Deploying CIP Security within a Converged Plantwide Ethernet Architecture

Design Guide

September 2021

Preface

Converged Plantwide Ethernet (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 achieve 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 by 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.

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

CPwE CIP Security provides a comprehensive explanation of the CIP Security application design. It includes information about key requirements, possible deployment models, potential challenges, technology considerations, and guidelines for implementation and configuration of these specific use security cases within the CPwE framework.

Document Organization

This document contains the following chapters and appendices:

Chapter	Description
Chapter 1, "CPwE CIP Security Overview"	CPwE Overview, CPwE Industrial Security Framework Overview, CPwE CIP Security in alignment with ISA/IEC 62443, and CIP Security Solution Use Cases
Chapter 2, "CPwE CIP Security Design Considerations"	System Components, IACS Security Policy Considerations, Technology Considerations, and Architectural Considerations

Chapter	Description
Chapter 3, "CPwE CIP Security Configuration"	Describes how to configure CPwE CIP Security within the CPwE architecture based on the design considerations and recommendations of the previous chapter. This includes deploying, changing, and removing CIP Security properties using FactoryTalk® Policy Manager.
Chapter 4, "Verifying and Troubleshooting the Deployment"	Information on verifying and troubleshooting CPwE CIP Security.
Appendix A, "References"	Links to documents and websites that are relevant to *Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide*.
Appendix B, "Acronyms and Initialisms"	List of acronyms and initialisms used in this document.
Appendix C, "About the Cisco Validated Design (CVD) Program"	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs).

For More Information

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:
    - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

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

For More Information

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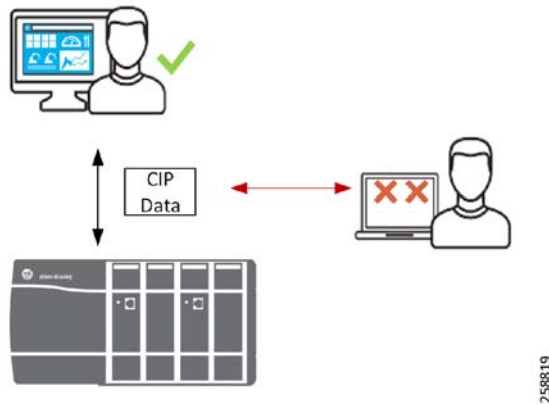
- A **denial-of-service (DoS) attack** (Figure 1-2) is a process where an unauthorized entity sends large amounts of arbitrary packets to overwhelm the IACS device (CPU and resources) thus rendering the device inoperable resulting in loss of availability.

Figure 1-2   Denial-of-Service (DoS) Attack
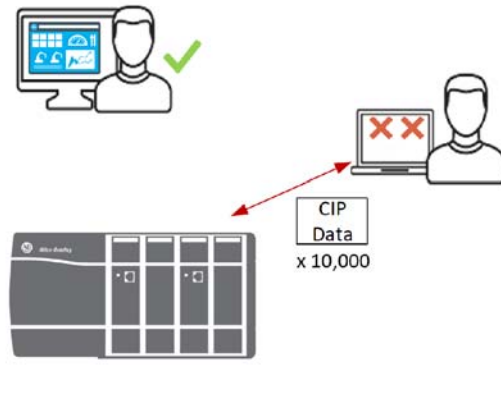
- A **man-in-the-middle (MITM) attack** (Figure 1-3) is a process where an unauthorized entity intercepts and changes the data to issue unauthorized commands or alter alarm thresholds, thus damaging or shutting down equipment and operations resulting in loss of integrity.

Figure 1-3   Man-in-the-Middle (MITM) Attack
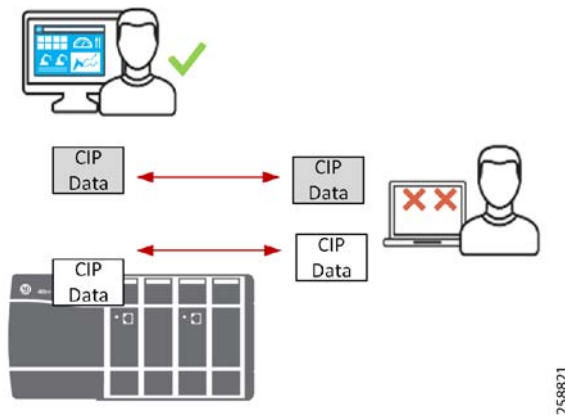
With all the opportunities and challenges faced by industrial operations, there is a strong need for the following requirements:

- **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.
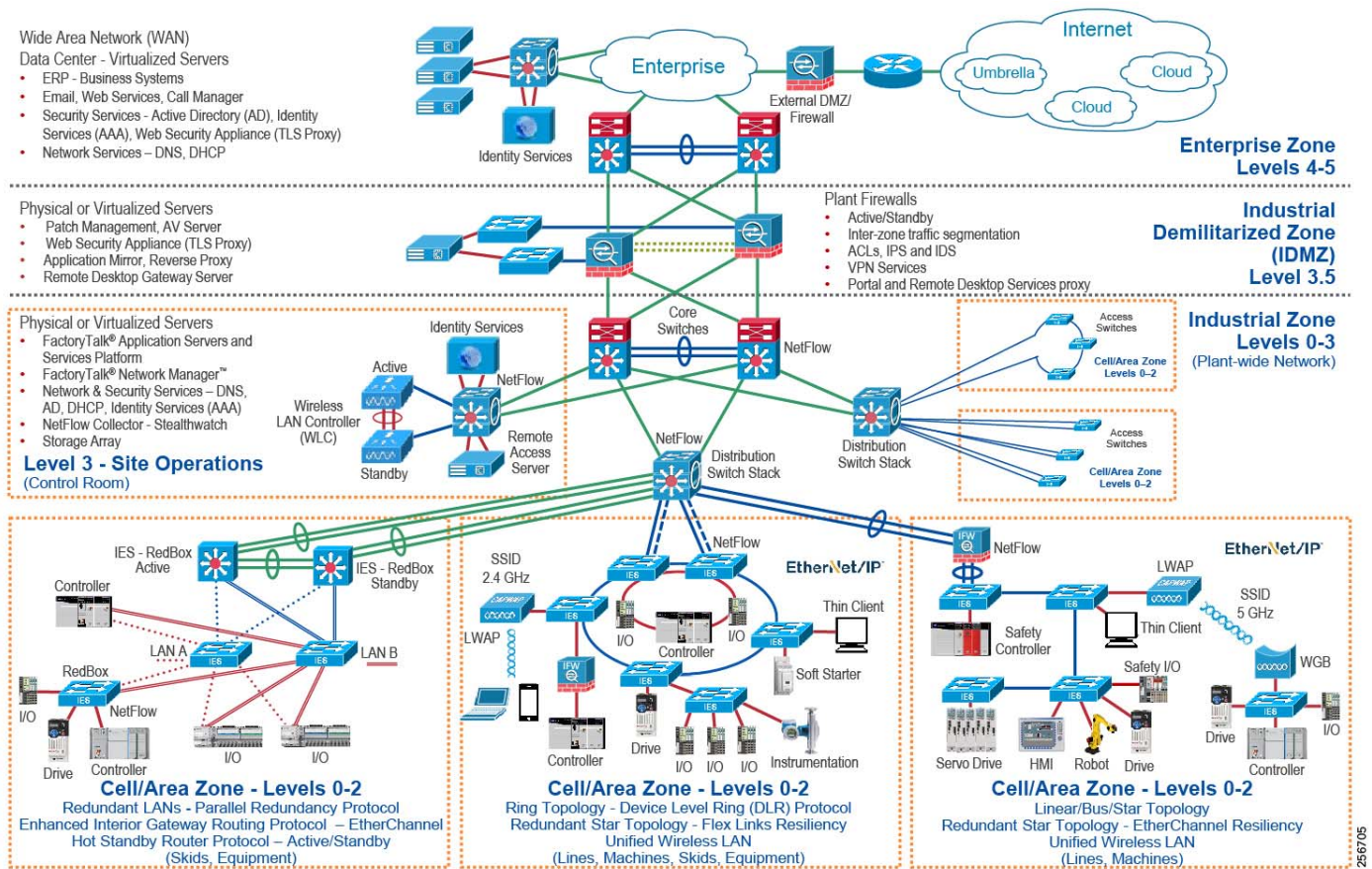
CPwE Overview

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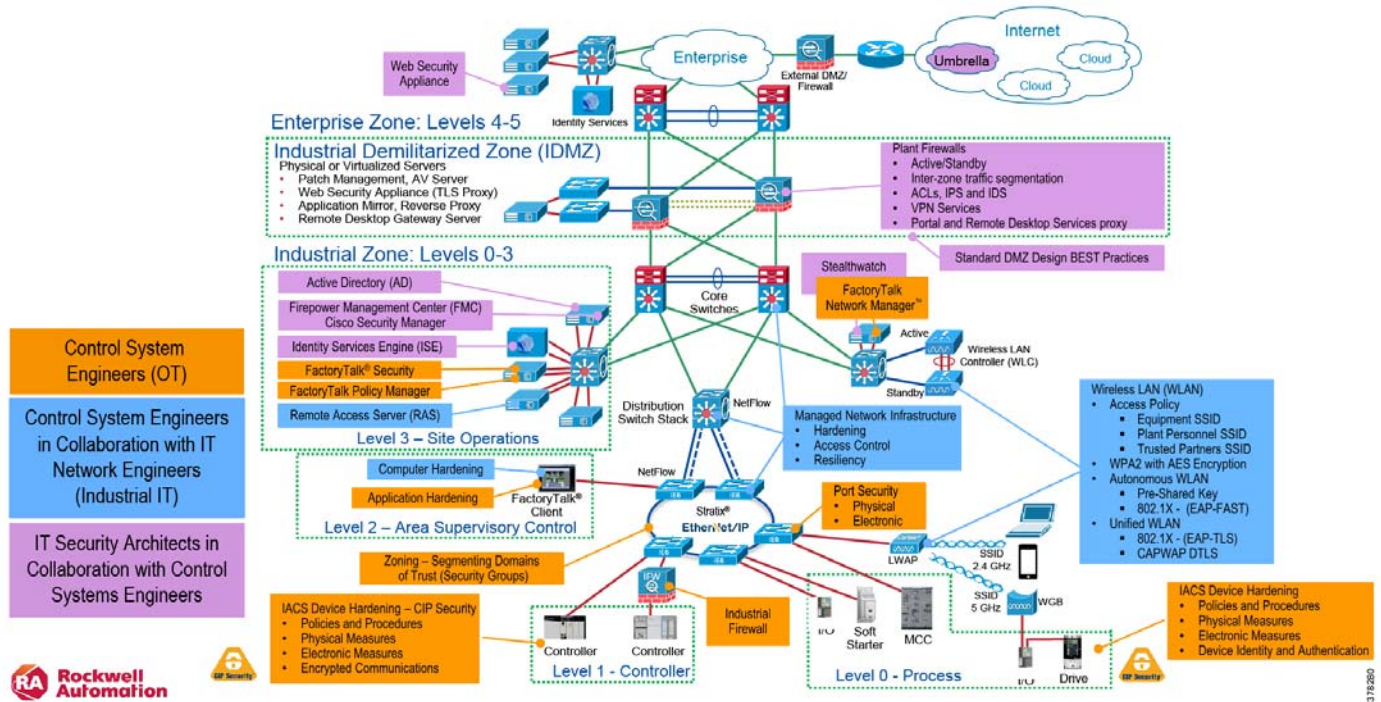
The CPwE Industrial Security Framework (Figure 1-5), using a defense-in-depth approach, is aligned to industrial security standards such as ISA/IEC-62443 Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

