Fundamentals of Securing EtherNet/IP Networks

Plant-wide Benefits of EtherNet/IP Seminar
Agenda

- Industrial Network Security Trends
- Defense-in-Depth
- CPwE Network Security Framework
- Scalable Secure Remote Access
- Additional Information
Security concerns are just another consideration in an ever-changing world.
Industrial Network Security Trends
Commonly Reported Business Disruptions

- Application of Security patches
- Theft
- Denial of Service
- Unauthorized actions by employees
- Unauthorized remote access
- Unauthorized access
- Natural or Man-made disasters
- Worms and viruses
- Sabotage
- Unintended employee actions

Unaddressed security risks increase potential for disruption to IACS uptime and safe operation
Industrial Network 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

A secure application depends on multiple layers of protection. Industrial security must be implemented as a system.
Logical Model
Converged Multi-discipline Industrial Network
Industrial Network Security Trends

Industry Security Standards

- Network and Security Services
  - NERC CIP (Critical Infrastructure Protection) Compliant Security Program
- Four phased approach used to assist asset owners in NERC CIP compliance
- Phases include the creation of
  - Main Governance Framework
  - Technical Assessment Services
  - Physical Security Services
  - Training
- Deliverable for any phase
  - Current state documentation
  - Future state recommendations
  - Options for remedial action
Industrial Network Security Trends

Network Technology Convergence

**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?**
Industrial Network Security Trends
Common Industrial Protocol (CIP)

- Open standard to integrate control, device configuration and data collection for Industrial Automation and Control Systems
- Open by Default
  - Secured by configuration
- Security stance is required
  - Protect the network
  - Defend the edge
  - Defense-in-Depth
Security is essentially two pronged:
- **Technical** vs. **Non-technical**
- A **balanced** Security Program must address both Technical (technology) and Non-Technical (policies and procedures) Elements

- Technical controls - Firewalls, Group Policy Objects, Layer 3 ACLs, etc. - provide restrictive measures for non-technical controls
- Non-technical controls - rules for environments, such as policy and procedure, risk management
- Security is only as strong as the weakest link
- Vigilance and Attention to Detail are KEY to the long-term security success
When a Technical Control is lacking, the non-technical control will only provide so much protection
- Example: Policy states you should not surf the web from a 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 a 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
Security Policies and Procedures

- Comprehensive network security model
  - Multi-layer security approach – Defense-in-Depth
    - Procedural, physical and electronic measures
  - Alignment with applicable industry standards
  - Risk assessment:
    - Determination of acceptable risk
    - Current risk analysis
    - Deployment of risk mitigation techniques

- Security policies
  - Policy - plan of action with procedures to protect company assets
    - Non-Technical: Rules for controlling human interactions in complex systems
  - Security policies are unique from company to company, although there are some common attributes and methodology to developing
  - Industrial security policy, unique from and in addition to enterprise security policy
  - Identify Domains of Trust and appropriately apply security to maintain policy

Securing industrial assets requires a comprehensive network security model developed against a defined set of security policies
## Industrial Network Security Trends

### Industrial vs. Enterprise Network Requirements

<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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Precedence of Priorities</th>
<th>Industrial (IAT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Types of Data Traffic</th>
<th>Industrial (IAT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Converged network of data, control, information, safety and motion</td>
<td>Converged network of data, voice and video</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Industrial (IAT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implications of a Device Failure</th>
<th>Industrial (IAT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Production is down ($$’s/hour … or worse)</td>
<td>Work-around or wait</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Protection</th>
<th>Industrial (IAT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Isolate threat but keep operating</td>
<td>Shut down access to detected threat</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upgrades</th>
<th>Industrial (IAT) Network</th>
<th>Enterprise (IT) Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scheduled during downtime</td>
<td>Automatically pushed during uptime</td>
</tr>
</tbody>
</table>
Defense-in-Depth
Multiple Layers to Protect the Network and Defend the Edge

