CHAPTER 1

CPwE CIP Security Overview

This chapter includes the following major topics:

CPwE CIP Security Introduction

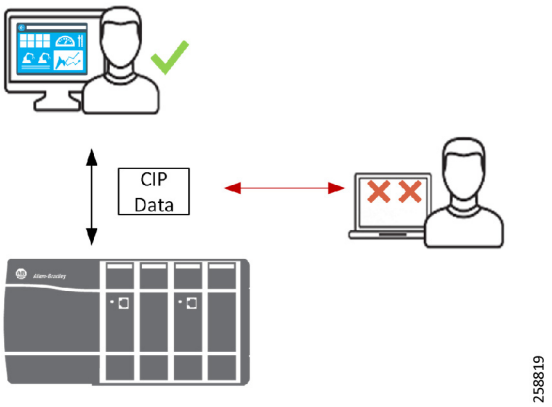
The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including 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:

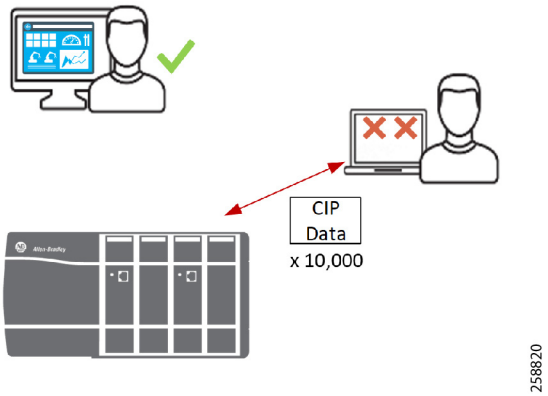
- A **reconnaissance attack** (Figure 1-1) is a multi-stage process, which includes an unauthorized entity eavesdropping on data in transit between IACS devices. This typically results in the unauthorized entity learning more about the activities and vulnerabilities of the operation leading to loss of 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 1-1 Reconnaissance Attack



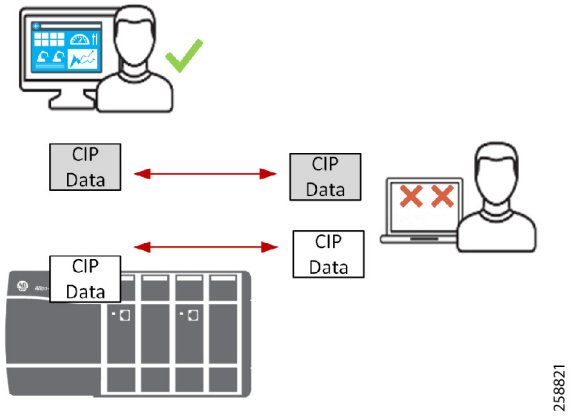
- A **denial-of-service (DoS) attack** (Figure 1-2) is a process where an unauthorized entity sends large amounts of arbitrary packets to overwhelm the IACS device (CPU and resources) thus rendering the device inoperable resulting in loss of availability.

Figure 1-2 Denial-of-Service (DoS) Attack



- A **man-in-the-middle (MITM) attack** (Figure 1-3) 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 1-3 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 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 over 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. See the following sections for more details and limitations:

- CIP Security Properties in Chapter 2, "CPwE CIP Security Design Considerations"
- CIP Security Limitations in Chapter 2, "CPwE CIP Security Design Considerations"

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.

