Security for the Connected Enterprise

Architectural Security Framework

FactoryTalk Applications
- FactoryTalk AssetCentre
- A set of asset-centric tools to securely manage your production environments.
- Tracks users' actions, manages asset-configuration files, and provides backup and recoveryof operating asset configurations
- Monitor the Audit Value and read in the Controller Log

FactoryTalk Services
- FactoryTalk Security
- A part of the FactoryTalk software suite that provides centralized role-based access-control.
- Data Access Control
- Provides user access controls and role-based security to Controllers, HMI and Software
- Allows the administrator to configure who can change all of the tags in the controller

Stratix 8300
- Port Security – Dynamic learning of MAC addresses
- ACL (Access Control List) - Local/ Authentication through AAA Server
- Quality of Service (QoS) - Minimize Impact of DDoS Attack
- Device Authentication with Learn Mode
- Programmable port control (on/off)
- Unauthorized device identification
- HTTP Secure-Encrypted administrative traffic
- VLANs, Segmenting Domains of Trust

FactoryTalk Client
- User Authentication
- FactoryTalk View Site Edition (SE) Security can be applied to:
  - Displays
  - Objects
  - Applications

CompactLogix
- Switch Mode key to "RUN"
- Physically Protect EtherNet/IP Ports
- Keyed, Lock-in, Blockout Port Products
- Firmware Digital Signatures
- Program Change Detection and Logging
- Program Source Protection
- Program Data Access Control

Cell Area
- Restrict access to authorized personnel only
- Control panels, devices, cabling, and control room
- Locks, gates, authentication devices, surveillance

Enterprise Zone
Levels 4 and 5

Patch Management
Terminal Services
Application Mirror
AV Server

Firewall (Active)

Firewall (Standby)

Cisco ASA 5500

Gbps Link for Failover Detection

Industrial Demilitarized Zone (IDMZ)

Industrial Demilitarized Zone (IDMZ)

Industrial Zone
Levels 0-3

Physical or Virtualized Servers

FactoryTalk Application Servers
View
Historian
Asset Center
Transaction Manager

FactoryTalk Services Platform
Directory
Security/Audit

Data Servers

Catalyst 3750X

Site Operations
Level 3

Catalyst 6500
Route Switch Processor

Catalyst 3750X
Distribution Switch
Switch Stack

FactoryTalk Client

Stratix 5900
- Zone-Based Policy Firewall (ZFW)
- Permit/deny traffic to enter/leave a Security Zone based on explicit preconfigured policies/rules

Stratix 8300

Stratix 5700

Stratix 5700 with DLR

Level 2 HMI

Level 1 Controller

Level 0 Process

Stratix 5900

Cell/Area Zones
Levels 0-2

Level 2 HMI

Level 1 Controller

Level 0 Process

Cell/Area Zones
Levels 0-2

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

Stratix 5700
- 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
- Device Authentication with Learn Mode
- Programmable port control (on/off)
- Unauthorized device identification
- HTTP Secure-Encrypted administrative traffic
- VLANs, Segmenting Domains of Trust

Panelview
- User Authentication
- FactoryTalk View Site Edition (SE)
- Security can be applied to:
  - Displays
  - Objects
  - Applications

ControlLogix
- Switch Mode key to "RUN"
- Physically Protect EtherNet/IP Ports
- Keyed, Lock-in, Blockout Port Products
- Firmware Digital Signatures
- Program Change Detection and Logging
- Program Source Protection
- Program Data Access Control
- Trusted Slot Designation
- Encrypted Communications (1756-EN2TSC)

Note: Information presented here is for illustrative purposes only

Rockwell Automation

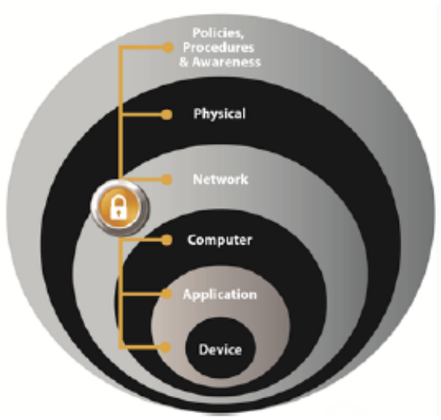
Security Considerations in Converged Plantwide Ethernet (CPwE) Architectures

Publication IASIMP-QR035B-EN-E

Defense-in-Depth

Multiple Layers to Protect the Network and Defend the Edge

- **Physical** – limit physical access to authorized personnel: Policies, procedures, and technology to escort/track visitors
- **Network** – security framework, 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



A balanced **Industrial Security Program** must address both Technical and Non-Technical Elements

Non-technical controls - rules for environments: e.g. standards, policies, procedures, training 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)

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

Ten Actionable Steps

Enhance your industrial reliability and security with these ten actionable steps.