- **Physical Security** – limit physical access to authorized personnel: Cells/Areas, control panels, devices, cabling, and control room. This may also include policies, procedures and technology to escort and track visitors
- **Network Security** – infrastructure framework – e.g. unified threat management (UTM) security appliances and integrated protection of networking assets 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 accounting (AAA) software
- **Device Hardening** – change management, controller communication encryption, and restrictive network connectivity through authentication
Defense-in-Depth
Physical Security - Examples

- Keyed solutions for copper and fiber
- Lock-in, Blockout products secure connections
Defense-in-Depth
Computer Hardening - Examples

- Security Patch Management - establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches
  - Keep computers up-to-date on service packs and hot fixes
    - Disable automatic updates
    - Check software vendor website
    - Test patches before implementing
    - Schedule patching during downtime
  - Deploy and maintain Anti-X (e.g. - virus, spyware, malware) detection software
    - Disable automatic updates and automatic scanning
    - Test definition updates before implementing
    - Schedule manually initiated scanning during downtime
- Uninstall unused Windows components
  - Protocols and Services
- Protect unused or infrequently used USB, parallel or serial interfaces
Defense-in-Depth
Product & System-level Security: Microsoft Patch Management

White paper
Computer System Security Updates: Why patch your computers?

Knowledgebase Article #: 35530*
Microsoft Patch Qualification for Rockwell Automation software products

*TechConnect support contract required

http://rockwellautomation.custhelp.com/app/answers/detail/a_id/35530
RA Knowledgebase

- **Answer ID# 54102**
- Summary and links to RA Security-related Disclosures relating to RA products
- Page updated as new articles added to Knowledgebase
- Updates to page can be pushed to subscribers

Recommendation:
- Register account on KB
- Subscribe to article #54102 as “Add to My Favorite”
Defense-in-Depth
Controller Hardening - Examples

- Physical procedure:
  - Restrict Industrial Automation and Control System (IACS) access to authorized personnel
  - Switch the Logix Controller key to “RUN”
Defense-in-Depth
Controller Hardening - Examples

- Electronic design - Logix Controller Source Protection
  - Source Protection to lock down Add-On Instruction
  - Viewing can be permitted if desired
  - V19 enhancements
    - Source Key values are obfuscated in Studio 5000
    - Source Keys can also be named. The name is displayed in place of the Source Key value
Defense-in-Depth
Controller Hardening - Examples

- Electronic design - Logix Controller
  Data Access Control
  - Users can assign External Access
    settings of Read/Write, Read Only, or
    None to tags
  - Useful to control which tags can be
    modified from an HMI or other external
    application
  - A cryptographically licensed trusted
    connection is established between Studio
    5000 and the Logix controller
    - Ensures tags designated as Read-Only or
      None can only be changed by Studio 5000
  - Users can also define tags as Constants.
    - Constants can not be modified by
      controller logic

Improves security of tags
especially when used in conjunction with
FactoryTalk Security or the CPU Lock tool
Defence-in-Depth
Controller Hardening – Examples - Trusted Slot Designation

- A ControlLogix controller can have a trusted communication module(s) to restrict the valid communications path to/from the controller.
- When configured, ControlLogix controller will reject any attempt to connect to it with Studio 5000 or RSLogix through any other module.
Defense-in-Depth
Authentication, Authorization, Accounting (AAA)

1. Authentication
   Who are you?
   Keep the Outsiders Out

2. Authorization
   Where can you go?
   Keep the Insiders Honest

3. Accounting
   What service level do you receive?
   Personalize the IACS Application

4. Accounting
   What are you doing?
   Increase Network Visibility
Defense-in-Depth
Application Security - Examples

- Use FactoryTalk Security to
  - Manage the insider threat by authenticating the user and authorizing the use of Rockwell Automation software applications used to access automation devices.

