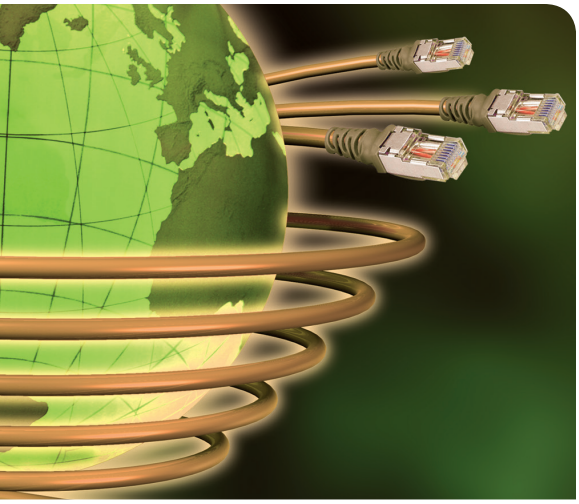


## Rockwell Automation and Cisco Four Key Initiatives:

- **Common Technology View:**
  A single system architecture, using open, industry standard networking technologies, such as Ethernet, is paramount for achieving the flexibility, visibility, and efficiency required in a competitive manufacturing environment.
- **Coverged Plantwide Ethernet Architectures:**
  These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture™ and Cisco's Industrial Intelligence, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.
- **Joint Product and Solution Collaboration:**
  Stratix 8000™ Industrial Ethernet switch incorporating the best of Cisco and the best of Rockwell Automation.
- **People and Process Optimization:**
  Education and services to facilitate Manufacturing and IT convergence and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.

# Design Considerations for Securing Industrial Automation and Control System Networks

## Synopsis

The continuing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically industrial automation technology with information technology (IT). EtherNet/IP helps enable network technology convergence through the use of standard Ethernet and Internet Protocol (IP) technology. EtherNet/IP, as a single industrial network technology, can facilitate (see Figure 1):

- Multi-discipline application convergence – e.g. discrete, continuous process, batch, drive, safety, motion, power, time synchronization, supervisory information, asset configuration/diagnostics and energy management
- Standard IT technology – future-ready, increased sustainability and reduced risk of deployment
- Better asset utilization through a common network infrastructure that can also support lean initiatives
- Common toolsets and required skills / training (e.g. assets for design, deployment and troubleshooting, as well as human assets)
- Standard and established IT security technology, best practices, policies and procedures
- Seamless plant-wide / site-wide information sharing due to IP pervasiveness - routability and portability across data links (e.g. Ethernet and Wi-Fi)

Although technology has been the enabler behind industrial automation and information technology convergence, the business aspects have sustained this continual trend:

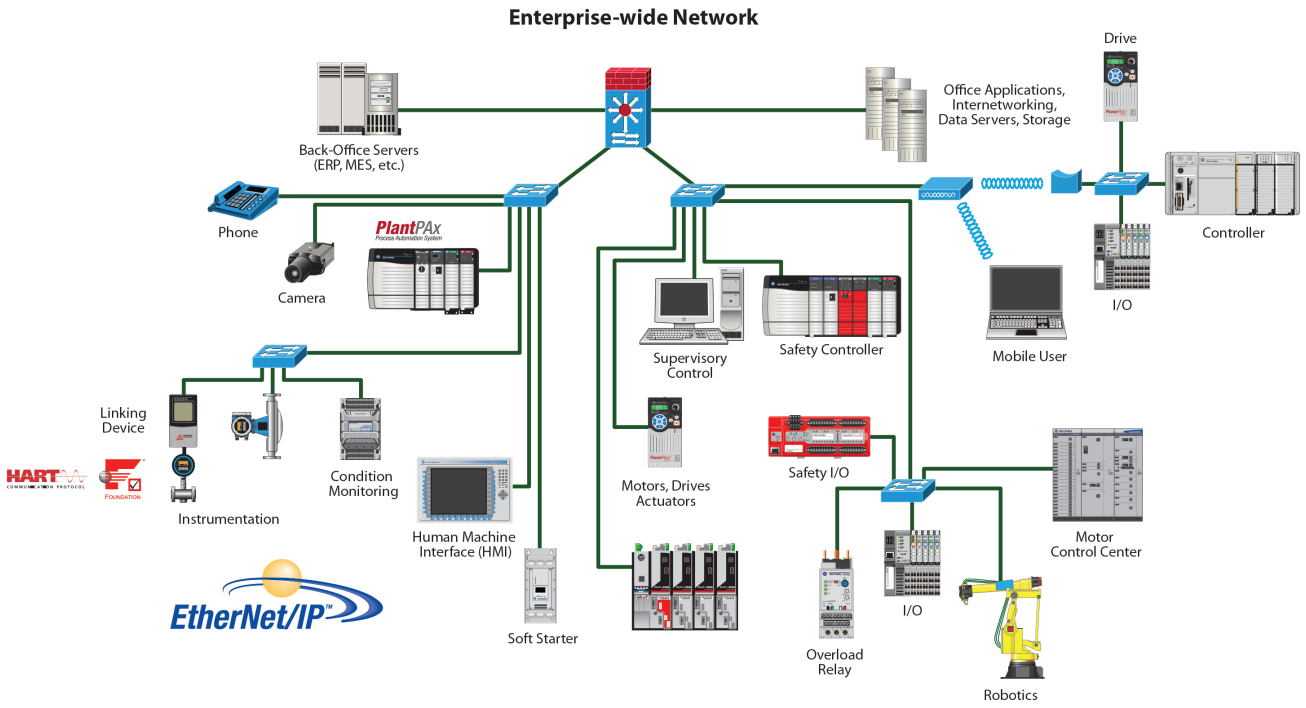
**Integration –** converging business systems with plant-wide / site-wide systems for more key performance indicators (KPIs), regulatory compliance (e.g. genealogy and track and trace), as well as supply chain management

