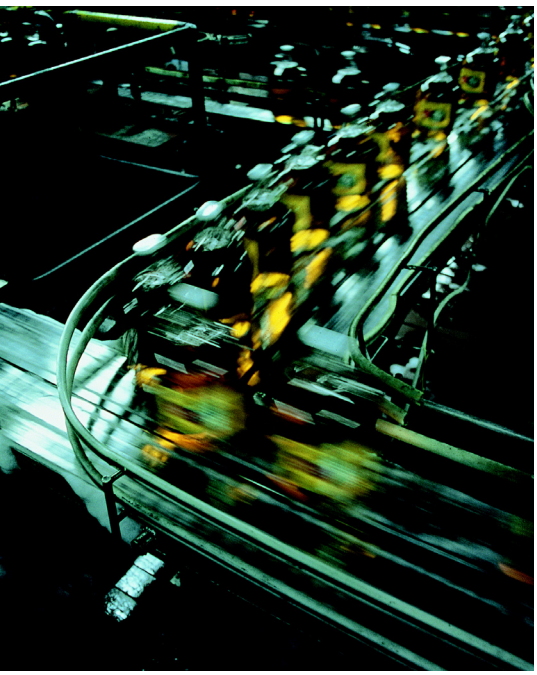


CIP Security within a Converged Plantwide Ethernet Architecture

White Paper

May 2020

Rockwell Automation and Cisco Four Key Initiatives:

- Common Technology View:
  A single scalable architecture, using open EtherNet/IP™ standard networking technologies, is paramount to enable the Industrial Internet of Things for achieving the flexibility, visibility, and efficiency required in a competitive manufacturing environment.
- Converged Plantwide Ethernet Architectures:
  Collection of tested and validated architectures developed by subject matter authorities at Cisco, Panduit, and Rockwell Automation. The content of CPwE is relevant to both Operational Technology (OT) and Information Technology (IT) disciplines and consists of documented architectures, best practices, guidance, and configuration settings to help manufacturers with design and deployment of a scalable, reliable, safe, secure, and future-ready plant-wide industrial network infrastructure.
- Joint Product Collaboration:
  Stratix® 5950 industrial firewall, FactoryTalk® Network Manager™ software, Stratix 5700, Stratix 5400, Stratix 5410, and Stratix 5800 Industrial Ethernet Switches, incorporating the best of Cisco and the best of Rockwell Automation.
- People and Process Optimization:
  Education and services to facilitate Operational Technology (OT) and Information Technology (IT) convergence, which can assist with successful architecture deployment, and helps to enable efficient operations that allow critical resources to focus on increasing innovation and productivity.

Document Reference Number: ENET-WP043B-EN-P

CIP Security within a Converged Plantwide Ethernet Architecture

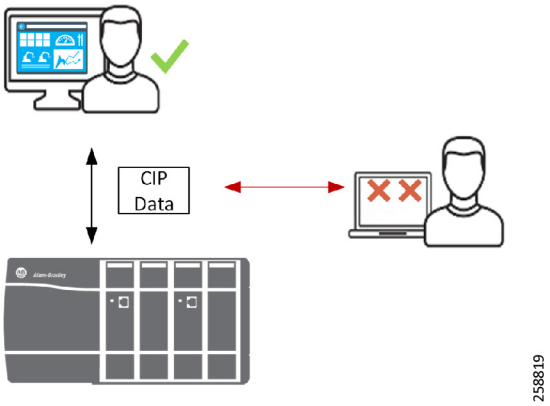
The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).

IIoT helps offer the promise of business benefits by using innovative technology such as mobility, collaboration, analytics and cloud-based services. The challenge for industrial operations is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

While reaping the benefits of OT-IT convergence, IACS applications within the CPwE architecture face continuous threats such as malware propagation, data exfiltration, network scanning, and so on. Furthermore, many IACS communication protocols are deficient of security properties such as authentication, integrity, and confidentiality putting IACS devices and their data at risk. Unprotected communication protocols could potentially be exploited to cause disruptive events that negatively impact the operation or availability of IACS equipment. Some examples include:

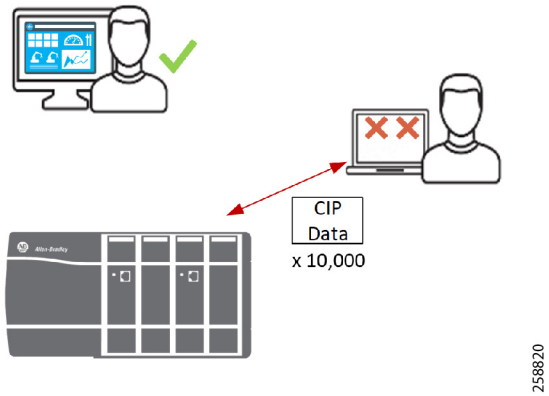
- A **reconnaissance attack** (Figure 1) is a multi-stage process, which includes an unauthorized entity eavesdropping on data in transit between IACS devices. This typically results in the unauthorized entity learning more about the activities and vulnerabilities of the operation leading to loss of confidentiality. Though this type of attack may not have an immediate impact on industrial operations, it can lead to more serious events such as capturing credentials or obtaining intellectual property.

Figure 1 Reconnaissance Attack



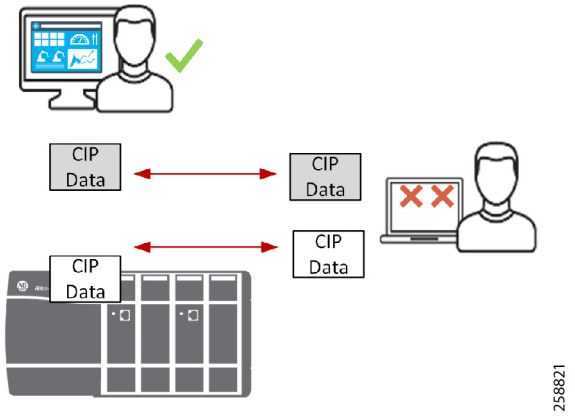
- A **denial-of-service (DoS) attack** (Figure 2) is a process where an unauthorized entity sends large amounts of arbitrary packets to overwhelm the IACS device (CPU and resources) thus rendering the device inoperable resulting in loss of availability.

Figure 2 Denial-of-Service (DoS) Attack



- A **man-in-the-middle (MITM) attack** (Figure 3) is a process where an unauthorized entity intercepts and changes the data to issue unauthorized commands or alter alarm thresholds, thus damaging or shutting down equipment and operations resulting in loss of integrity.