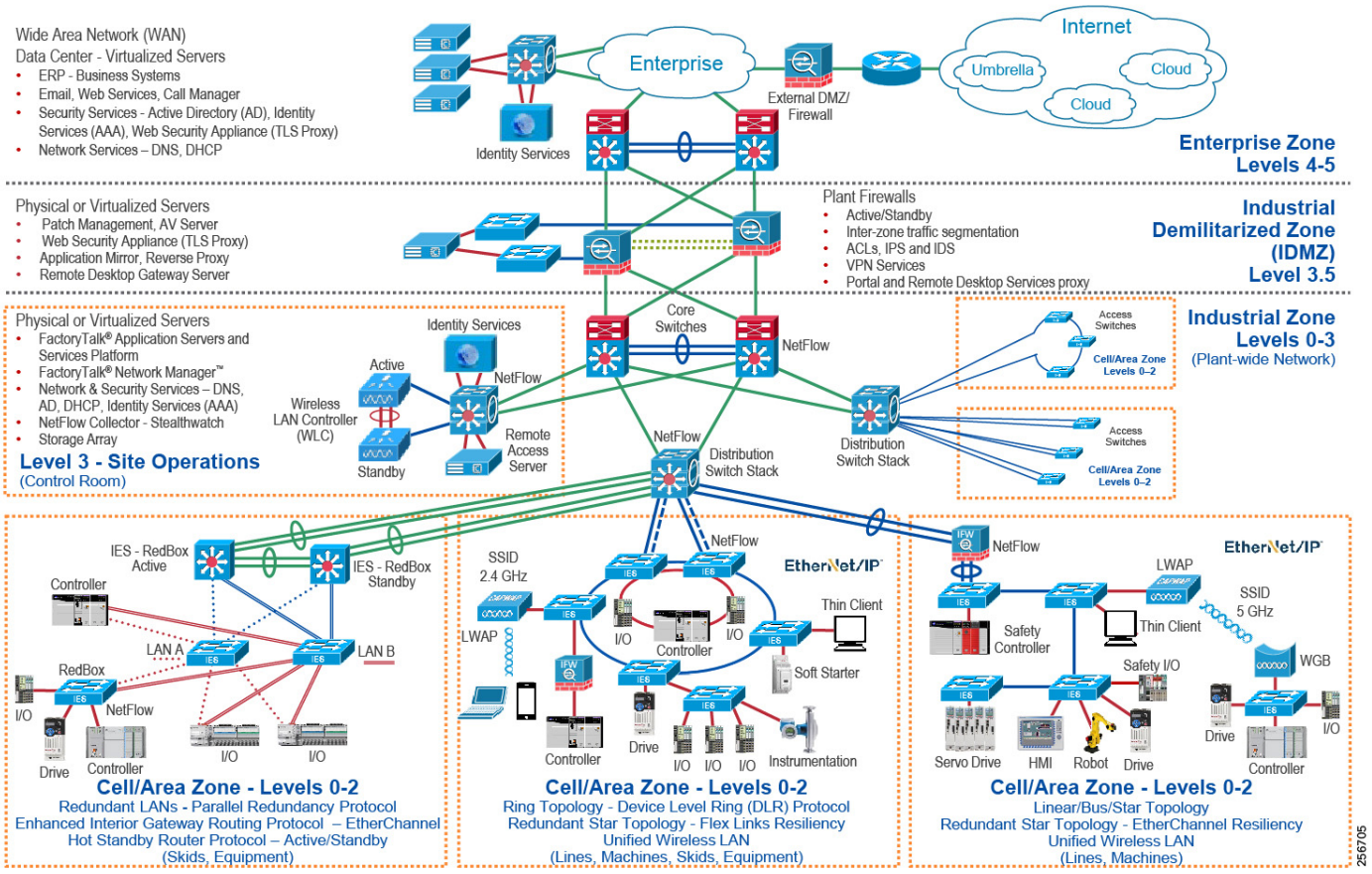
CPwE Overview

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 1-4) 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 1-4 CPwE Architectures