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
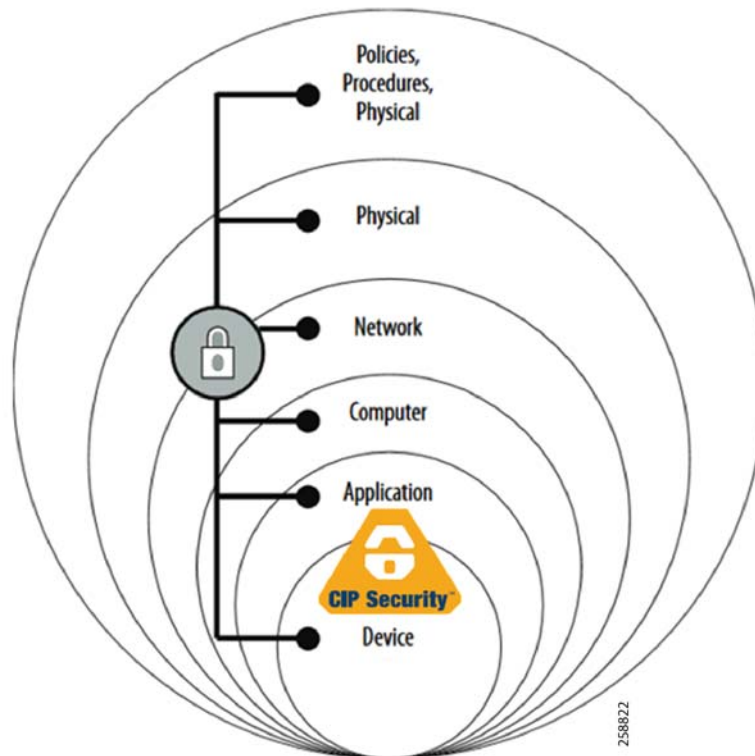
In a defense-in-depth security approach (Figure 1-6), different solutions are needed to address various network and security requirements for a plant-wide or site-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different 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
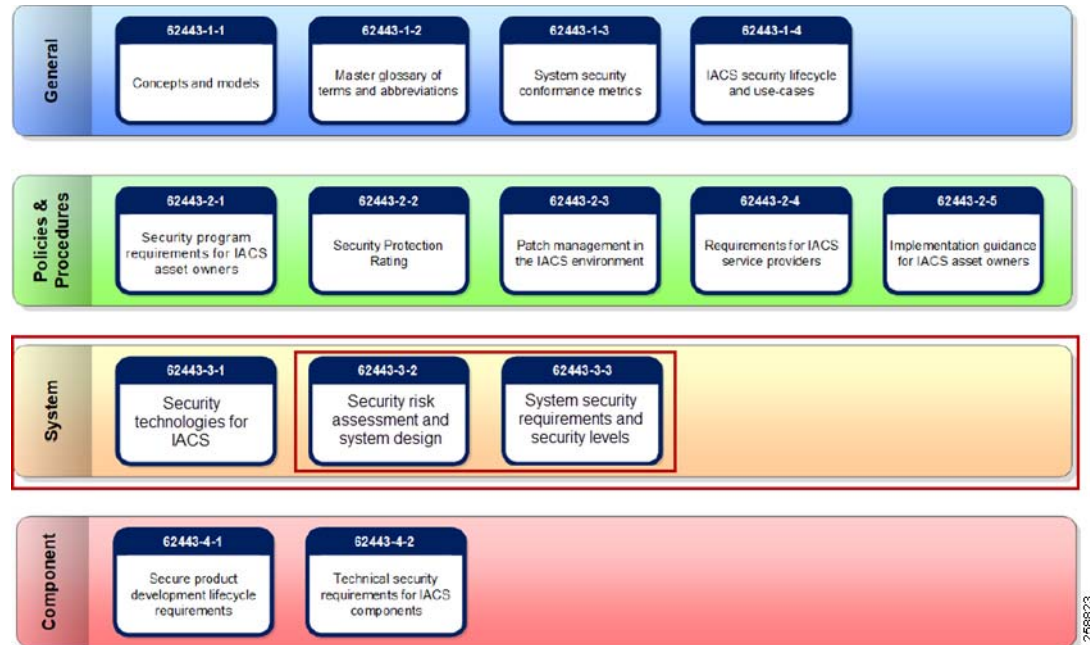
The CPwE CIP Security solution use cases focus on the System ISA/IEC 62443-3-2 and 3-3 sections of the series, which addresses requirements at the system level.