- How does it work?
  - Provides centralized A&A by verifying the identity of each user and;
  - Granting or denying each user's request to perform a particular set of actions on resources within the system.
Defense-in-Depth
Application Security - Examples

- Safety Lock / Unlock
- Safety Signature Create / Delete
- OpenProject
- CopyFrom
- ExportTags
- GoConnected
- GoOnline
- SaveProject
- SaveProjectAs
- ConvertProject
- CompactProject
- ExportProject
- DownloadProject
- UploadProject
- ChangeControllerMode
- EditProjectCommPath
- ChangeTagValue
- RecreateProject
- EditControllerProperties
- EditControllerPrograms
- EditSerialPorts
- EditCST
- LockControllerCreateTask; DeleteTask; EditTask
- CreateProgram; DeleteProgram; EditProgram
- CreateTag; DeleteTag; EditTag
- CreateUDT; DeleteUDT; EditUDT
- CreateModule; DeleteModule
- CreateRoutine; DeleteRoutine
- EditRoutineProperties
- EditRoutine
- AxisDirectCommand

With FactoryTalk Security, administrators can secure these actions in Studio 5000 (partial list)...
Network Security Framework
Converged Plant-wide Ethernet (CPwE) Reference Architectures

- 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 Cell/Area Zone
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)

- 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)
Network Security Framework
Industrial Demilitarized Zone (IDMZ) – Application Mirror
| Firewall with Application Layer Security | Multi-layer packet and traffic analysis  
Advanced application and protocol inspection services  
Network application controls |
|------------------------------------------|----------------------------------------------------------------------------------|
| IPS and Anti-X Defenses                  | 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 |
| Access Control and Authentication         | 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 |
| SSL and IPSec Connectivity               | 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 |
| Intelligent Networking Services          | Low latency  
Diverse topologies  
Multicast support  
Services virtualization  
Network segmentation & partitioning  
Routing, resiliency, load-balancing |

Modern Firewalls (UTMs) provide a range of security services
Network Security Framework
Unified Threat Management (UTM)

- Enterprise-wide Business Systems
  - Levels 4 & 5 – Data Center
  - Enterprise Zone

- Plant-wide Site-wide Operation Systems
  - Levels 3 - Site Operations
  - Industrial Zone
  - Level 3.5 - IDMZ

- Remote Site #1
  - Local Cell/Area Zone #1
  - Plant-wide Site-wide Operation Systems

- Local Cell/Area Zone #1
  - Remote Access Server (RAS)
  - Call Manager
  - Storage Array

- Levels 0-2
  - Cell/Area Zones

- Stratix 5900
  - 1) Site-to-Site Connection
  - 2) Cell/Area Zone Firewall
  - 3) OEM Integration

- Local OEM Skid / Machine #1

- UTM
  - Site-to-Site Connection
  - OEM Integration

- EtherNet/IP
  - 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
Network Security Framework
Unified Threat Management (UTM) – Stratix 5900

- The Stratix 5900 UTM security appliance is a ruggedized all-inclusive UTM with features such as firewall, secure routing, VPN (virtual private network), intrusion prevention, NAT (network address translation) and content filtering.

- Site-to-Site Connection, tunnels the Industrial Zone trusted network to a remote site over an untrusted network using a site-to-site VPN connection.

- Cell/Area Zone Firewall, to protect a Cell/Area Zone from the greater Industrial Zone.

- Physical features
  - RJ-45 Gigabit WAN
  - 4 – 10/100Base-Tx LAN ports
  - Shock /Vibration & Extended Temperature
  - DIN rail mount

- Network features
  - ACL / Firewall
  - DHCP
  - QoS
  - VLAN
  - NAT

Stratix 5900 Security Appliance
Network Security Framework
Controller Secure Communications

2b) IPsec tunnel from 1756-EN2TSC module to Cisco ASA Firewall
IPsec tunnel from ASA Firewall to Windows Server 2008

2a) IPsec tunnel from 1756-EN2TSC module to Windows Server 2008

1) IPsec tunnel between two 1756-EN2TSC modules

1756-EN2TSC

Local Cell/Area Zone #1

Local Cell/Area Zone #2

Local Cell/Area Zone #3

Levels 4 & 5 – Data Center
Enterprise Zone

Level 3.5 - IDMZ

Level 3 - Site Operations
Industrial Zone

2b) IPsec tunnel from 1756-EN2TSC module to Cisco ASA Firewall
IPsec tunnel from ASA Firewall to Windows Server 2008