**Connectivity –** more IACS devices connected for better IACS asset utilization, optimization and management

**Applications –** expanded application support (e.g. energy management and sustainability initiatives)

**Collaboration –** industrial automation and IT groups, who previously had little interaction, are now collaborating to share standards, best practices, innovations and security policies, procedures and technology

Figure 1: Converged Plant-wide/Site-wide Network Infrastructure




To help further facilitate and support network technology convergence, Rockwell Automation and Cisco have collaborated to develop Converged Plantwide Ethernet (CPwE) reference architectures (see references 1, 4, and 5). These CPwE reference architectures provide design considerations, guidance, recommendations, best practices and solutions. Together, Rockwell Automation and Cisco are able to help customers successfully design and deploy a scalable, robust, secure and future-ready plant-wide / site-wide network infrastructure utilizing standard networking and security technology. This collaboration also helps address the cultural and organizational convergence of the industrial automation and information technology domains. These IACS focused reference architectures are built on technology and industry standards common between industrial automation and information technology (IT). These include technology standards such as the IEEE 802.3/802.1 standard Ethernet, Internet Engineer Task Force (IETF), standard Internet Protocol (IP), and the ODVA Common Industrial Protocol (CIP™). For additional information about ODVA, see references 12, 13 and 14.

IACS networks are generally open by default to allow both technology coexistence and device interoperability. This requires that IACS networks be secured by configuration – i.e. protect the network and defend the edge. Securing an IACS network infrastructure requires a comprehensive industrial security model based on a well-defined set of security policies and procedures. Industrial security policies and procedures need to 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). These industrial security policies and procedures should leverage established IT processes to identify both security risks and potential mitigation techniques to address those risks.

This white paper outlines general considerations to help design and deploy a holistic defense-in-depth industrial security policy to help secure networked IACS assets. Three aspects of the CPwE Industrial Network Security Framework (see Figure 3) will be specifically expanded upon within this white paper. This content is relevant to both an industrial automation control system engineer and an information technology network engineer:

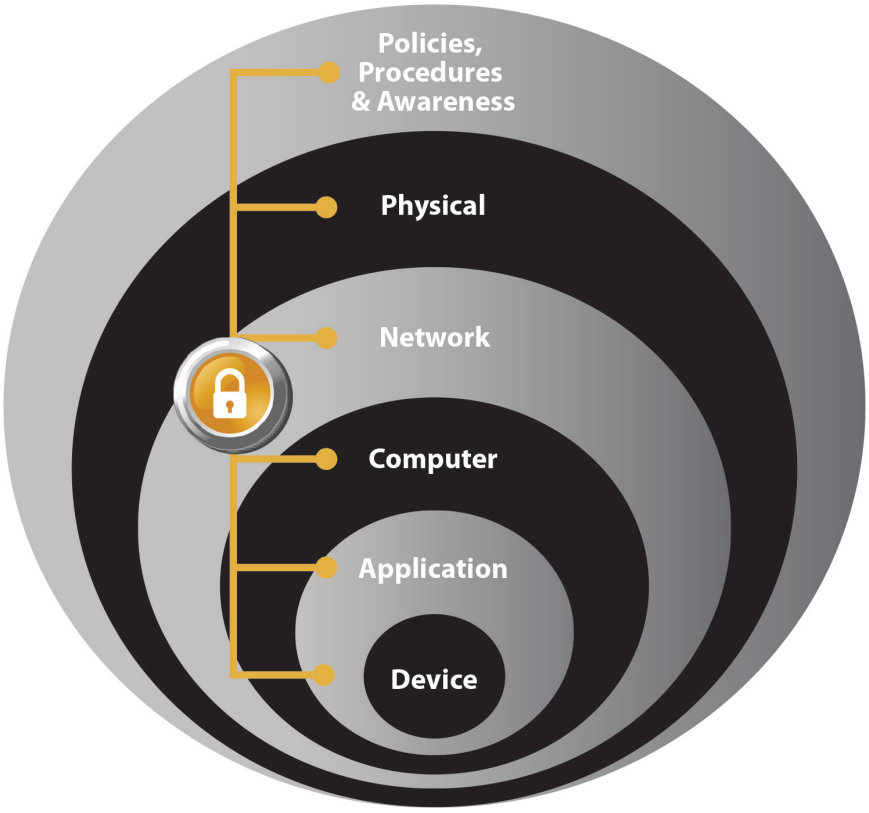
- Layer 2 Access Switch Hardening, see Figure 3
- Unified Threat Management (UTM), see Figure 4
- Controller Hardening – Encrypted Communications, see Figure 5

A listing of additional reference materials is available at the end of this white paper. Please note the reference list includes other resources not specifically called-out within this white paper.