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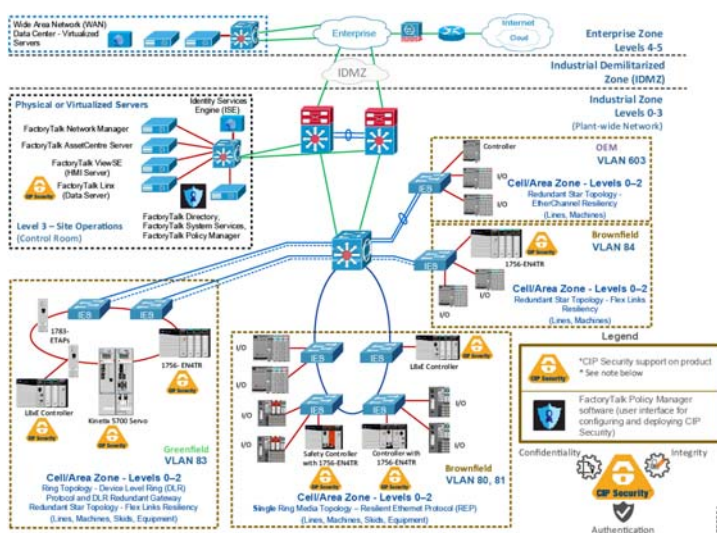
Note   At the time of this publication, Rockwell Automation IACS devices supporting CIP Security include the following:

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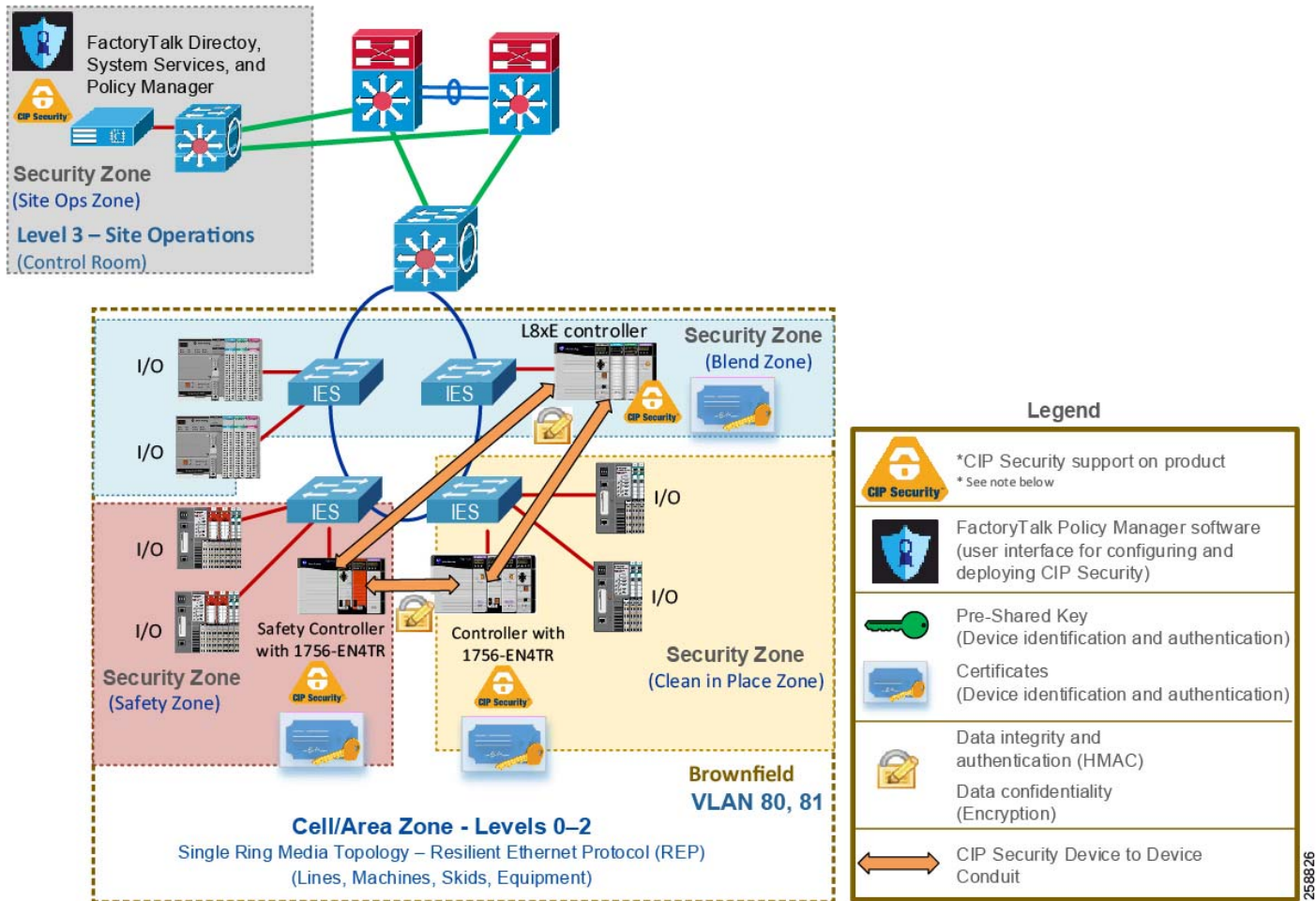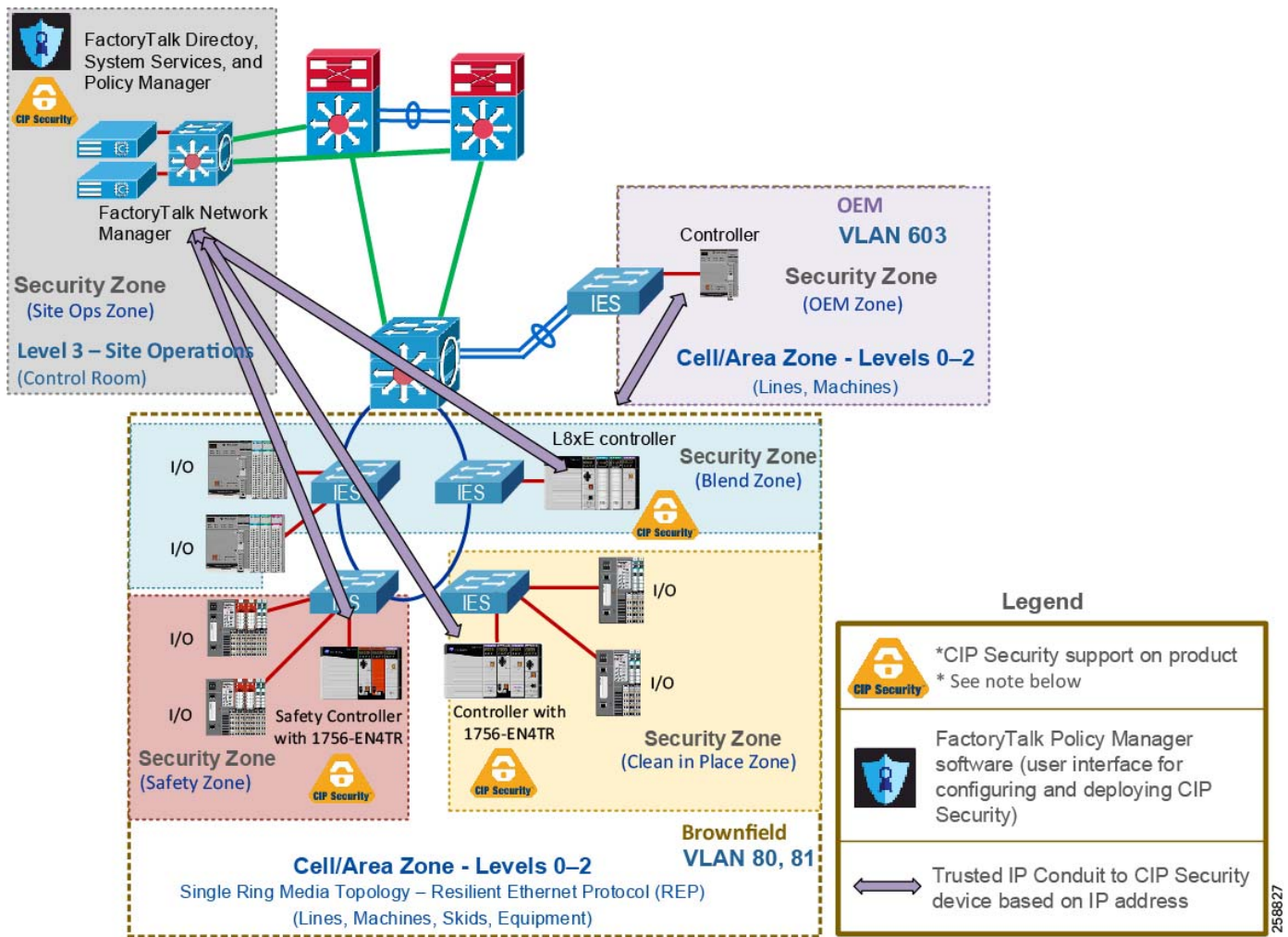
See the specific vendor IACS device user manual, technical specification, or release notes publications for verification of CIP Security support.

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.

CPwE CIP Security Design Considerations

This chapter describes basic design considerations when implementing CIP Security in an IACS architecture. This CRD offers basic guidance for CIP Security, including security policy considerations incorporating a threat model overview, alignment with ISA/IEC 62443, technology considerations with TLS/DTLS protocols, and architectural considerations with network segmentation, which IACS networking personnel could use to design and deploy their architecture. This also includes the CPwE CIP Security Solution use cases and their various components and their relation to each other.