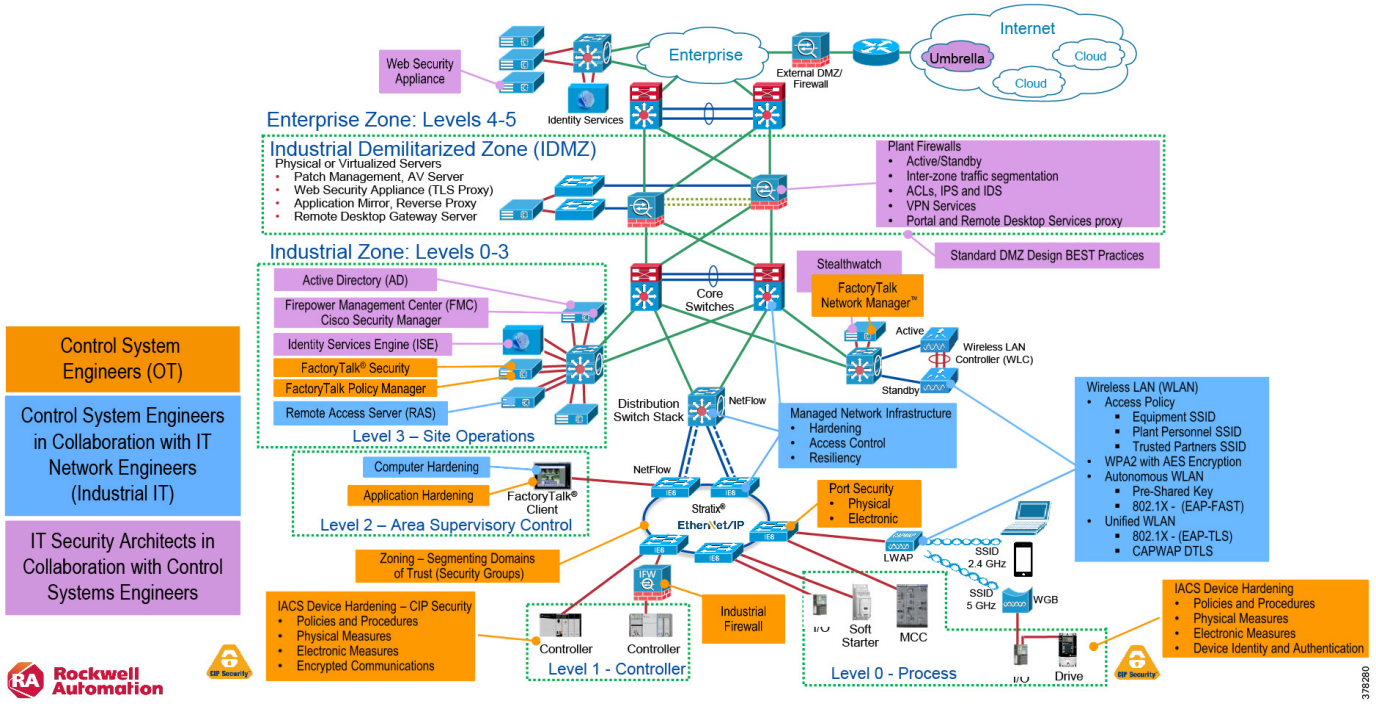
CPwE Industrial Security Framework Overview

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 1-5).

- **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 whitelisting), 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 1-5 CPwE Industrial Security Framework



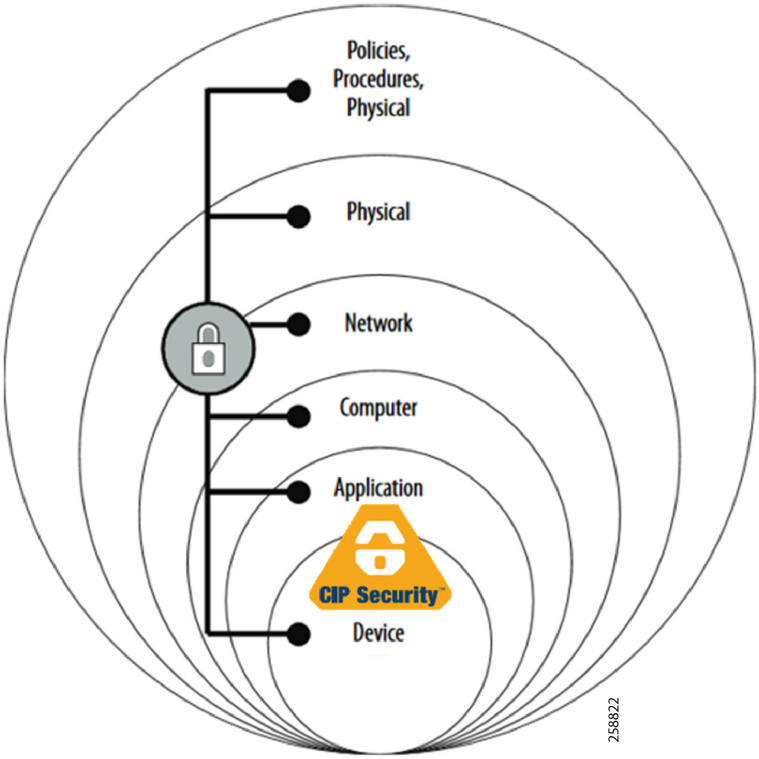
The CPwE Industrial Security Framework (Figure 1-5), using a defense-in-depth approach, is aligned to industrial security standards such as ISA/IEC-62443 Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

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 1-6), 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 or 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 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 1-6 Defense-in-Depth Security



In a defense-in-depth security approach (Figure 1-6), 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