3) L2TP tunnel from Windows 7 client to 1756-EN2TSC module

UTM

Workstation

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

Local Cell/Area Zone #1

Levels 0-2
Cell/Area Zones
The ControlLogix (PAC) 1756-EN2TSC secure communication module utilizes either IPsec (IP security) or L2TP (Layer 2 Tunneling Protocol) to provide authentication and data encryption over a trusted CPwE network:

- Authentication of the communication end points (both client and server)
- Data authenticity and integrity (via message integrity checks)
- Data confidentiality (via encryption algorithms)

**ControlLogix to ControlLogix**
- Permanent connection for peer to peer ControlLogix communications, IPsec-encrypted tunnel between the two 1756-EN2TSC modules

**ControlLogix to Data Server**
- Permanent connection between ControlLogix and data server applications
- Smaller applications, IPsec-encrypted tunnel from 1756-EN2TSC module to Windows Server 2008
- Larger applications, IPsec-encrypted tunnel from 1756-EN2TSC module to Cisco ASA firewall, then IPsec-encrypted tunnel from ASA firewall to Windows Server 2008

**Workstation to ControlLogix**
- Ad hoc temporary connection for ControlLogix configuration and management, L2TP-encrypted tunnel from Windows 7 client to 1756-EN2TSC module
Network Security Framework
Controller Secure Communications

- Once the IPsec association is established, data between two endpoints is fully encrypted
- As many as 8 IPsec or L2TP tunnels per module
- Advanced Encryption Standard (AES) 256
  - NIST standard for the encryption of data
- The module supports the same number of TCP and CIP connections as the 1756-EN2T module (256 CIP connections and 128 TCP/IP connections).
- Supports the ControlLogix trusted slot feature
- USB port and IP address configuration switches can be disabled
- This module is intended for use within the trusted CPwE Industrial Network Security Framework. This module is not intended for use on an untrusted network.
Security Solutions

Work With Us to Help Mitigate Your Risk

Similar to the key tenants of integrity, safety, system availability and performance, security has become essential in the design and operation of contemporary control systems. Rockwell Automation recognizes the importance of security for industrial control applications. We embrace the employment of defense in depth practices to mitigate risk through a layered, system-level security approach.

We offer tools, products and services that can help you build security into your control system. In addition, our Network and Security Services capabilities help you design, troubleshoot and verify that your system meets the level of security that is right today and tomorrow.

Although security is merely one aspect of a complete, system-level control solution, it remains an integral aspect to the Rockwell Automation controls philosophy and we remain committed to evolve security solutions to meet your needs:

- Membership ☆ Leadership: Applying Standards to Help Your Security
- Process Control Security Architecture
- Global Security Compliance

Have a security concern? Email us with your question or comments. To address specific concerns, or to report issues you may have with Rockwell Automation products as employed in larger systems, you can contact us at secure@ra.rockwell.com.

Communicate securely with us using PGP. Our Public Key Ring can be found here. Learn more about Pretty Good Privacy (PGP) and Asymmetric key cryptography.

secure@ra.rockwell.com
Industrial 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, ISA/IEC-62443 (Formerly ISA-99)
- Implement Defense-in-Depth approach: no single product, methodology, nor technology fully secures industrial networks
- Establish an open dialog between Industrial Automation and IT groups
- Establish a Industrial security policy, unique from Enterprise security policy
- Establish a IDMZ between the Enterprise and Industrial Zones
- Work with Rockwell Automation Network and Security Services team
- Practice 5 simple, actionable steps to enhance industrial security:
  1. Control who has access
  2. Employ firewalls and intrusion detection/prevention
  3. Patch and update your system
  4. Manage your passwords
  5. Turn the processor key(s) to Run mode
Secure Remote Access – What does this mean to you?
- Intermittent, Ad hoc Connection?
- Permanent, Site-to-Site Connection?
Design Considerations