Figure 3 Man-in-the-Middle (MITM) Attack



With all the opportunities and challenges faced by industrial operations, there is a strong need for the following requirements:

- **Authentication**—Authentication is any process by which a system verifies the identity of an individual/system who wishes to access it. The two common methods to use:
  - Pre-Shared key (secret)—An agreement in advance of a shared secret password that only the two communicating entities have.
  - Digital Certificates—A certificate authority issues a digital certificate to assure that the two communicating entities are who they say they are.
- **Confidentiality**—Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. This also implies that unauthorized individuals should not have any type of access to the data. Confidentiality on data is achieved by using encryption.
- **Integrity**—Data Integrity confirms that only authorized parties can modify data. Integrity for data means that changes made to data are done only by authorized individuals and systems. Integrity on data is achieved by using digital signature or Hash-based Message Authentication Code (HMAC).

The ODVA, Inc. Common Industrial Protocol (CIP™) standard is an open application layer protocol for EtherNet/IP networks. CIP defines a standard grouping of objects as object models and as device profiles, which helps aid IACS devices to behave identically from device to device. This contributes to a reliable IACS device performing all its operations and functions as intended. Designing an IACS device with security built-in not only reinforces reliability but also confirms only authorized entities interact with that device.

CIP Security™ is the secure extension of CIP with the well-known standard transport layer security (TLS). The concept is like hypertext transfer protocol (HTTP) over TLS, also known as HTTPS. It uses proven standard technology to minimize potential vulnerabilities that may impact IACS applications. By leveraging open security IETF-standard TLS (RFC 5246) and DTLS (RFC 6347) protocols to help secure EtherNet/IP traffic, CIP Security provides the following properties:

- **Device identity and authentication**—Aids EtherNet/IP IACS devices in building trust by allowing each to provide identity through certificate exchange or pre-shared keys.
- **Data integrity and authentication**—Helps confirm the data has not been tampered with or falsified while in transit with TLS HMAC.
- **Data confidentiality (encryption)**—Increases the overall device security posture; message encryption can be enabled to avert unwanted data reading and disclosure.

Note IACS devices currently supporting CIP Security are still able to interoperate with IACS devices that do not support it on the same network. For example, Allen-Bradley® ControlLogix® 5580 (1756-L8xE) version 32 or higher with CIP Security enabled will still be able to communicate with a non-CIP Security IACS device such as Compact 5000™ I/O EtherNet/IP Adapter (5069-AEN2TR) with minimal to no additional configuration required.

An additional feature within Rockwell Automation IACS devices currently supporting CIP Security will allow disabling HTTP (webpage) on IACS devices for additional IACS device hardening.

Deploying CIP Security within a Converged Plantwide Ethernet Architecture (CPwE CIP Security) Design Guide outlines several security architecture use cases for designing and deploying CIP Security technology across plant-wide or site-wide IACS applications. CPwE CIP Security was architected, tested and validated by Rockwell Automation with assistance by Cisco Systems and Panduit.

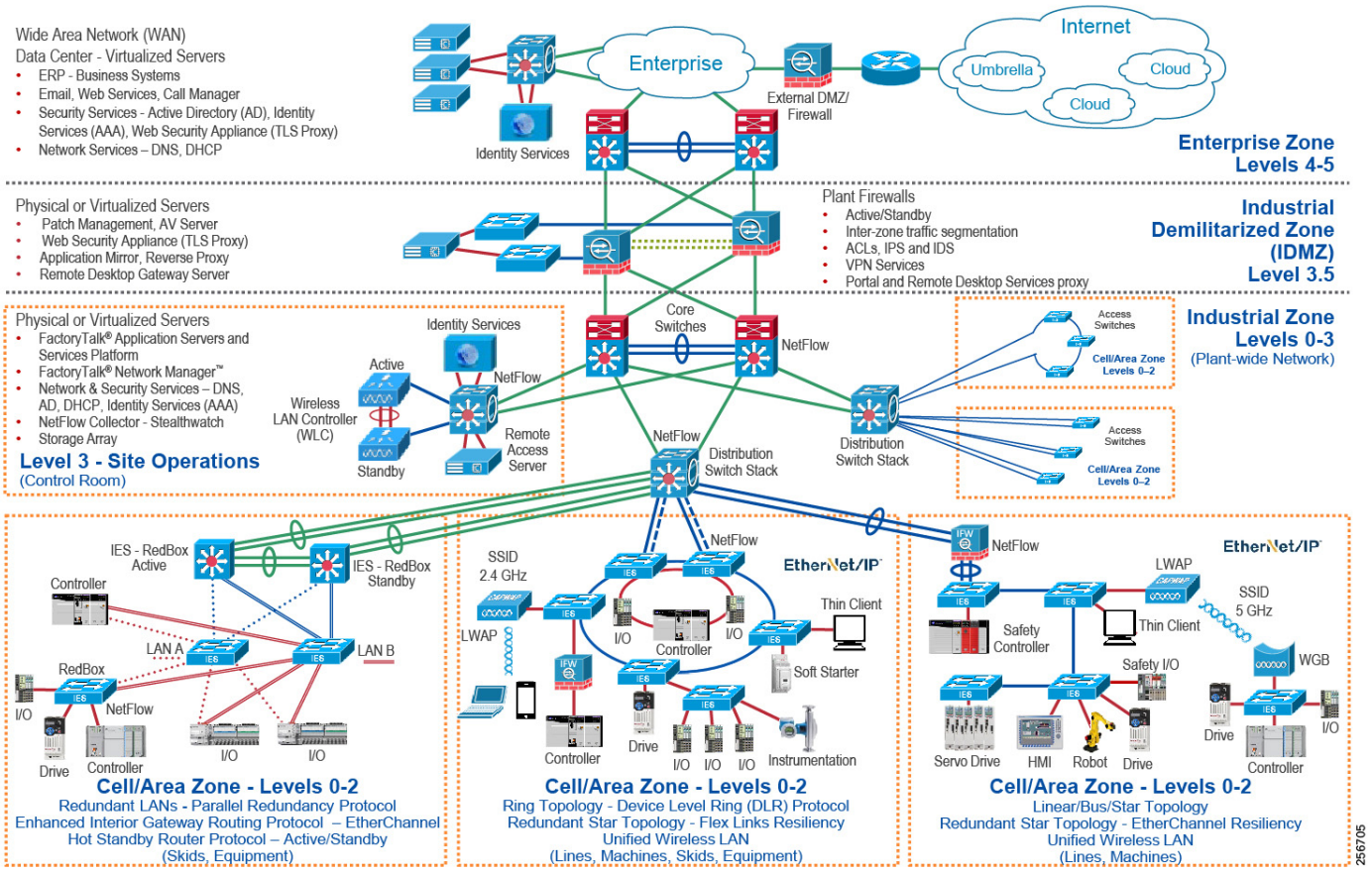
CPwE Overview

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architectures (Figure 4) were architected, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines.