## Holistic Industrial Security

No single product, technology or methodology can fully secure Industrial Automation and Control System (IACS) applications. Protecting IACS assets requires a defense-indepth security approach, Figure 2, 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. For example, multiple layers of network security to help protect networked assets (e.g. data and end points) and multiple layers of physical security to help protect high value assets.

Figure 2: Defense-in-Depth Security – Multiple Layers of Defense



To achieve a defense-in-depth approach, an operational process is required to establish and maintain the security capability. A security operational process includes the follow actions:

1. Identify IACS asset device types and locations within the plant-wide / site-wide network infrastructure
2. Identify potential internal and external vulnerabilities and threats to those IACS assets and assess the associated risks
3. Understand the application and functional requirements of the IACS assets (e.g. 24x7 operations, communication patterns, topology, required resiliency and traffic types)
4. Understand the associated risks of balancing the application and functional requirements of IACS assets with the need to protect the availability, integrity and confidentiality of IACS asset data

Designing and implementing a comprehensive IACS network security framework should serve as a natural extension to the IACS process. The industrial network security framework should be pervasive and core to the IACS process. Network security should not be implemented as a bolt-on component. A balanced security framework must address both technical (technology) and non-technical (policies and procedures) elements.

As depicted in Figure 2, defense-in-depth layers for securing IACS assets include, but are not limited to:

Policies, Procedures and Awareness – plan of action around procedures and education to protect company assets (risk management) and provide rules for controlling human interactions in IACS systems.

Physical Security – document and implement the operational and procedural controls to manage physical access to cells/areas, control panels, devices, cabling, the control room and other locations to authorized personnel only. This should also include policies, procedures and technology to escort and track visitors.

Network Security – industrial network security framework (see Figure 3) is made up of network infrastructure hardware and software designed to block communication paths and services that are not explicitly authorized. Assets may include firewalls, unified threat management (UTM) security appliances and integrated protection within network assets such as switches and routers.

Computer Hardening – patch management policy (see reference 10), Anti-X (e.g. virus, spyware, malware) detection software, uninstall unused windows components; protect unused or infrequently used USB, parallel or serial interfaces on any computer being connected to the IACS network.

Application Security – implement change management and accounting (e.g. FactoryTalk AssetCentre), as well as authentication and authorization (e.g. FactoryTalk Security) to help keep track of both access and changes by users.

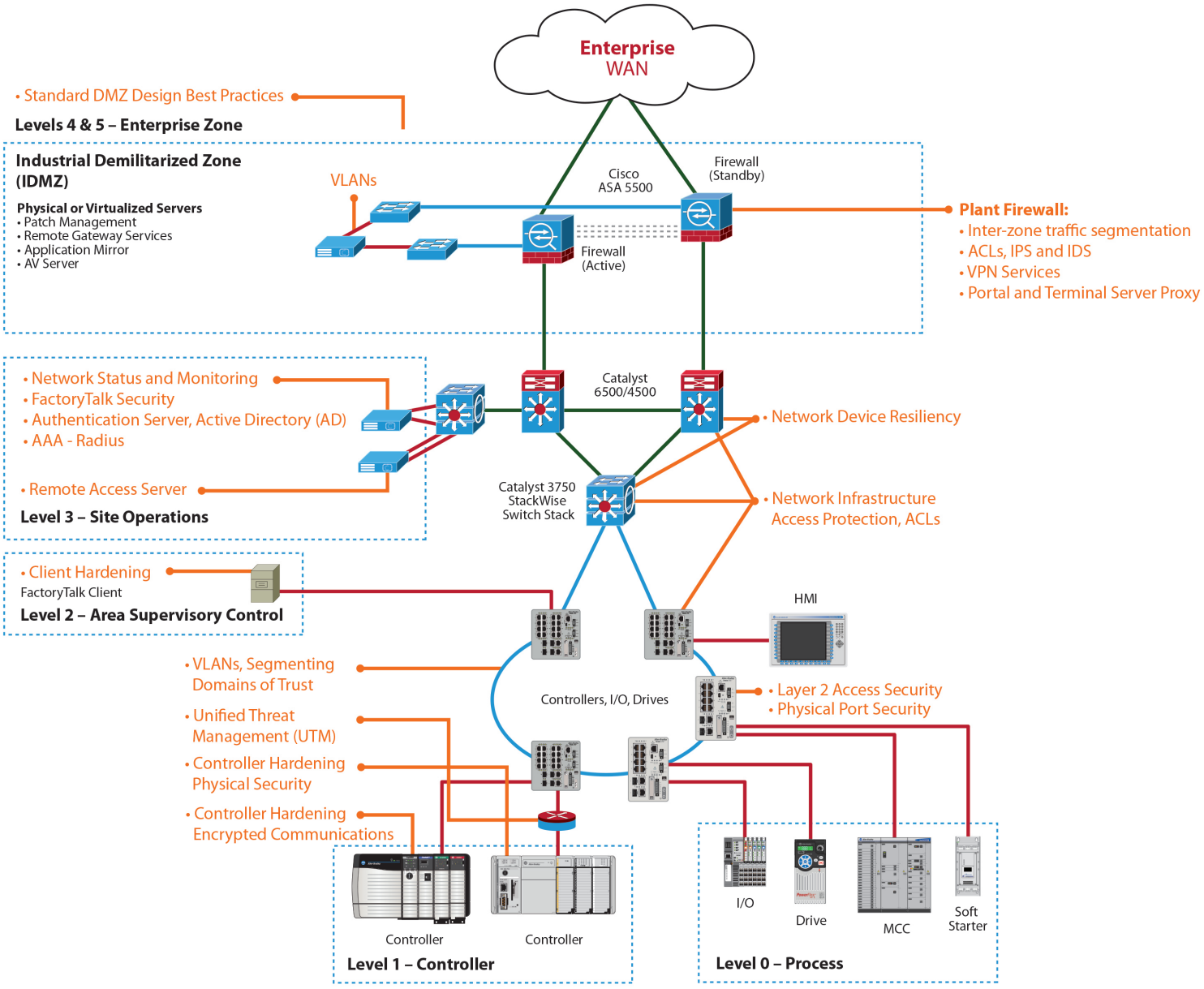
Device Hardening – restrict physical access to authorized personnel only, disable remote programming capabilities, encrypt communications (see Figure 5), restrict network connectivity through authentication (see Figure 5), restrict access to internal resources (e.g. routines and tags) through authentication and authorization.