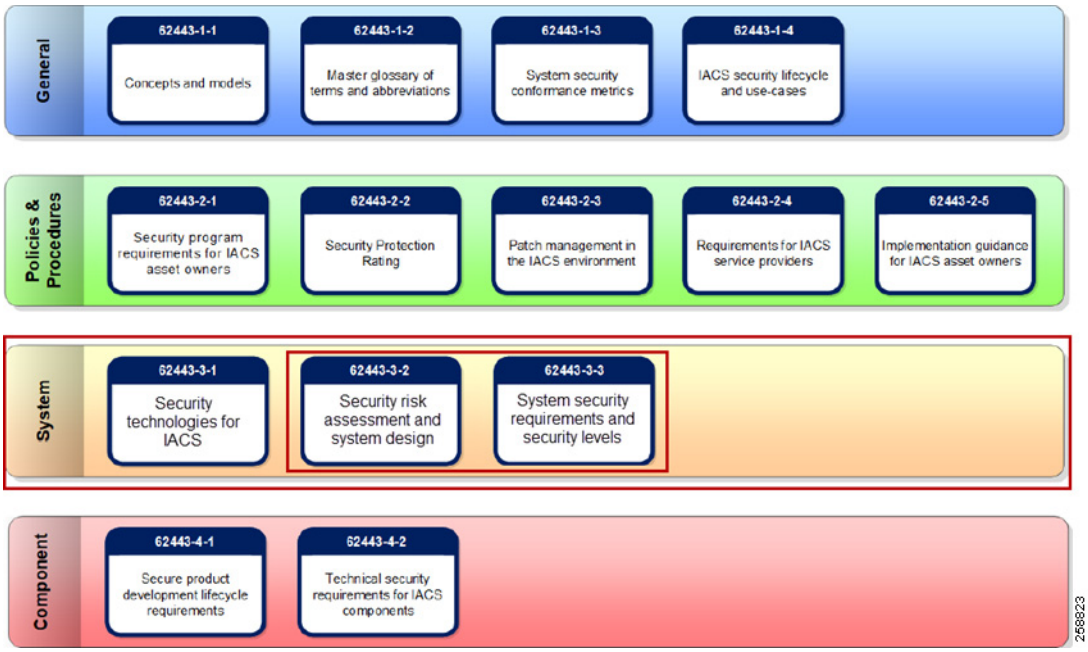
- *Cloud Connectivity to a Converged Plantwide Ethernet Architecture Design Guide* outlines several industrial security architecture use cases for designing and deploying restricted end-to-end outbound connectivity from FactoryTalk applications to the Rockwell Automation cloud within a CPwE architecture.
  - 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 1-7). 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 1-7 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.

The CIP Security architecture is based on logical segmentation following the ISA/IEC 62443-3-2 Zones and Conduits model. Segmentation is a practice of zoning the IACS network to 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. Conduits control access to and from different zones. Any EtherNet/IP communication between zones must be through a defined conduit. The ability to proactively control interactions between IACS devices and manage internal and external data flows will help reduce security risks.

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.

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)

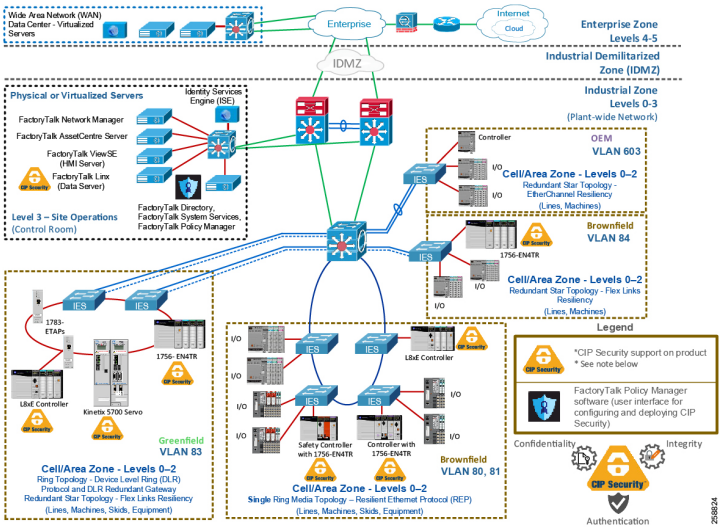
FRs specify security capabilities that enable a component to mitigate threats for a given security level. CIP Security properties can be applied as a building block to support the security posture of an organization.

