!
- This means that every almost network event can be predicted
  - Some exceptions, like ARP, NetBIOS traffic, etc.
- If it can be predicted, it can be whitelisted and authorized via tiered firewall rule sets and layer 3 access control lists (ACLs)
- If these can be whitelisted, other network events can be tuned for disclosure in intrusion detection and prevention systems (IDS/IPS)

Knowing what you have in your process allows for the creation of a defensible network architecture and response posture

REMEMBER: Security is about variable management.
Steps to Increasing Security (cont)

3. Harden your endpoints

- Enable the security features of products implemented in the environment!
- Configure what you already have in the environment
  - Most Microsoft Windows platforms now support firewalls. Use them.
  - Enable Infrastructure & Application security features (Active Directory features, etc.)
  - Enable Control System software and hardware security features (key switch, etc.)
- Through the processes created in the Industrial Control System Security Program (see step 1), maintain ICS life cycle by enacting:
  - Endpoint Protection updates (patches, virus definitions, host IDS/IPS signatures, etc)
  - Change and Configuration management

Variables: Good guys need to manage all of them. The bad guys only need one variable for compromise...
Steps to Increasing Security (cont)

4. Audit the Environment

Design/Implementation Audits
- Configuration audits to verify end states conforms to the Conceptual and Detailed Design projects
- Very important as “things change” during implementation

Safety Audits
- Many times required by regulation – now part of the common “culture”

Security Audits
- Many times required by regulation (depending on industry)
- Ensures proper security management going forward (i.e. hire/fire procedures, governance and security programs, etc.)
- Security should be and will be part of the common “culture”
5. Monitor the Systems

SI VIS PACEM, PARA BELLUM
If you wish for peace, prepare for war.

- Infrastructure: double edged sword
  - The purveyance of an attack (vector)
  - Greatest asset in digital protection (mitigation)
- Many Commercial & FOSS packages available to assist
  - Multi-Tier and Distributed UTM and Intrusion Detection/Prevention Systems
  - Distributed packet capture, Syslog, SNMP, Nagios and various management apps

If you wish for a stable, secure network, prepare for the day your network completely falls apart, fails, and turns against you.

COMPLACENCY KILLS—100% VIGILANCE IS REQUIRED
The End...for now...

- Go Beyond Defense-in Depth: no single methodology nor technology fully secures industrial networks.

- **This is a people problem too!**
  - Industrial Control Systems Security Programs are uniquely different from Enterprise Security Programs
  - Work with Rockwell Automation Network & Security Services team and establish an open dialog between Manufacturing and IT
Process Security 2012 & Beyond...

- It’s about continuing Partnering & Collaboration efforts
  - Users, Vendors, Researchers and Agencies
  - Cooperation and coordination
- It’s about enhancing Communication
  - Needs, desires and vigilance
  - Interdepartmental relationships
  - Consistency and Objectivity
- It’s about furthering Standards
  - Process, Policy & Procedures (with compensating controls)
  - Internal and External - emerging global standards
  - Continuous Improvement (Suppliers & Users)
- It’s about ongoing Acknowledgement and Addressing Risk
  - Everybody has something to lose
  - Everybody has something to protect

IGNORING RISK IS NOT AN OPTION
Network & Security Services

ASSESS

• Assess the current state of the security program, design, policy
• Assess the current state of the network design, implementation
• Assess the current state of a manufacturing data center

DESIGN/PLAN

• Design and plan a network infrastructure
• Design and plan security program, policy, infrastructure, business continuity plan
• Design and plan a SANs infrastructure

IMPLEMENT

• Installation, procurement and configuration of a network
• Implementation of a security program, infrastructure design, policy training
• Installation, procurement and configurations of a SANs infrastructure

AUDIT

• Audit current architecture compared to governing body (ODVA, IEEE, ANSI/TIA)
• Audit security program compared to governing body (NERC CIP, ISA-99, NIST 800-53, NIST 800-82)

MANAGE/MONITOR

• Manage, maintain and monitor uptime and issues on networks (LAN, SAN, WAN)
• Managed Security Services (Incident response, disaster recovery, monitoring)
Additional Resources

- Website: [http://www.rockwellautomation.com/security](http://www.rockwellautomation.com/security)

- Whitepapers
  - Reference Architectures for Manufacturing
  - Securing Manufacturing Computer and Controller Assets
  - Production Software within Manufacturing Reference Architectures

- Design and Implementation Guides
  - ODVA - Network Infrastructure for EtherNet/IP: Introduction and Considerations
  - ODVA - EtherNet/IP Media Planning and Installation Manual
  - Rockwell Automation and Cisco Design and Implementation Guide – manufacturing reference architectures
Additional Resources - Webcasts

Rockwell Automation and Cisco webcasts:

- What Every IT Professional Should Know about Plant Floor Networking
- What Every Plant Floor Controls Engineer Should Know about Working with IT

Rockwell Automation Knowledge Network webcasts:

- Rockwell Automation and Cisco: Best Practices
- Reference Architectures: Fundamentals of Ethernet Network Design
- Securing Manufacturing and Enterprise Network Convergence
- Industrial Ethernet Resiliency
Thank You!!!
Questions? Comments?

Bradford H. Hegrat, CISSP, CISM
bhhegrat@ra.rockwell.com
+1.440.840.5145