CPwE key tenets include:

- **Smart IIoT devices**—Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP), facilitating both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS devices
- **Zoning (segmentation)**—Smaller connected LANs, functional areas, and security groups
- **Managed infrastructure**—Managed Allen-Bradley Stratix industrial Ethernet switches (IES), Cisco Catalyst® distribution/core switches, FactoryTalk Network Manager software, and Stratix industrial firewalls
- **Resiliency**—Robust physical layer and resilient or redundant topologies with resiliency protocols
- **Time-critical data**—Data prioritization and time synchronization via CIP Sync™ and IEEE-1588 Precision Time Protocol (PTP)
- **Wireless**—Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- **Holistic defense-in-depth security**—Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (for example, OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture
- **Convergence-ready**—Seamless plant-wide or site-wide integration by trusted partner application

Figure 4 CPwE Architectures



Note This release of the CPwE architecture focuses on EtherNet/IP, which uses the ODVA, Inc. Common Industrial Protocol (CIP) and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP, CIP, CIP Safety™, CIP Security, or CIP Sync, see the following URL: http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

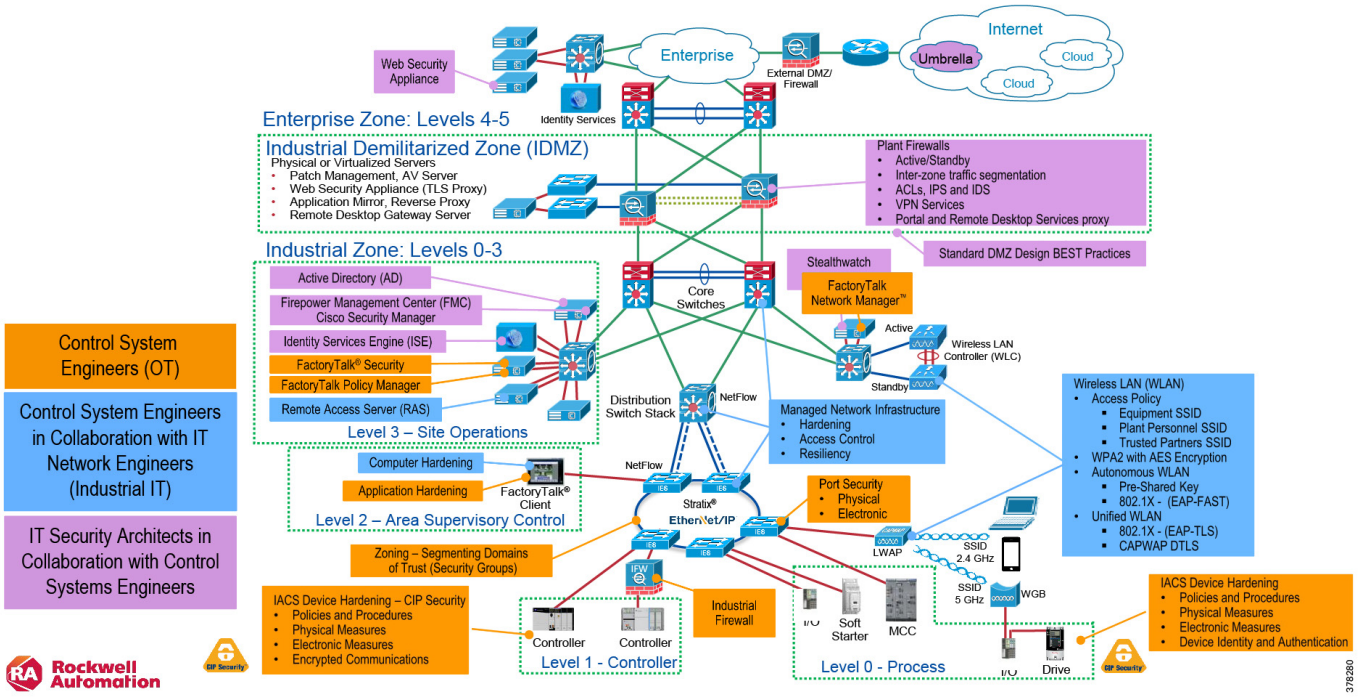
CPwE Industrial Security Framework Overview

No single product, technology, or methodology can fully secure plant-wide architectures. Protecting IACS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical) utilizing diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture (Figure 5).

- **Control System Engineers** (highlighted in tan)—IACS asset hardening (for example, physical and electronic), IACS application hardening (for example, CIP Security with FactoryTalk Policy Manager), infrastructure device hardening (for example, port security), network monitoring and change management (for example, FactoryTalk Network Manager), network segmentation (trust zoning), industrial firewalls (with deep packet inspection) at the IACS application edge, and IACS application authentication, authorization, and accounting (AAA).

- **Control System Engineers in collaboration with IT Network Engineers** (highlighted in blue)—Computer hardening (OS patching, application white listing), network device hardening (for example, access control, and resiliency), network monitoring and inspection, and wired and wireless LAN access policies.
- **IT Security Architects in collaboration with Control Systems Engineers** (highlighted in purple)—Identity and Mobility Services (wired and wireless), network monitoring with anomaly detection, Active Directory (AD), Remote Access Servers, plant/site firewalls, Industrial Demilitarized Zone (IDMZ) design best practices, data brokers (for example, Web Security Appliance), and OpenDNS (for example, Umbrella).