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

CIP Security Solution Use Cases

The CPwE CIP Security solution use cases apply to both brownfield (legacy) and greenfield (new) deployments (Figure 1-8) and follow the best practice framework of CPwE.

Figure 1-8 CIP Security Reference Architecture



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

- ControlLogix 5580 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

For a more information on Rockwell Automation products and software that support CIP Security listed above, see Table 2-3.

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

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

Table 1-1 CPwE CIP Security Solution Use Cases

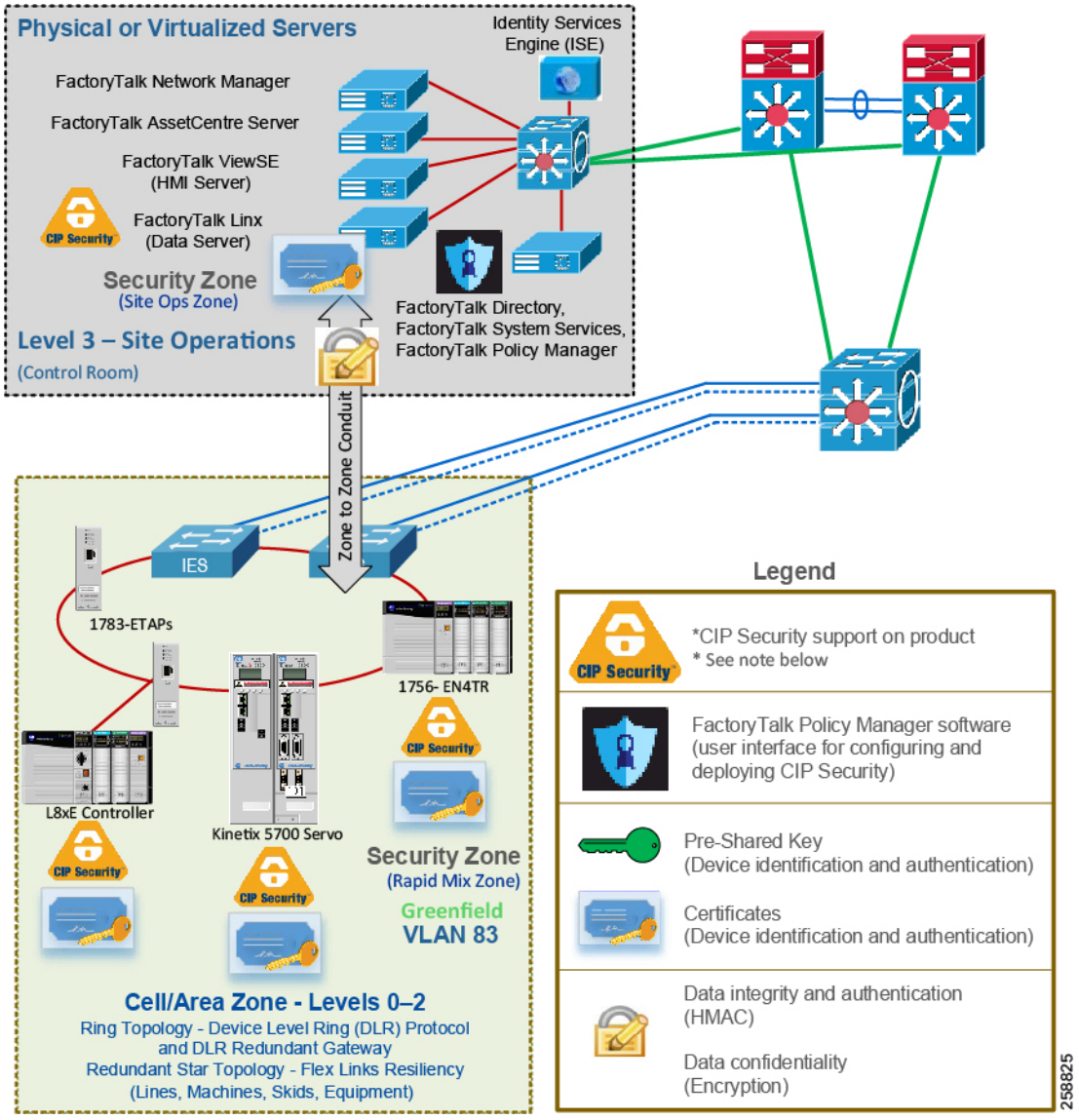
Use Case	Description	Security Properties
CIP Security protection with Zone to Zone Conduits	CIP Security helps create protection for EtherNet/IP communications between the Level 3 - Site Operations FactoryTalk Applications to each Cell/Area Zone(s) CIP Security IACS device (Levels 0-2).	• Device identification 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 1-9).