For additional information on defense-in-depth security, see references 4, 5, 6, 7 and 9.

# Industrial Network Security Framework

Converged Plantwide Ethernet (CPwE) reference architectures use industry standards to establish an industrial network security framework as shown in Figure 3. This industrial network security framework establishes a foundation for network segmentation for both traffic management and policy enforcement (e.g. security, remote access, and Quality of Service (QoS)). The industrial network security framework utilizes a defense-in-depth approach and is aligned to industrial security standards such as ISA/IEC-62443 (formerly ISA-99) Industrial Automation and Control Systems (IACS) Security and NIST800-82 Industrial Control System (ICS) Security.

Figure 3: CPwE Industrial Network Security Framework



The key tenets of industrial network security framework utilizing defense-in-depth includes:

**Industrial Security Policy –** The key to a successful industrial security strategy is risk assessment and analysis to understand the potential vulnerabilities that need to be mitigated, specifically what to protect and how. Establishing an industrial security policy focused on the needs of an IACS provides a roadmap for applying security technologies and best practices to protect IACS assets, while avoiding unnecessary expenses and excessive restrictive access. The industrial network security framework should be pervasive and core to the IACS process. Industrial network security services should not inhibit nor compromise the IACS operation

Risk and security assessments are the starting point for any security policy implementation. Security assessments analyze your current state, from technologies to policies, procedures to behavior. This analysis offers a realistic picture of your security posture (current risk state) and what it will take (mitigation techniques) to get to where you need to be (acceptable risk state). A multi-discipline team of operations, engineering, IT and safety representatives should collaborate in the development and deployment of this industrial security policy based on your risk assessment.

**Industrial Demilitarized Zone (IDMZ) –** Sometimes referred to as a perimeter network that exposes a trusted network to an untrusted network, the purpose of the IDMZ is to add an additional buffer layer of security. This buffer zone provides a barrier between the Industrial and Enterprise Zones, but allows for data and services to be shared securely.

- All network traffic from either side of the IDMZ terminates in the IDMZ; no traffic directly traverses the IDMZ
  - · Only path between Industrial and Enterprise Zones
  - · No common protocols in each logical firewall
- EtherNet/IP IACS traffic does not enter the IDMZ, it remains in the Industrial Zone
- Primary services are not permanently stored in the IDMZ
- All data is transient, the IDMZ shall not permanently store data
- Utilize an application data mirror to move data in and out of the Industrial Zone
- Limit outbound connections from the IDMZ
- Be prepared to “turn-off” access to the Industrial Zone via the firewall
- Set-up functional sub-zones within the IDMZ to segment access to data and services (e.g. IT, Operations, Trusted Partner zone)
- IDMZ is also a demarcation line for segmenting network policies between the Enterprise and Industrial Zones. Segmenting network services such as Quality of Service (QoS), Virtual LANS (VLANs), and Multicast traffic. These services exist in both the Enterprise and Industrial Zones and should be segmented.

Controller Hardening –

- Restrict logical access through authentication and authorization (see Figure 5), encrypt communications (see Figure 5), and use change management to track both access and changes
- Restrict physical access to IACS assets. Utilize cable lock-in and port blockout devices (such as Panduit's) to prevent "walk up, plug in" access

Layer 2 Access Switch Hardening –

- Restrict logical access by enabling cryptographic version of switch operating system (OS) (e.g. SSH, HTTPS, SNMPv3 and implement port MAC security)
- Restrict physical access. Utilize cable lock-in and port blockout devices (i.e. Panduit's) to prevent "walk up, plug in" access

Firewalls – Modern firewalls (i.e. unified threat management (UTM)) provide a range of security services: deploy a UTM security appliance with stateful packet inspection (SPI) firewall (barrier), application awareness and intrusion detection/prevention systems (IDS/IPS) around and within the industrial network infrastructure (see Figure 4).