Business Challenges Facing Operations

Implementation of Lean Initiatives Through Better Asset Optimization

- Reduce scheduled and unscheduled downtime; increase Overall Equipment Effectiveness (OEE)
- Affects of resource downsizing; challenges of aging workforce replacement
- Leveraging shared and distributed company resources
- Leveraging expertise of partners
  - Equipment Builders
  - System Integrators
  - Automation and networking vendors
  - Contractors
- Simplify asset management – change management, version control, regulatory compliance, and software license management
- Network and application authentication and authorization
- Simplify remote client health management
Design Considerations
Trusted Partners Value Differentiation

- Global availability of equipment, machines and services
- Scalable service differentiation
  - Equipment Builders, System Integrators, vendors, contractors
- Equipment Builder cost pressures
  - Machine / Skid build cost
  - On-site commissioning; reduction in resources and duration
  - Warranty support; dispatching of resources
  - Optimization services; partnership vs. supplier
- IT-ready solutions
  - Elimination of security back doors
  - Holistic industrial network infrastructure security solutions
Design Considerations
Remote Access Challenges

- Industrial Automation and Control System (IACS) applications are often managed by plant-wide / site-wide personnel, while enterprise-level remote access solutions such as VPNs are the responsibility of the IT organization.
- Remote access can expose critical IACS applications to viruses, malware and other risks that may be present when using remote or partner computers, potentially impacting operations.
- Limiting the accessibility to only functions that are appropriate for remote users (role and location based authorization).
Design Considerations
Solution is Application Driven

- It's not about the technology, it’s about:
  - Security policies and procedures – Enterprise and Industrial
  - Industrial Automation and Control System (IACS) Security Standards (ISA/IEC-62443, NIST 800-82)
- One-size-does-not-fit-all:
  - Industry type requirements
  - Customer application requirements
  - Customer size and support infrastructure
- Scalable “best” solution … must avoid good/better/best approach
- Balance between technology (technical) and procedures (non-technical)
Design Considerations
Solution is Application Driven

- For industrial plants and sites, ask yourselves these questions:
  - Do you have an IT security policy?
  - Do you have an Industrial security policy?
  - If yes, do you have a remote access policy for employees
    - What remote access technology and products do you utilize?
  - If remote access policy exists, do you have a “partner” remote access policy and the ability with methodology to manage partner access?
  - If yes, do you have a secure tunnel from your enterprise network to the Industrial Automation and Control System plant-wide / site-wide network?

- Partners (e.g. OEM, SI), these are the type of questions to ask your customers’ IT departments, also ask yourselves:
  - How convergence-ready is my solution?
Converged Plant-wide Ethernet (CPwE) Model – Option 1

Secure remote access for employees and trusted partners
- Meeting the security requirements of IT while enabling plant/site personnel to leverage trusted partners and shared, distributed company resources
- Common IT Infrastructure
- Following established IACS security standards
- Enables remote asset management: monitoring, configuration and audit
- Helps simplify change management, version control, regulatory compliance and software license management
- Helps simplify remote client health management
- One size does not fit all – scalable secure solutions
CPwE – Option 1 Solution

Remote Engineer or Partner

Cisco VPN Client

Internet

Enterprise Zone Levels 4 and 5

Industrial Demilitarized Zone (IDMZ)

Industrial Zone Site Operations and Control Level 3

Cell/Area Zones Levels 0–2
1. Remote engineer or partner establishes VPN to corporate network; access is restricted to IP address of IDMZ firewall.
CPwE – Option 1 Solution

1. Remote engineer or partner establishes VPN to corporate network; access is restricted to IP address of IDMZ firewall

2. Portal on IDMZ firewall enables access to industrial application data and files
   - Intrusion protection system (IPS) on IDMZ firewall detects and protects against attacks from remote host
1. Remote engineer or partner establishes VPN to corporate network; access is restricted to IP address of IDMZ firewall