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



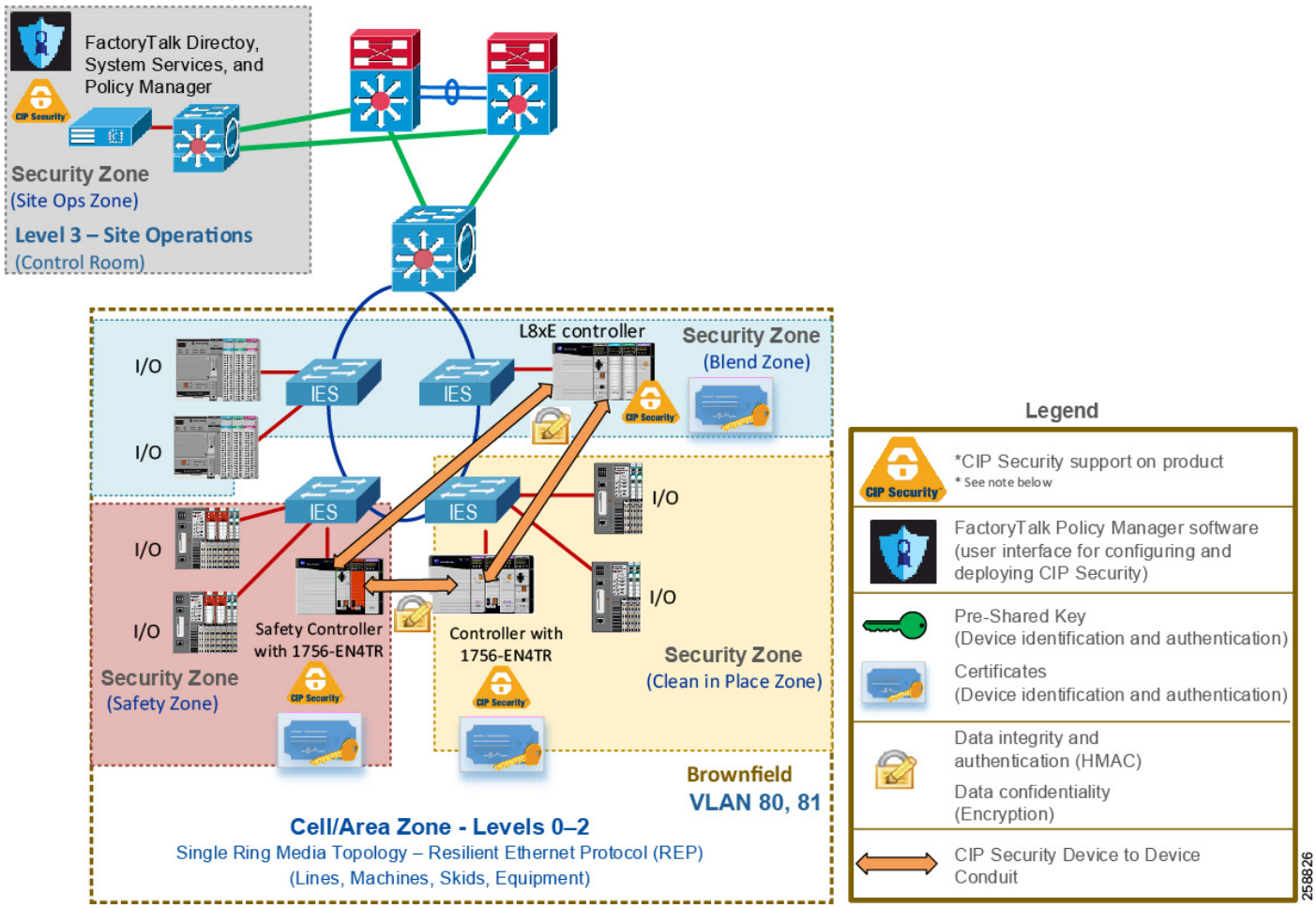
Note See the specific vendor IACS device user manual, technical specification, or release notes publications for verification of CIP Security support.