Network Infrastructure Access Protection – Implement access control lists (ACLs) and port security on network infrastructure devices such as switches and routers. Implement network infrastructure resiliency with redundant path topologies to ensure the availability of IACS data.

Domains of Trust – Segment the network into smaller areas based on functions or access requirements.

Secure Remote Access Policy – Implement policies, procedures and infrastructure to enable employee and trusted partner secure remote access. For additional information on secure remote access, see references 8 and 9.

Three aspects of the CPwE Industrial Network Security Framework (see Figure 3) will be specifically expanded upon within this white paper. This content is relevant to both an industrial automation control system engineer and an information technology network engineer:

- Layer 2 Access Switch Hardening, see Figure 3
- Unified Threat Management (UTM), see Figure 4
- Controller Hardening – Encrypted Communications, see Figure 5

# Layer 2 Access Switch Hardening

Layer 2 access switches, such as the Stratix 5700 and Stratix 8000, can be hardened to restrict access by several techniques as shown in Figure 3:

1. Physically:
   a. Restrict access to the control panel or zone enclosure to authorized personnel only
   b. Utilize Panduit's block outs for the open access ports and lock-ins for the copper and fiber media

2. Electronically:
    a. Layer 2 media access control address (MAC) security on access ports
    b. Layer 3 access control lists (ACLs)
    c. Virtual local area networks (VLANs) to segment the Cell/Area Zone into smaller domains of trust
    d. Disabling access ports from the programmable automation controller (PAC) and operator interface utilizing CIP communications (application layer protocol for EtherNet/IP)
    e. Traffic threshold settings to monitor (via CIP communication) any potential denial of service (DOS) attacks
    f. Enabling cryptographic version of switch operating system (OS) (e.g. SSH, HTTPS, SNMPv3)

# Unified Threat Management

Modern firewalls provide a range of security services. These unified threat management (UTM) devices combine several security functions into a single appliance to protect your IACS network at the perimeter. The Stratix 5900 UTM security appliance is a ruggedized all-inclusive UTM with features such as firewall, secure routing, virtual private network (VPN), intrusion prevention, network address translation (NAT) and content filtering.

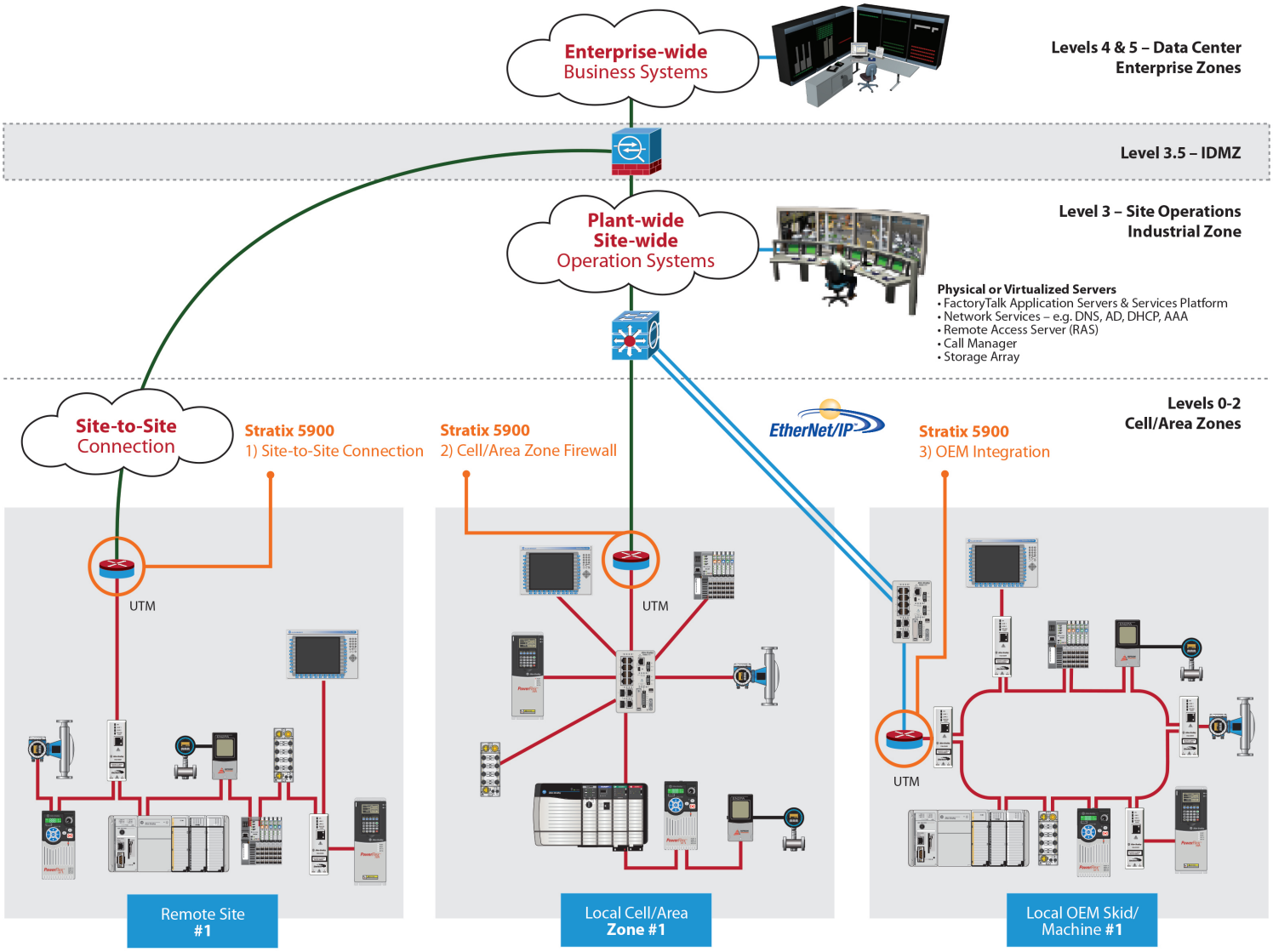
There are 3 use cases (see Figure 4) specifically addressed within this white paper for UTM within the CPwE Industrial Network Security Framework (see Figure 3):