Figure 5 CPwE Industrial Security Framework



The CPwE Industrial Security Framework (Figure 5), using a defense-in-depth approach, is aligned to industrial security standards such as ISA/IEC 62443 Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

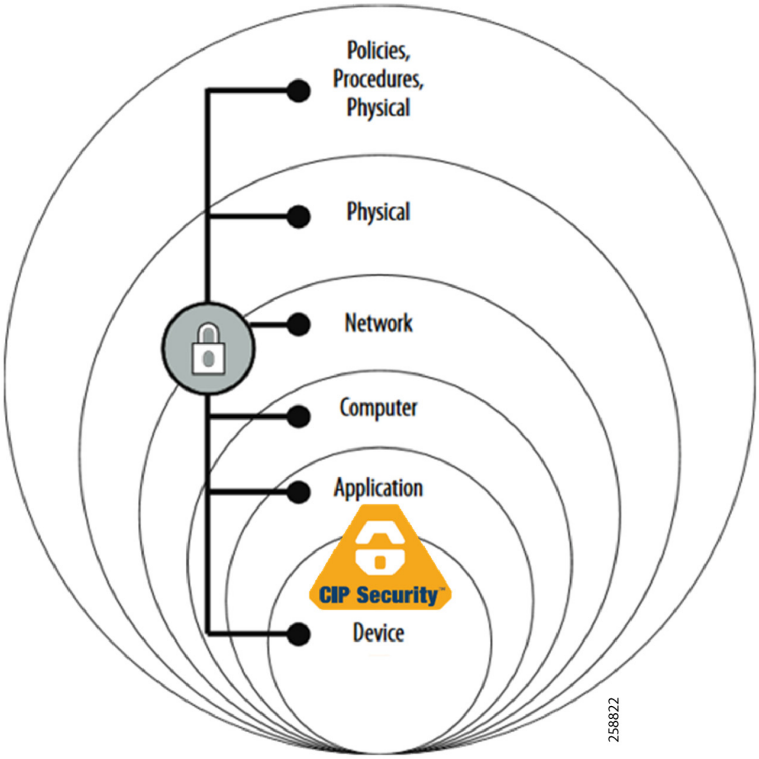
Defense-in-depth applies policies and procedures that address many different types of threats. Enforced at the IACS device and application level in the defense-in-depth security architecture (Figure 6), CIP Security enables CIP-connected IACS devices to authenticate each other before transmitting and receiving data. Device connectivity is then limited to only trusted devices. Optionally, to increase the overall IACS device security posture, it can be combined with data integrity and message encryption to guard against packet tampering and to avert unwanted data reading and disclosure.

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

1. Identify IACS asset device types and locations within the plant-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 including 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 help protect the availability, integrity, and confidentiality of IACS asset data.

Figure 6 Defense-in-Depth Security



In a defense-in-depth security approach (Figure 6), different solutions are needed to address various network and security requirements for a plant-wide or site-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of industrial security.

- *Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several industrial security architecture use cases, with Cisco ISE, for designing with visibility, segmentation, and anomaly detection throughout a plant-wide IACS network infrastructure.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several industrial security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk® applications, throughout a plant-wide or site-wide IACS network infrastructure.

  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html

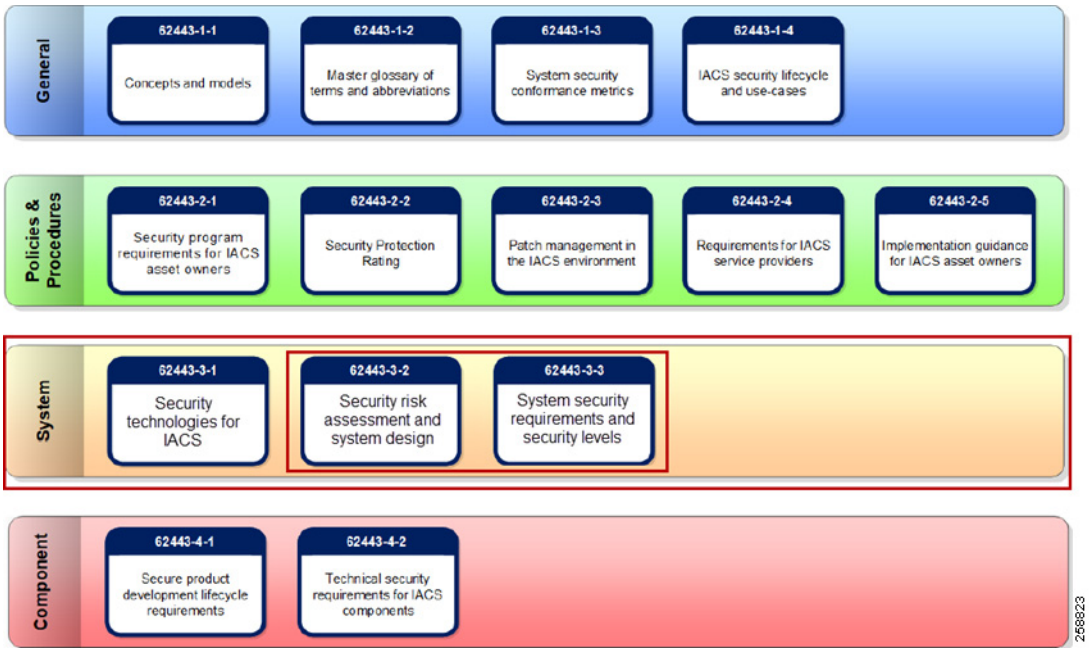
- *Cloud Connectivity to a Converged Plantwide Ethernet Architecture Design Guide* outlines several industrial security architecture use cases for designing and deploying restricted end-to-end outbound connectivity from FactoryTalk applications to the Rockwell Automation cloud within a CPwE architecture.
  - Rockwell Automation site: https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html
- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing, deploying, and managing industrial firewalls throughout a plant-wide IACS network. The Industrial Firewall is ideal for IACS applications that need trusted zone segmentation.
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
  - Cisco site: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-%20DIG.html

CPwE CIP Security in Alignment with ISA/IEC 62443

An IACS is deployed in a wide variety of industries such as oil and gas, pharmaceuticals, consumer packaged goods, pulp and paper, transportation, mining, and energy. IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations. As IACS networks migrate to converged architectures to take advantage of IIoT innovation, the challenge for industrial operations and OEMs is developing a balanced security stance while maintaining availability and usability.

To meet the industrial security needs of a wide variety of industries, Rockwell Automation correlates the development of CIP Security standard in Rockwell Automation® IACS devices with the international standard ISA/IEC 62443 (Figure 7). The series of standards are designed specifically for IACS and defines procedures to implement a secure IACS application. By aligning CPwE CIP Security with ISA/IEC 62443, Cisco, Panduit, and Rockwell Automation have committed to following global industrial security best practices based on defense-in-depth.

Figure 7 ISA/IEC 62443 Series of IACS Standards



The CPwE CIP Security solution use cases focus on the System ISA/IEC 62443-3-2 and 3-3 sections of the series, which addresses requirements at the system level.

- **62443-3-1** describes the application of various security technologies to an IACS environment. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a controls systems environment.
- **62443-3-2** addresses security risk assessment and system design for IACS. This standard is primarily directed at asset owners or end users.
- **62443-3-3** provides the foundation for assessing the security levels provided by an IACS system. The principle audience includes suppliers of industrial automation and control systems, system integrators and asset owners.