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, for example ControlLogix to ControlLogix message instructions (MSG) through the TLS network protocol (Figure 1-10).

Figure 1-10 Use Case 2—CIP Security Protection with Device to Device or Zone Conduits



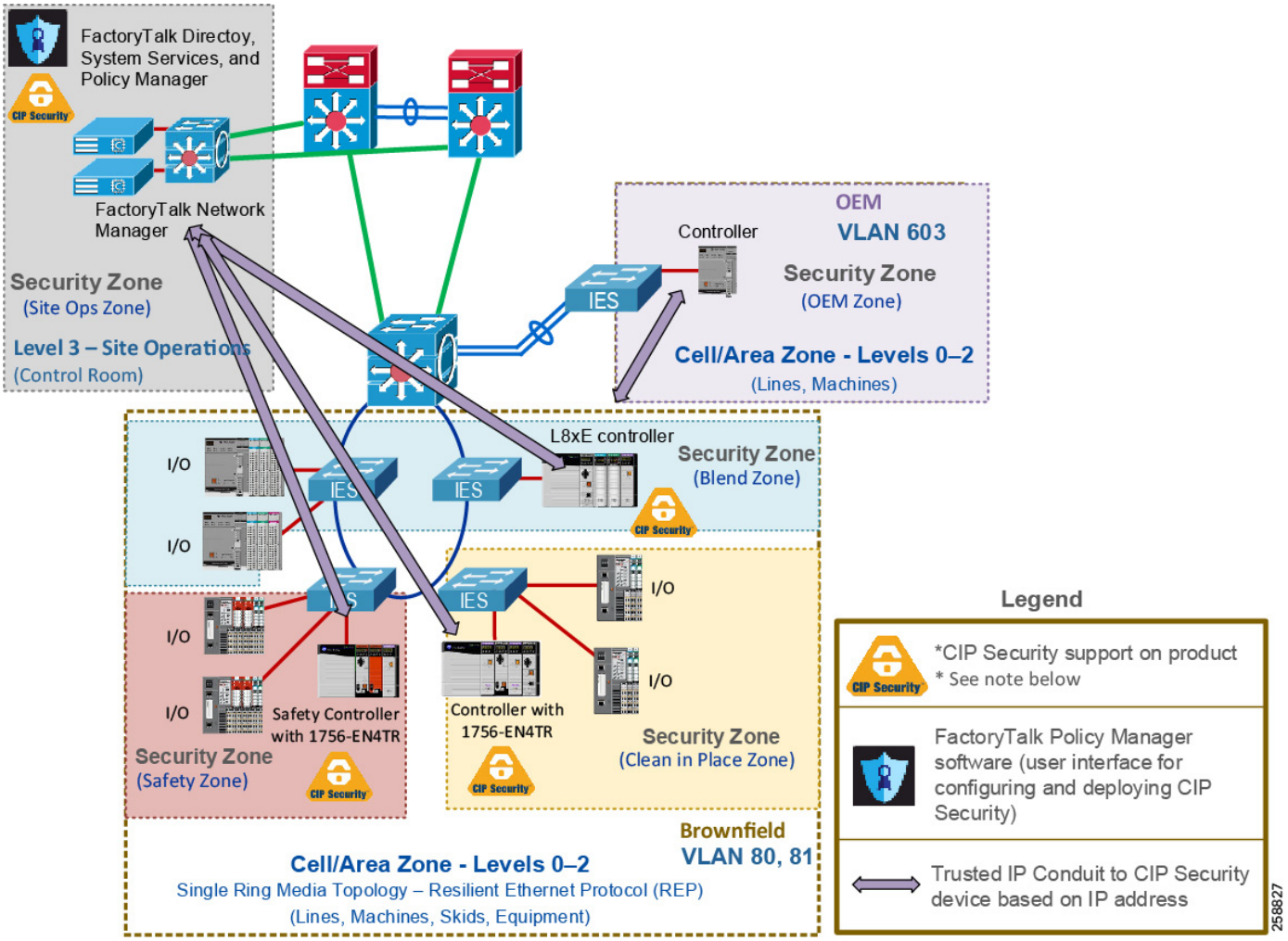
Note See the specific vendor IACS device user manual, technical specification, or release notes publications for verification of CIP Security support.

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 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 1-11).

Figure 1-11 Use Case 3—Rockwell Automation CIP Security with Trusted IP Conduits



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