1. 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
2. Cell/Area Zone Firewall – to protects Cell/Area Zone from the greater Industrial Zone
3. OEM Integration – provides seamless integration from a machine builder or process skid builder solution into their customer's plant-wide / site-wide network infrastructure. For additional information about OEM integration solutions, see reference 11

### 1. Stratix 5900 Site-to-Site Connection Capabilities

- A traditional virtual private network (VPN) is a secured connection between two devices over an "untrusted" (unsecured) network. Choice of VPN technology varies between each implementation and vendor; generally, the data to be transmitted over the untrusted network is either encrypted or encapsulated to protect the integrity of the data and to prevent any form of eavesdropping.
- Site-to-site VPN to help create a connection between remote IACS applications back to the central site (Industrial Zone) over an untrusted network (private, semi-private, or a public). Site-to-site VPNs use well established technologies that are widely deployed in enterprise networks and IT domains.
- Since EtherNet/IP is built on standard IP, the site-to-site network can use any Layer 2 technology that supports IP. The Stratix 5900 has both Ethernet and Smart Serial wide area network (WAN) ports which help allow connectivity to a variety of WAN network technologies (e.g. Ethernet, Wi-Fi, 3/4G cellular, MPLS or other traditional technologies such as xDSL or T1/E1).

Figure 4: Stratix 5900, UTM Security Appliance, within CPwE




- Site-to-site VPN is a permanent, "always on" technology. This allows for continual monitoring of the remote IACS application. Because the networking technology is standard, the IACS VPN connection can also be leveraged for other critical applications such as IP surveillance cameras or physical security systems for remote sites.
- Stratix 5900 Site-to-Site Connection Design Considerations
  - Installation of an untrusted network (private, semi-private, or a public) to all distributed remote sites is not required
  - Firewalls terminate the VPN tunnels and filter traffic on both sides of the connection
  - Not an ad hoc, temporary, dial on-demand solution

2. Stratix 5900 Cell/Area Zone Firewall Capabilities

- As a Cell/Area Zone firewall, the Stratix 5900 can filter traffic between the Cell/Area Zone and the rest of the Industrial Zone
- Stratix 5900 Cell/Area Zone Firewall Design Considerations
  - Restricts network communication paths and services to and from the Cell/Area Zone
  - Zone based firewall that supports traffic filtering, stateful inspection, and IPS/IDS. It can be used as either a routed or a transparent firewall
  - Supports Authentication, Authorization and Accounting (AAA) network security server (Tacacs+ or Radius)
  - Supports network address translation (NAT), to allow network address transparency from the Cell/Area Zone IACS network to the plant-wide / site-wide network, thus minimizing the quantity of IP addressing to be assigned and managed within the Industrial Zone

3. Stratix 5900 OEM Integration Capabilities

OEM (machine builder or process skid builder) simplified design and deployment

- Network address translation (NAT) – project reuse (IP addressing), enabling network address transparency from OEM solutions within the Cell/Area Zone IACS network to the plant-wide / site-wide network, thus minimizing the quantity of IP addressing to be assigned and managed within the Industrial Zone.
- Strong OEM solution segmentation through Layer 3 routing and firewall. For example, an OEM may include a Stratix 5900 as part of their solution to tightly control traffic in and out of the OEM machine/skid. Conversely, an end user might deploy a Stratix 5900 between their plant-wide / site-wide network and the OEM machine/skid to tightly control traffic in and out of that OEM machine/skid into the greater Industrial Zone.