The CIP Security architecture is based on logical segmentation following the ISA/IEC 62443-3-2 Zones and Conduits model. CIP Security properties implemented within the Zone and Conduits model allow IACS networks to move towards a zero-trust security model by shifting the perimeter away from the network edge and toward the actual data. A zero-trust security model is based on a “never trust and always verify” security posture.

- **Zones** create smaller domains of trust to help protect the IACS network from the known and unknown risks in the network.
  - IACS devices are identified and grouped in zones according to common functionality and security requirements. This can be a combination of CIP Security capable IACS devices and ones that are not.
- **Conduits** control access to and from different zones. Any EtherNet/IP communication between zones must be through a defined conduit. Conduits can be defined using the following properties:
  - The communication technologies being used.
  - The protocol it transports.
  - The security properties it needs to provide to its connected zones.

The ability to proactively control interactions between IACS devices and manage internal and external data flows will help reduce security risks.

The ISA/IEC 62443-3-3 for System Security Requirements directly supports the defense-in-depth approach through its seven Foundational Requirements (FR) for securing an IACS:

- FR1: Identification and authentication control (IAC)
- FR2: Use control (UC)
- FR3: System integrity (SI)
- FR4: Data confidentiality (DC)
- FR5: Restricted data flow (RDF)
- FR6: Timely response to events (TRE)
- FR7: Resource availability (RA)

FRs specify security capabilities that enable a component to mitigate threats for a given security level. CIP Security can be applied as a building block to achieve the following FRs:

- Device identity and authentication to achieve FR1—Identification and authentication control (IAC) by ensuring only trusted controllers can access and configure the device.
- Data confidentiality (encryption) to achieve FR4—Data confidentiality (DC) through confidentiality of data in transit.
- Zones and Conduits to achieve FR5—Restricted data flow (RDF) by using zones to create smaller domains of trust to help protect the IACS network then any communication between zones must be through a defined conduit to restrict data flow.

Note For more information on ISA/IEC 62443 series of standards, see the Quick Start Guide from the ISA Global Cybersecurity Alliance at the URL: https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards

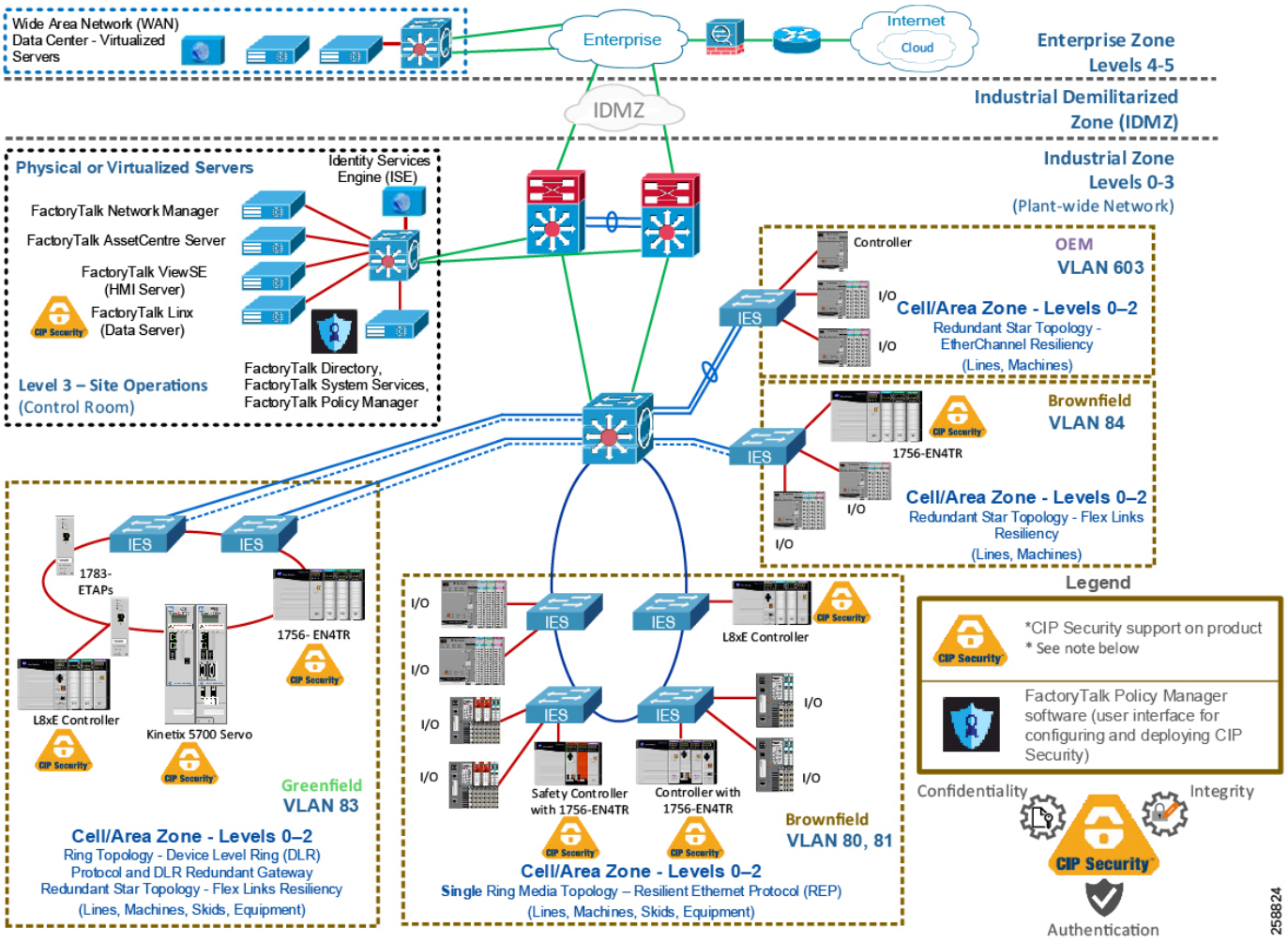
CPwE CIP Security Solution Use Cases

Rockwell Automation IACS devices currently supporting CIP Security include the following advantages:

- **Centralized System Management**—The FactoryTalk Policy Manager software is the commissioning tool used to easily create and deploy security policies to many IACS devices at once.
- **Micro-segmentation**—CIP Security is enforced at the IACS device and CIP application level, allowing segmentation to be applied at the actual IACS device and data.
- **Disable HTTP ports**—Rockwell Automation products that support CIP Security can enable or disable the unsecure HTTP ports/protocols of IACS devices in an IACS application.
- **Legacy system support**—Rockwell Automation IACS devices that support CIP Security options with legacy IACS devices:
  - Trusted IP Conduits can be created to authorize EtherNet/IP communication originating from an IACS device that does not support CIP Security to one that does support it based on IP address.
  - Retrofitting ControlLogix 5570-based IACS applications with the latest CIP Security enabled 1756-EN4TR communication module to secure EtherNet/IP communications.