1. Control who has access to various areas of your network using features such as Access Control Lists and port blocking features.
2. Ensure robust and reliable operations by limiting and managing network traffic through the use of Firewalls and Intrusion Detection/Prevention Systems.
3. Protect PC assets by using anti-virus and application whitelisting. Reference material: Achieving Secure, Remote Access to Plant-Floor Applications and Data, Publication # ENET-WP009.
4. Establish a system patching policy to keep software up to date. Reference material: Computer System Security Updates, Publication # SECUR-WP002.
5. Develop security policies to manage the "human factor", for example: managing and protecting passwords, managing removable media and use of personal devices.
6. Implement a level of physical control by putting the key-switch on your Logix Controller in Run Mode.
7. Control who is allowed to do what from where in the application with FactoryTalk® Security.
8. Monitor what is going on in your system with Controller Change Detection and FactoryTalk® AssetCentre.
9. Protect your intellectual property with Logix Source Protection.
10. Limit access with physical controls such as keyed connectors, Lock-in & Blockout products, Data Access Ports/locking cabinets.

Bill of Materials

Qty	Catalog #	Description
		System: Communication Hardware
1	1783-BMS10CL	Stratix 5700 Layer 2 Managed Switch, 10 Ports, Lite
1	1783-BMS10CGN	Stratix 5700 Layer 2 Managed Switch, 10 Ports, Full with CIP Synch, NAT, and DLR
1	1783-RMS10T	Stratix 8300 Layer 3 Managed Switch, 10 Ports
1	1783-SR	Stratix 5900 Security Appliance

Additional Resources

1783-TD001-EN-P	Stratix Ethernet Device Technical Data
ENET-WP031-EN-E	Design Considerations for Securing Industrial Automation
ENET-WP037-EN-E	Deploying Identity Services within a CPwE Architecture
ENET-WP038-EN-E	Securely Traversing IACS Data Across the IDMZ
ENET-WP025-EN-E	Scalable Secure Remote Access Solutions for OEMs
ENET-PP006-EN-E	Allen-Bradley Stratix 5900 Services Router
ENET-WP005-EN-E	Securing Manufacturing Computing and Controller Assets
ENET-WP006-EN-E	Production Softwarewith Manufacturing Reference Architectures
ENET-WP009-EN-E	Secure Remote Access to Plant Floor Applications
ENET-WP022-EN-E	Top 10 Recommendations for Plantwide EtherNet/IP
SECUR-WP002-EN-E	Patch Management and Computer System Security Updates
GMSC10-BR004-EN-P	Network and Security Services Brochure
ENET-TD001-EN-P	Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (DIG)

Reference Architecture Web Page
http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page

Industrial Security Web Page
http://rockwellautomation.com/security

About the Products

Stratix Managed Switches

Managed industrial ethernet switches embedded with Cisco technology.
- Access Control Lists
- Device Authentication with Learn Mode
- Programmable port control (on/off)
- Unauthorized device identification
- Encrypted administrative traffic

Stratix 5900™ Services Router

A services router that provides security features and managed switching features in an industrially hardened product.
- Secure routing and firewall capabilities
- Virtual Private Network (VPN)
- Intrusion protection capabilities
- Network Address Translation
- Access Control Lists (ACL)

ControlLogix® PAC

Programmable Automation Controller (PAC) use a common control engine with a common development environment to provide high performance in an easy-to-use environment.
- Trusted Slot Designation
- Change Detection and Logging
- Firmware Digital Signatures

CompactLogix® PAC

Programmable Automation Controller (PAC) that helps provide cost-effective integration of a machine or safety application into a plant-wide control system.
- Change Detection and Logging (Studio 5000 v20 and later)
- Firmware Digital Signatures

Studio 5000™

Logix Designer application lets you consolidate controller programming and drive system configuration, operation and maintenance into a single software environment.
- Logix Controller Source Protection
- Logix Controller Data Access Control
- Controller Change Detection and Logging
- High Integrity AOI's

FactoryTalk® AssetCentre

A set of asset-centric tools to securely manage your production environments.
- Tracks users' actions, manages asset-configuration files, and provides backup and recovery of operating asset configurations
- Monitor the Audit Value and read in the Controller Log

FactoryTalk® Security

A part of the FactoryTalk software suite that provides centralized role-based access-control.
- Data Access Control
- Provides user access controls and role-based security to Controllers, HMI and Software
- Allows the administrator to configure who can change all of the tags in the controller

Reference Architectures

Validated architecture guidelines for industrial applications jointly developed by Rockwell Automation and Cisco.
- Provides design considerations, guidance and best practices to help you design and deploy secure and future-ready EtherNet/IP network infrastructures
- Security framework utilizing defense-in-depth approach
- Guidance on remote access policies and approaches providing for a robust and secure solution

Network and Security Services

Field consulting services that help customers assess, design, implement, recommend and maintain ICS networks.
- Asset-based risk and vulnerability assessments
- Definition of security policies, procedures and guidelines
- Development of technical security controls