Note The client/server terminology is commonly used with TCP and TLS/DTLS connections and originator/target for CIP connection. However, for simplicity of this document, the terms client/server will be generalized and used throughout this document when discussing the behavior associated with a connection of an IACS device. The client initiates a connection and the server listens for and accepts a connection.

System Components

The following tables and section list the Rockwell Automation and Cisco components that are involved in this reference design:

- Table 2-1 lists the Rockwell Automation and Cisco network components.
- Table 2-2 lists the Rockwell Automation IACS hardware components.
- Table 2-3 lists the Rockwell Automation software components.
- Additional Resources lists additional resources related to Rockwell Automation products.

Table 2-1   Network Hardware and Firmware

Role	Product	Technology	Software Release
Core Switch	Cisco Catalyst 9500 swtich	Switch Virtual	16.12.x
Distribution Switch	Cisco Catalyst 9300 switch	StackWise 480	16.12.x
Layer 2 Industrial Ethernet Switch (IES)	Allen-Bradley Stratix 5700/5400 switch	DLR Redundant Gateway, DLR, REP, Flex Links, EtherChannel	15.2(7)E

Table 2-2   IACS Hardware and Firmware

Role	Product	Catalog number	Firmware Version
Programmable Automation Controller (PAC)	ControlLogix 5580[1] controller	1756-L85E[1]	32.011
PAC	ControlLogix 5570 controller	1756-L75/B	32.011
PAC	CompactLogix™ 5380 controller	5069-L340ERM/A	32.011
Safety PAC	GuardLogix 5570 controller	1756-L73S	32.011
Ethernet Communication module	ControlLogix EtherNet/IP module[1]	1756-EN4TR/A[1]	2.001
I/O module	POINT I/O™ EtherNet/IP Adapter	1734-AENTR/B	5.016
I/O module	Compact 5000™ I/O EtherNet/IP Adapter	5069-AEN2TR/B	3.011

1. The following note lists the catalog numbers with the associated firmware versions that currently support CIP Security.

Note   At the time of this publication, Rockwell Automation products 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

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

Table 2-3   Rockwell Automation Software and Firmware

Role	Product/Service	Host	Firmware Version
FactoryTalk Services Platform[1]			6.11.00 (CPR 9 SR 11)
Network Directory Certificate Authority (CA) CIP Security configuration interface	FactoryTalk Network Directory FactoryTalk System Services[1] FactoryTalk Policy Manager[1] software	Windows Server 2016	6.11.00 (CPR 9 SR 11)
Data Server	FactoryTalk Linx[1] software	Windows Server 2016	6.11.00 (CPR 9 SR 11)
HMI Server	FactoryTalk View SE software	Windows Server 2016	11.00.00 (CPR 9 SR 11)
HMI Client	FactoryTalk View SE software	Windows 10	11.00.00 (CPR 9 SR 11)
Design and programming	Studio 5000 Logix Designer®[1] software	Windows 10	32.00.00 (CPR 9 SR 11)
Network management tool	FactoryTalk Network Manager software	Windows Server 2016	1.07

1.   The following note lists the catalog numbers with the associated firmware versions that currently support CIP Security.

Note   In the initial release of CIP Security, it is required to install FactoryTalk System Services and FactoryTalk Policy Manager software on the computer that hosts the FactoryTalk Network Directory.

- FactoryTalk System Services is the Certificate Authority (CA), which is the service that signs and issues client certificates to give assurance for the authenticity of a a communicating party. It runs as a service in the background to help enable the deployment of CIP Security policies configured in the FactoryTalk Policy Manager commissioning tool.

- FactoryTalk Policy Manager is the commissioning tool graphical user-interface (GUI) used to configure, deploy, and view the system communication security policies.

Additional Resources

For more information and a list of Rockwell Automation products supporting CIP Security including software and hardware, see:

- *FactoryTalk Policy Manager Getting Results Guide*, publication FTALK-GR001—Describes how to install and use FactoryTalk System Services and FactoryTalk Policy Manager.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/gr/ftalk-gr001_-en-e.pdf

- *FactoryTalk Security System Configuration Guide Quick Start*, publication FTSEC-QS001—Describes how to use FactoryTalk Services Platform with FactoryTalk Security.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-e.pdf

- *FactoryTalk Linx Getting Results Guide* LNXENT-GR001—Describes information on installing, navigating, and using FactoryTalk Linx.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/gr/lnxent-gr001_-en-e.pdf

- *CIP Security with Rockwell Automation Products Application Technique* SECURE-AT001—Describes components and concepts that are part of the Rockwell Automation method of implementing CIP Security in an IACS.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/at/secure-at001_-en-p.pdf

- *ControlLogix 5580 and GuardLogix 5580 Controllers User Manual*, publication 1756-UM543—Describes how to design, implement, and maintain an industrial control system that uses ControlLogix or GuardLogix based controllers.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um543_-en-p.pdf

- *ControlLogix EtherNet/IP Network Devices User Manual*, publication 1756-UM004—Describes how to use ControlLogix EtherNet/IP communication modules with a Logix 5000™ controller and communicate with devices on the EtherNet/IP network.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um004_-en-p.pdf

- *Kinetix 5700 Servo Drives User Manual*, publication 2198-UM002—Describes how to use Kinetix 5700 drive system with associated power supplies, single-axis inverters, dual-axis inverters, and accessory modules in a Logix 5000 control system.
  https://literature.rockwellautomation.com/idc/groups/literature/documents/um/2198-um002_-en-p.pdf

IACS Security Policy Considerations

In traditional IACS applications, much of the data remained in isolated systems not connected to other networks, which made understanding the threat landscape for IACS networks straightforward as most threats were local. As a result, many IACS networks and assets were designed and built before any industrial security threats surfaced, therefore industrial communication protocols did not have any security mechanisms.