The CPwE CIP Security solution use cases apply to both brownfield (legacy) and greenfield (new) deployments (Figure 8) and follow the best practice framework of CPwE.

Figure 8 CIP Security Reference Architecture



Note At the time of this publication, Rockwell Automation IACS devices supporting CIP Security include the following:

- 1756-L8xE controllers starting with version 32 or higher (GuardLogix® controllers do not support CIP Security)

  (In ControlLogix/GuardLogix 5570-based systems, retrofit the latest CIP Security enabled 1756-EN4TR communication module to secure EtherNet/IP communications.)
- 1756-EN4TR communication module
- Kinetix® 5700 servo drives starting with firmware version 11.xx or higher
- FactoryTalk Linx starting with version 6.11 or higher

To see if an IACS device supports CIP Security, refer to the specific vendor IACS device user manual or technical specification publications.

The solution use cases in Table 1 are addressed by CPwE CIP Security.

Table 1 CPwE CIP Security Solution Use Cases

Use Case	Description	Security Properties
CIP Security protection with Zone to Zone Conduits	CIP Security helps create protection for EtherNet/IP communications between the Level 3 - Site Operations FactoryTalk Applications to each Cell/Area Zone(s) CIP Security IACS device (Levels 0-2).	• Device identification and authentication • Data confidentiality (encryption) • Data integrity and authentication
CIP Security protection with Device to Device or Zone Conduits	CIP Security helps create protection for EtherNet/IP communications between IACS devices in different zones, for example ControlLogix to ControlLogix message instructions (MSG).	• Device identification and authentication • Data confidentiality (encryption) • Data integrity and authentication
CIP Security protection with Trusted IP Conduit	For IACS applications, use FactoryTalk Policy Manager to create conduits with a list of trusted IP addresses for EtherNet/IP communications between non-CIP Security IACS devices and applications to CIP Security IACS devices.	• Trusted IP feature

CIP Security Protection with Zone to Zone Conduits

Most threats originate from high in the IACS architecture where Windows and other operating systems are more prevalent. These threats attempt to deny access or service, obtain sensitive data or even input false commands to the lower level Industrial Zone.

CIP Security helps create protection for EtherNet/IP communications between the Level 3 - Site Operations FactoryTalk Applications to each Cell/Area Zone(s) CIP Security IACS device (Levels 0-2) (Figure 9).

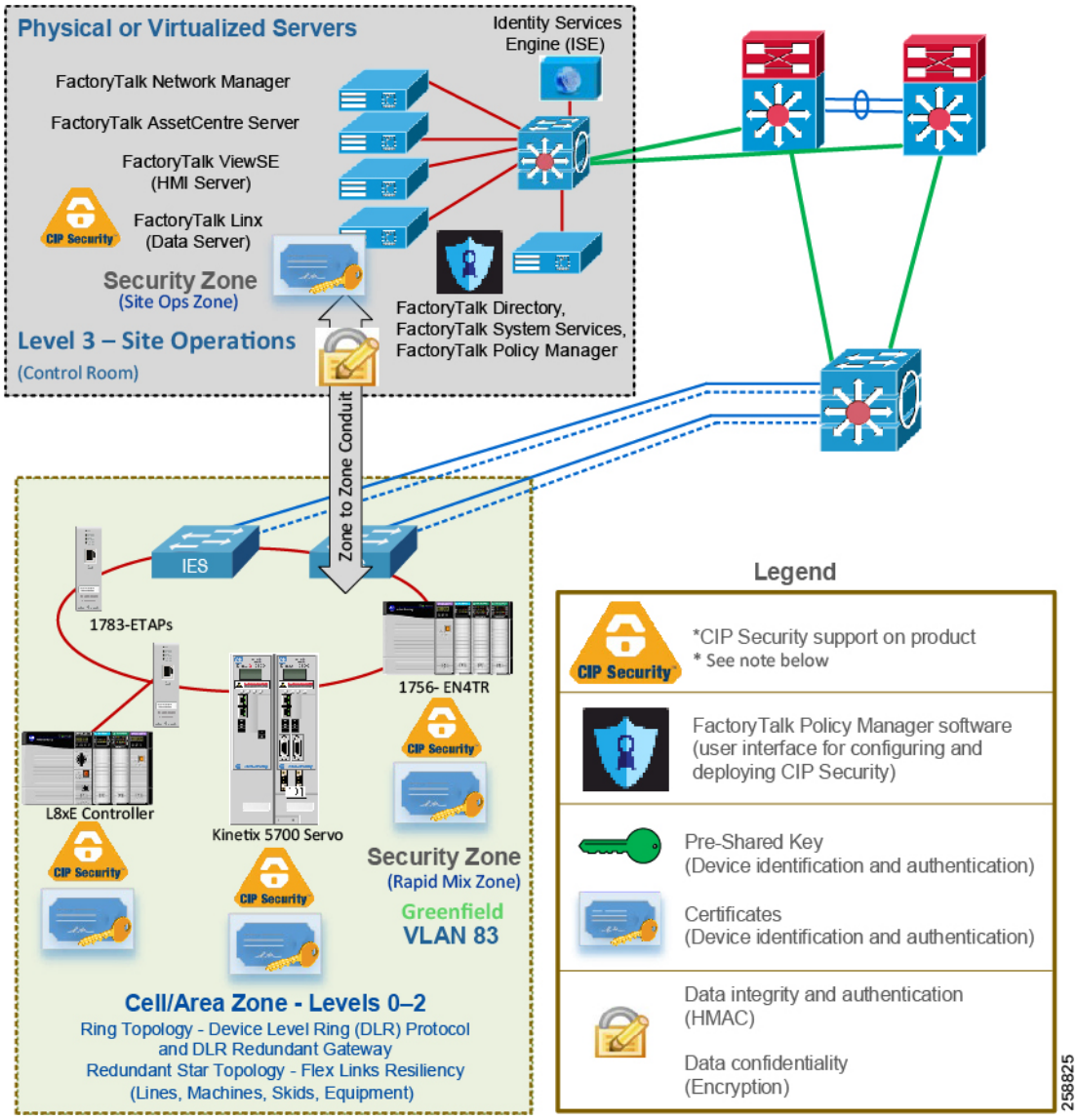
With the device identification and authentication properties of CIP Security, communicating entities must provide some information about themselves that is trustworthy and verifiable before data is exchanged. To build this endpoint trust, a certificate or pre-shared (secret) key can be used to provide identity to the device:

- Pre-shared keys are used to prove identity that is based on keys that are shared in advance among the communicating parties.
- A certificate is used to provide identity based on the X.509v3 standard.