2. Portal on IDMZ firewall enables access to industrial application data and files
   - Intrusion protection system (IPS) on IDMZ firewall detects and protects against attacks from remote host

3. Firewall proxies a client session to remote access server
CPwE – Option 1 Solution

1. Remote engineer or partner establishes VPN to corporate network; access is restricted to IP address of IDMZ firewall

2. Portal on IDMZ firewall enables access to industrial application data and files
   - Intrusion protection system (IPS) on IDMZ firewall detects and protects against attacks from remote host

3. Firewall proxies a client session to remote access server

4. Access to applications on remote access server is restricted to specified plant-wide/site-wide resources through industrial application security
CPwE – Option 1 Solution

IDMZ

FactoryTalk Application Servers
- View
- Historian
- AssetCentre
- Transaction Manager

FactoryTalk Services Platform
- Directory
- Security/Audit
- Data Servers

Cisco Adaptive Security Appliance (ASA) 5520 Firewall

Industrial Zone

Cisco 3750G StackWise Layer 3 Distribution Switch

Remote Access Server
- Remote Desktop Services
- Studio 5000
- FactoryTalk View Studio
- RSLinx Classic / Enterprise

Cell/Area Zones

Stratix 8000
Rockwell Automation
IE Managed
Layer 2 Access Switch

ControlLogix
Rockwell Automation
Programmable
Automation Controller

IACS Asset Protection
- Network Authorization
- Application Authorization
- Change management control
- Audit

Ring Topology

EtherNet/IP

Copyright © 2013 Rockwell Automation, Inc. All rights reserved.
CPwE – Option 1 Solution

IDMZ

SSL VPN

Industrial Zone

Cell/Area Zones

Cisco Adaptive Security Appliance (ASA) 5520 Firewall

FactoryTalk Application Servers
- Managed
- Historian
- Asset Centre
- Transaction Management
FactoryTalk Service
- Directory
- Security/Audit
Data Servers

SSL VPN Service

Please enter your username and password

USERNAME: 

PASSWORD: 

Login
CPwE – Option 1 Solution
CPwE – Solution

IDMZ

- FactoryTalk Application Servers
  - Main
  - Historian
  - Asset Centre
- Transaction Manager
- FactoryTalk Services Platform
  - Directory
  - Security
- Data Server

Industrial Zone

- Remote Access Server
  - Terminal Server
  - RSLinx Classic / Enterprise
- ControlLogix
  - Rockwell Automation Programmable Automation Controller

Cell/Area Zones

- Strata-8000
  - Rockwell Automation Managed
  - Layer 2 Access Switch

RDP
CPwE – Solution

IDMZ

Industrial Zone

Cell/Area Zones

ICS Asset Protection
- Network Authorization
- Application Authorization
- Change management control
- Audit

Stratix 8000
Rockwell Automation
IE Managed Layer 2 Access Switch

ControlLogix
Rockwell Automation
Programmable Automation Controller

Cisco Adaptive Security Appliance (ASA) 5520 Firewall

FactoryTalk Application Servers
- Main
- Historian
- Asset Centre
- Transaction Manager

FactoryTalk Services Platform
- Directory
- Security/Audit
- Data Servers

Cisco 37950
Rockwell Layer 3 Distribution Switch

Remote Access Server
- Terminal Server
- RSLogix 5000
- FactoryTalk View Studio
- RSLogix Classic/E Enterprise
CPwE – Solution

IDMZ

Industrial Zone

Cell/Area Zones

ICS Asset Protection
- Network Authorization
- Application Authorization
- Change Management Control
- Audit

Remote Access Server
- Terminal Server
- RSLogix 5000
- FactoryTalk View Studio
- RSView Classic / Enterprise
Industrial Automation and Control System Asset Protection

- Network and application authentication and authorization
- Change management and version control
- Audit and regulatory compliance
Fundamentals of Securing EtherNet/IP Networks

Plant-wide Benefits of EtherNet/IP Seminar