Stratix 5900 OEM Integration Design Considerations

- Restricts traffic to and from an OEM solution
  - Basic stateful inspection of all traffic
  - Intrusion Prevention System / Intrusion Detection System (IPS/IDS) on some traffic
  - Supports both routed and transparent firewalls
  - Supports Authentication, Authorization and Accounting (AAS) network security server (Tacacs+ or Radius)

Stratix 5900 Physical Features

- 1 - 1 Gbps WAN port
- Smart Serial WAN port
- 4 - 100 Mbps LAN ports
- Shock / Vibration & Extended Temperature
- DIN rail mount

Stratix 5900 Network Features

- Access Control Lists (ACLs) / Firewall
- DHCP
- Quality of Service (QoS)
- Virtual Local Area Network (VLAN)
- Network Address Translation (NAT)

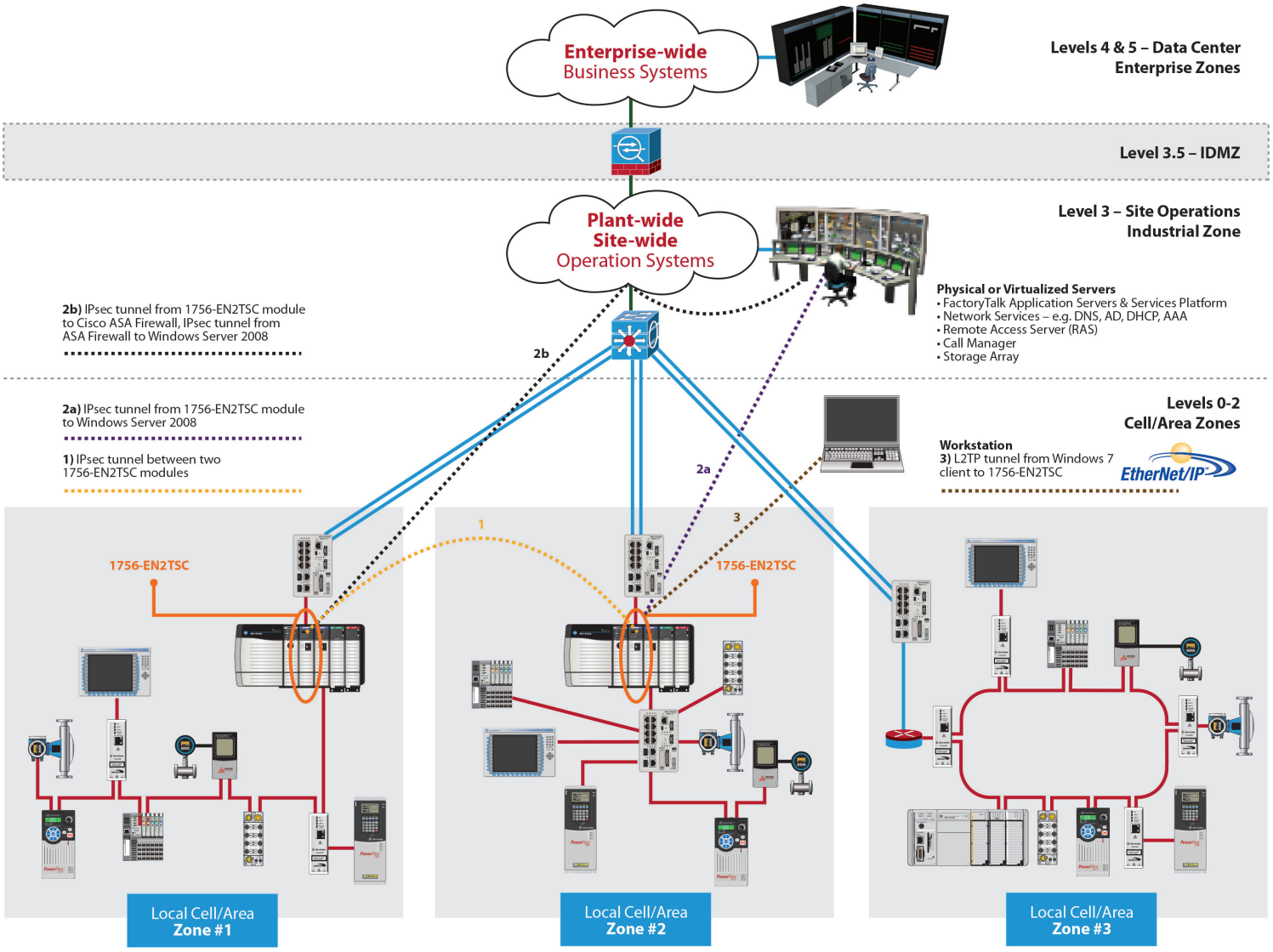
# Controller Hardening – Encrypted Communications

Within the Converged Plantwide Ethernet (CPwE) Industrial Network Security Framework (Figure 3), securing controller communications over a "trusted" network is about applying additional access control (authentication) and protecting the integrity (encryption) of the data. An example would be protecting the integrity and confidentiality of a batch profile or recipe that is being communicated from the Level 3 site operations to a controller in the Cell/Area Zone. The ControlLogix (PAC) 1756-EN2TSC secure communication module utilizes either IP security (IPsec) or Layer 2 Tunneling Protocol (L2TP) to provide authentication and data encryption over a trusted CPwE network.