Certificates are an agreement between communicating parties and a common entity called a Certificate Authority (CA). A trusted CA signs and issues certificates to requesters to prove their identities. Mutual trust is established when communicating parties exchange certificates signed by a common CA.

- **FactoryTalk System Services** is the certificate authority. It is the service that signs and issues client certificates to give assurance for a communicating party's authenticity.
- **FactoryTalk Policy Manager** is the commissioning tool graphical user-interface (GUI) used to configure, deploy, and view the system communication security policies.

Figure 9 Use Case 1—CIP Security Protection with Zone to Zone Conduits



Note See the specific vendor IACS device user manual or technical specification publications for verification of CIP Security support.

CIP Security Protection with Device to Device or Zone Conduits

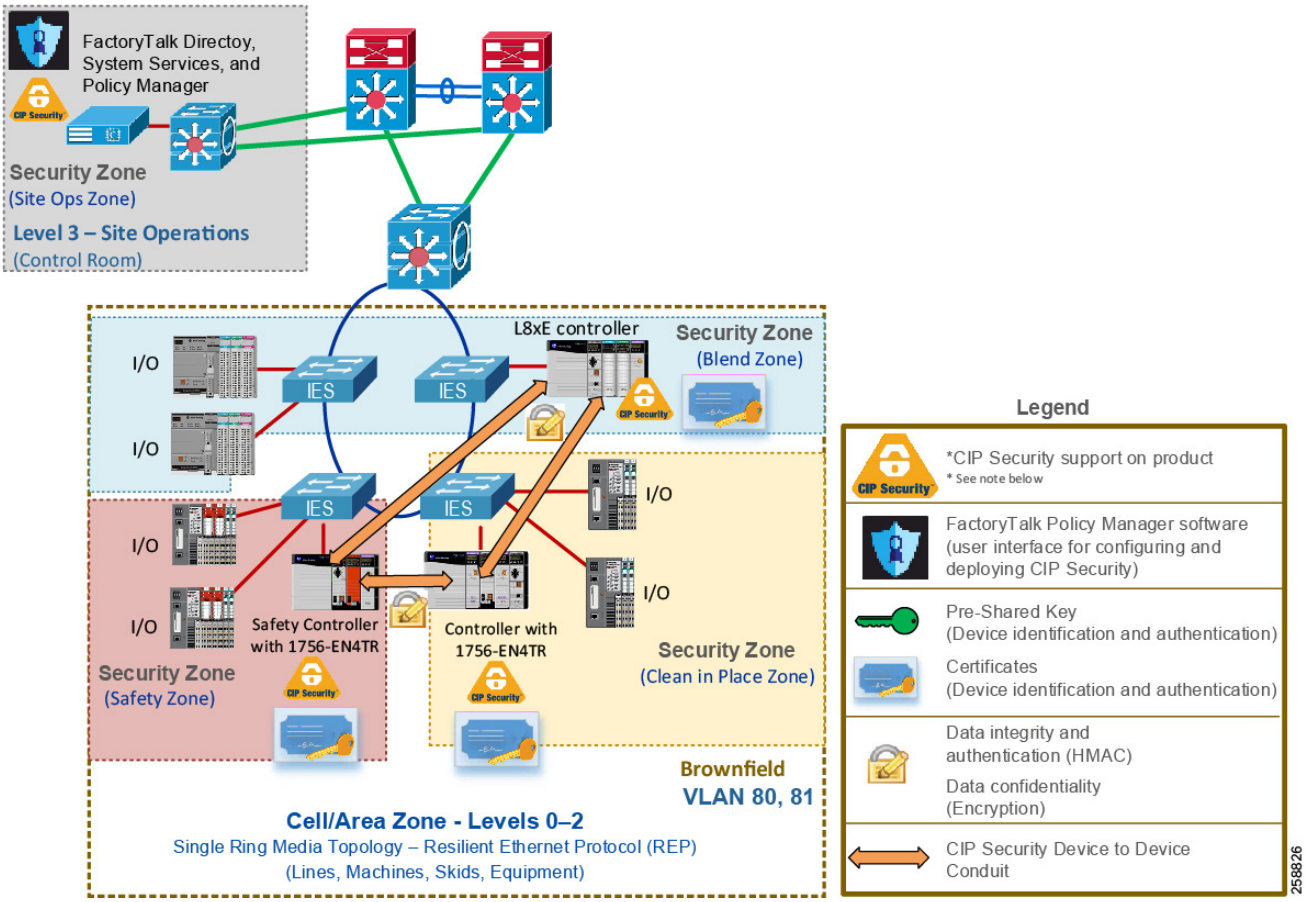
Data in transit can be intercepted, allowing for sensitive information such as secret recipes to be stolen. Even worse, data tampering by way of unauthorized changes to configuration, programs, commands, or alarming may cause personnel to initiate incorrect actions leading to a number of undesirable events, such as equipment damage, operation unavailability, endangering human life, and environmental impacts.

CIP Security helps create protection for EtherNet/IP communications between IACS devices in different zones (Figure 10), for example ControlLogix to ControlLogix message instructions (MSG) through the TLS network protocol.

- TLS and DTLS are network protocols that facilitate data transfer confidentially and securely between a client and a server device. DTLS is based on TLS but is used for User Datagram Protocol (UDP) connections instead of Transmission Control Protocol (TCP) connections.

CIP Security enables the sender IACS device to calculate a keyed hash before transit to send along with the original message. Hash functions use a deterministic algorithm that takes in one input and produces a fixed length string every time; therefore, using the same input will always result in the same output. The fixed length string is then encrypted with a shared key to create a keyed hash to ensure integrity and authenticity of the message. Once the receiver IACS device gets the message, it can run the hash algorithm and compare the output with the keyed hash received. If both keyed hashes are different, it means that the message was tampered with and is rejected.