With technological advances in IIoT and increased accessibility through converged IACS network infrastructure, data that was once kept in isolation is now readily available to management to help determine inefficiencies and aid in decision-making. IIoT helps offer the promise of business benefits by using innovative technology such as mobility, collaboration, analytics, and cloud-based services. It represents a gateway to digital transformation that connects plant-level or site-level and enterprise networks and securely connects people, processes, and technologies by adding analytics capabilities to IACS assets on the plant floor. More connected operations can create more potential entrance points for industrial security threats. These threats can come in many forms—physical or digital, internal or external, malicious or unintentional.

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. A balanced security framework must address both technical (technology) and non-technical (policies and procedures) elements. The degree of hardening depends upon the required security stance. Business practices, corporate standards, security policies, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are key factors in determining the appropriate security stance.

Understanding the security threats, risks, and vulnerabilities of a system is the starting point for any security policy implementation. The following security terminology is used in this publication:

- **Asset**—What we are trying to help protect. It can include property, people, information, and data that has value to an organization.

- **Threat**—What we are trying to help protect our asset from. Threats are potential events where anything might exploit a vulnerability to breach security and therefore cause possible harm.

- **Vulnerability**—A weakness or gap in a device, software, or security program that can be exploited by threats to gain unauthorized access to an asset.

- **Risk**—Risks are the potential effects of events, which are caused by threats.

- **Policies, procedures, and awareness**—A plan of action around procedures and education to help protect company assets (risk management) and provide rules for controlling human interactions in IACS systems.

IACS Threat Model Overview

Threats are undesirable events where anything might exploit a vulnerability to cause negative impacts on the operation or availability of equipment. Understanding threats to the IACS helps identify the appropriate countermeasures to mitigate them.

To better understand IACS threats, employ threat modeling, which is a preliminary step in a risk assessment to determine what the threats might be. A threat model identifies objectives and vulnerabilities and then defines countermeasures to mitigate the effects of threats to the system. Some considerations of threat modeling include addressing the following questions:

- What critical assets are in the IACS environment?

- What is the potential impact if something were to happen to one of those assets?

- What is the possible threat?

- What is a current threat in your IACS environment?

    - How difficult would it be to exploit?

    - Would it require a low level or high level of skill?

The threats today present themselves in many forms:

- **External**—Hackers seeking political or financial gain. A manufacturer's intellectual property can be a lucrative target for hackers. They might want to disrupt an industrial operation for financial, competitive, or political reasons. It is important to acknowledge even organizations not in the critical infrastructure sector or not targets of financial or political attacks can experience collateral damage from external threats. A well-known example is the NotPetya malware, a cyberattack masquerading as ransomware that affected thousands of computers worldwide in 2016 and 2017.

- **Internal**—Disgruntled employees. This category includes current and former employees, contractors, and third-party integrators. All these entities are familiar with a control system and industrial network of an organization and can present security and safety threats. In 2009, a contracted security guard managed to install malicious code in the HVAC control system causing damage to pharmaceutical storage at a medical facility.

- **Human error or accidental**—Employee errors. One of the most common security risks comes from innocent mistakes. This could include employees or contractors who unwittingly make a network misconnection, download the wrong program to a controller, or plug an infected device into the system. At a nuclear power plant, an engineer updated software on a computer and after the update the computer rebooted. The reboot also reset the data on the control system causing safety systems to interpret the data as a drop in coolant water reservoirs, initiating a plant shutdown.

At a minimum, the threat model approach should include the following information:

- Asset Management (Table 2-4)

    - Detailed inventory of existing devices and software, including firmware revisions

- Data Flows (Table 2-5)

- – Detailed observation and documentation of intended system functions and operation
- – Detailed observation and documentation of required data flows between devices
- – Detailed observation and documentation of required access to devices
- Identified Threats and Countermeasures (Table 2-6)
  - – Detailed observation and documentation of potential threats and countermeasures

The CPwE logical model employs commonly used industry standards such as the Purdue Model and ISA95 to organize the functions within industrial operations into Levels, and then organizes the Levels into Security Zones based on ISA/IEC 62443, as shown in Figure 2-1.