There are four use cases (see Figure 5) specifically addressed within this white paper to harden controller communications within the trusted CPwE Industrial Network Security Framework (see Figure 3):

1. ControlLogix to ControlLogix – permanent connection for peer to peer ControlLogix communications, IPsec-encrypted tunnel between the two 1756-EN2TSC modules
2. ControlLogix to FactoryTalk Application – permanent connection between ControlLogix and FactoryTalk application/data server
    a. Smaller applications, IPsec-encrypted tunnel from 1756-EN2TSC module to Windows Server 2008
    b. Larger applications, IPsec-encrypted tunnel from 1756-EN2TSC module to Cisco ASA firewall, and then IPsec-encrypted tunnel from ASA firewall to Windows Server 2008. This approach provides scalability through centralized management of security policies within the Cisco ASA firewall to simplify deployment and manageability on larger IACS applications
3. Workstation to ControlLogix – ad hoc temporary connection for ControlLogix configuration and management, L2TP-encrypted tunnel from Windows 7 client to 1756-EN2TSC module

Figure 5: 1756-EN2TSC – Secure Controller Communication – within CPwE




1756-EN2TSC Secure Communication Module Capabilities:

- Authenticates the communication end points (both client and server)
- Data authentication and integrity (via message integrity checks)
- Data confidentiality (via encryption algorithms)
- Support for up to 8 secure tunnels per module
- Advanced Encryption Standard (AES) 256 (NIST standard for the encryption of data)
- Optional disablement of onboard USB port and configuration dip switches to prevent physical tampering

- Secure HTTPS interface for configuration and monitoring of security related features
- Data Encryption Design Considerations:
  - Can be used in conjunction with other controller and device hardening features for additional granularity to access rules
  - Uses separate communication bridge module(s) for connectivity to networked IACS devices (e.g. I/O, drives, instrumentation)
  - The 1756-EN2TSC does not currently support communication through NAT devices
  - Uses standard Microsoft Windows 7 VPN Client to connect transient, ad hoc devices, like engineering workstations, to the controller
  - Embedded standard VPN clients are also used to connect to permanent devices like other controllers and Windows Server 2008
- This module is intended for use within the trusted CPwE industrial network security framework (Figure 3). This module in not intended for use on an untrusted (private, semi-private, or a public) network.

# Summary

No single product, technology or methodology can fully secure Industrial Automation and Control System (IACS) applications. Securing an IACS network infrastructure requires a defense-in-depth industrial network security framework to address both internal and external security threats. A balanced industrial network security framework must address both technical (electronic technology) and non-technical (e.g. physical, policy, procedural) elements. This industrial network security framework should be based on a well-defined set of security policies and procedures, leveraging established IT processes, while balancing the functional requirements of the IACS application itself.

Risk and security assessments are the starting point for any security policy implementation. Security assessments should look at your specific situation from technologies to policies, procedures to behavior, and give you a realistic picture of your current security posture (current risk state) and what it will take (mitigation techniques) to get to where you need to be (acceptable risk state). Rockwell Automation and Cisco recommend the formation of a multi-discipline team of operations, engineering, IT and safety representatives to collaborate in the development and deployment of your industrial security policy based on your risk assessment.

Rockwell Automation and Cisco have also collaborated to develop Converged Plantwide Ethernet (CPwE) reference architectures to help you address this industrial network security framework. This comes in the form of design considerations, guidance, recommendations, best practices, solutions and services to help you successfully design and deploy a scalable, robust, secure and future-ready plant-wide / site-wide network infrastructure. The CPwE Industrial Network Security Framework is aligned to industrial security standards such as ISA/IEC-62443 (formerly ISA-99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security in regards to a defense-in-depth security approach.

## Additional Reference Material

1. Rockwell Automation References Architectures Website
2. Rockwell Automation EtherNet/IP Website
3. Rockwell Automation Network and Security Services Website
4. Reference Architectures for Manufacturing White paper
5. Converged Plant-wide Ethernet Reference Architectures Design and Implementation Guide (DIG)
6. Top 10 Recommendations for Plantwide EtherNet/IP Deployments White paper
7. Securing Manufacturing Computing and Controller Assets White paper
8. Scalable Secure Remote Access - Solutions for OEMs White paper
9. Achieving Secure, Remote Access to Plant-Floor Applications and Data White paper
10. Patch Management and Computer System Security Updates White paper
11. Segmentation Techniques within the CPwE Cell/ Area Zone White paper
12. ODVA Website
13. Network Infrastructure for EtherNet/IP: Introduction and Considerations – ODVA
14. Securing EtherNet/IP Networks Guide

To learn more about how Cisco and Rockwell Automation can help you, please visit:

www.rockwellautomation.com/partners/cisco.html
http://www.cisco.com/web/strategy/manufacturing/cisco-rockwell_automation.html

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

**www.cisco.com**

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Rockwell Automation is a leading provider of power, control and information solutions that enable customers to get products to market faster, reduce their total cost of ownership, better utilize plant assets, and minimize risks in their manufacturing environments.

**www.rockwellautomation.com**

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000, Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788, Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600, Fax: (32) 2 663 0640



Publication ENET-WP031A-EN-E — June 2013