Figure 10 Use Case 2—CIP Security Protection with Device to Device or Zone Conduits



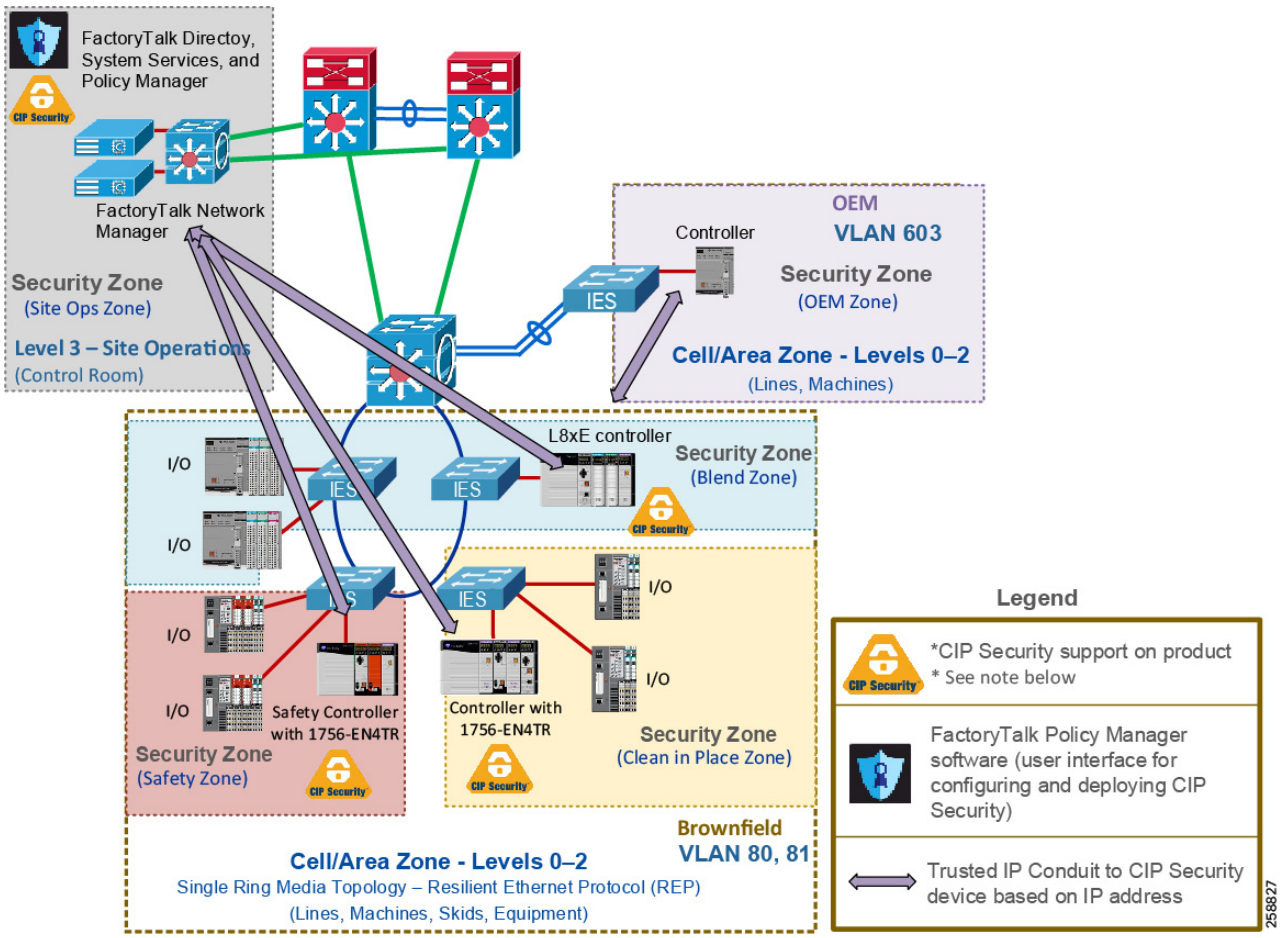
Note See the specific vendor IACS device user manual or technical specification publications for verification of CIP Security support.

CIP Security Protection with Trusted IP Conduits

Rockwell Automation IACS devices and software currently supporting CIP Security are still able to interoperate with IACS devices that do not support CIP Security on the same network by using the Trusted IP feature. The feature is like the concept of whitelisting in which it can be configured to authorize EtherNet/IP communication, based on IP address, between an IACS device that is capable of CIP Security and one that is not. This can be used for network management tools like FactoryTalk Network Manager that do not support CIP Security, but require a CIP connection to the CIP Security enabled IACS devices for asset discovery purposes.

For IACS applications, use FactoryTalk Policy Manager to create conduits with a list of trusted IP addresses for EtherNet/IP communications between non-CIP Security IACS devices and applications to CIP Security IACS devices (Figure 11).

Figure 11 Use Case 3—Rockwell Automation CIP Security with Trusted IP Conduits



Note See the specific vendor IACS device user manual or technical specification publications for verification of CIP Security support.

Summary

CPwE is a collection of architected, tested, and validated designs. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies.

The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations and OEMs with the design and deployment of a scalable, reliable, secure, and future-ready plant-wide or site -wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology. CPwE is brought to market through an ecosystem consisting of Cisco, Panduit, and Rockwell Automation emergent from the strategic alliance between Cisco Systems and Rockwell Automation.

Industrial IoT (IIoT) offers the promise of business benefits using innovative technologies such as mobility, collaboration, analytics, and cloud-based services. The challenge for industrial operations and OEMs is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. The *Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide* outlines several industrial security use cases for designing and deploying CIP Security technology throughout a plant-wide or site-wide Industrial Automation and Control System (IACS) network infrastructure. CPwE CIP Security highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the CPwE framework. CPwE CIP Security was architected, tested, and validated by Rockwell Automation with assistance by Cisco Systems and Panduit.

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:
  http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?
- Cisco site:
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

.

Panduit Corp. is a world-class provider of engineered, flexible, end-to-end electrical and network connectivity infrastructure solutions that provides businesses with the ability to keep pace with a connected world. Our robust partner ecosystem, global staff, and unmatched service and support make Panduit a valuable and trusted partner.

www.panduit.com

US and Canada:
Panduit Corp.
World Headquarters
18900 Panduit Drive
Tinley Park, IL 60487
iai@panduit.com
Tel. 708.532.1800

Asia Pacific:
One Temasek Avenue #09-01
Millenia Tower
039192 Singapore
Tel. 65 6305 7555

Europe/Middle East/Africa:
Panduit Corp.
West World
Westgate London W5 1XP Q
United Kingdom
Tel. +44 (0) 20 8601 7219

Latin America:
Panduit Corp.
Periférico Pte Manuel Gómez
Morin #7225 - A
Guadalajara Jalisco 45010
MEXICO
Tel. (33) 3777 6000

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 be more productive and the world more sustainable. In support of smart manufacturing concepts, Rockwell Automation helps customers maximize value and prepare for their future by building a Connected Enterprise.

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-WP043B-EN-P May 2020