Figure 2-1   CPwE Logical Zoning Based on Purdue Model and ISE/IEC 62443
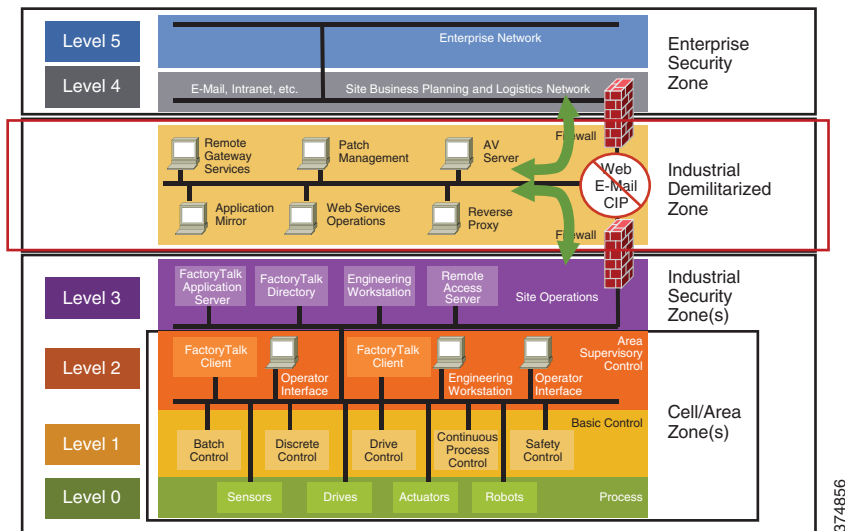
IACS Asset Management

Identifying new IACS assets (Table 2-4) that have been deployed or retired IACS assets that have been decommissioned provides the visibility needed to protect them and helps prioritize security efforts.

Table 2-4   Identification and Management of IACS Assets

Asset Data	Description
Asset management	- Asset Discovery - Maintaining an accurate up-to-date asset inventory - Tracking changes to assets over time

Table 2-4   Identification and Management of IACS Assets (continued)

Asset inventory information	• Manufacturer/Vendor • Current firmware version • Latest patches • Current configuration • Serial number • MAC address • IP address
Tools to help identify and manage IACS assets	• FactoryTalk AssetCentre software • FactoryTalk Network Manager software • FactoryTalk Linx Browser utility

Once an IACS asset inventory has been procured, prioritize the assets:

- Determine each IACS asset's relative value:
  - How much revenue/profit does it generate?
  - What is the cost to replace it?
  - How difficult would it be to replace?
  - How quickly can it be replaced?
- Define the type of protection for each IACS asset—confidentiality, integrity, or availability. Since IACS devices are grouped in zones with a common security requirement, this will help in selecting IACS devices and countermeasures to be used within zones.

FactoryTalk AssetCentre

Secure, manage, version, track, and report IACS asset information for IACS with FactoryTalk AssetCentre software (Figure 2-2). The FactoryTalk AssetCentre server centrally tracks and manages configuration changes and restricts who can make changes. This server functionality assists with diagnostics and troubleshooting and reduces maintenance time for IACS assets. An accurate and current asset inventory documentation enables better ongoing management of IACS devices. It can also support backup and recovery in case there is a need to restore IACS devices.

Figure 2-2   FactoryTalk AssetCentre
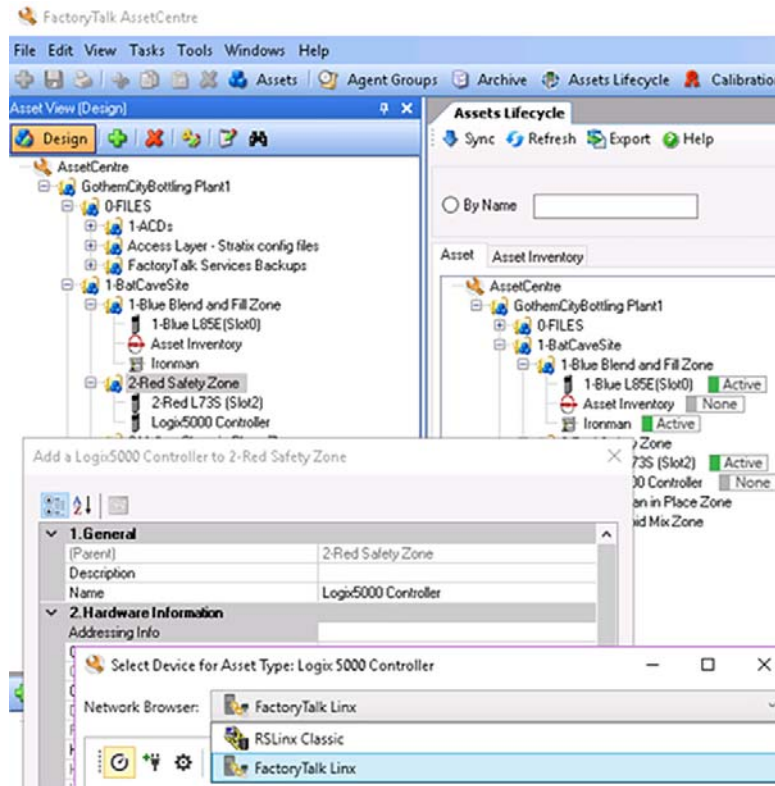
FactoryTalk Network Manager

FactoryTalk Network Manager (FTNM) software is a network management tool (Figure 2-3). It is designed to help operation teams gain full visibility of network devices and IACS assets in the context of industrial operations and provides improved architecture availability and performance, leading to increased overall equipment effectiveness (OEE). It provides the capabilities to view the network topology and manage switch-level alarms as they happen for more improved decision-making.

Figure 2-3   FactoryTalk Network Manager
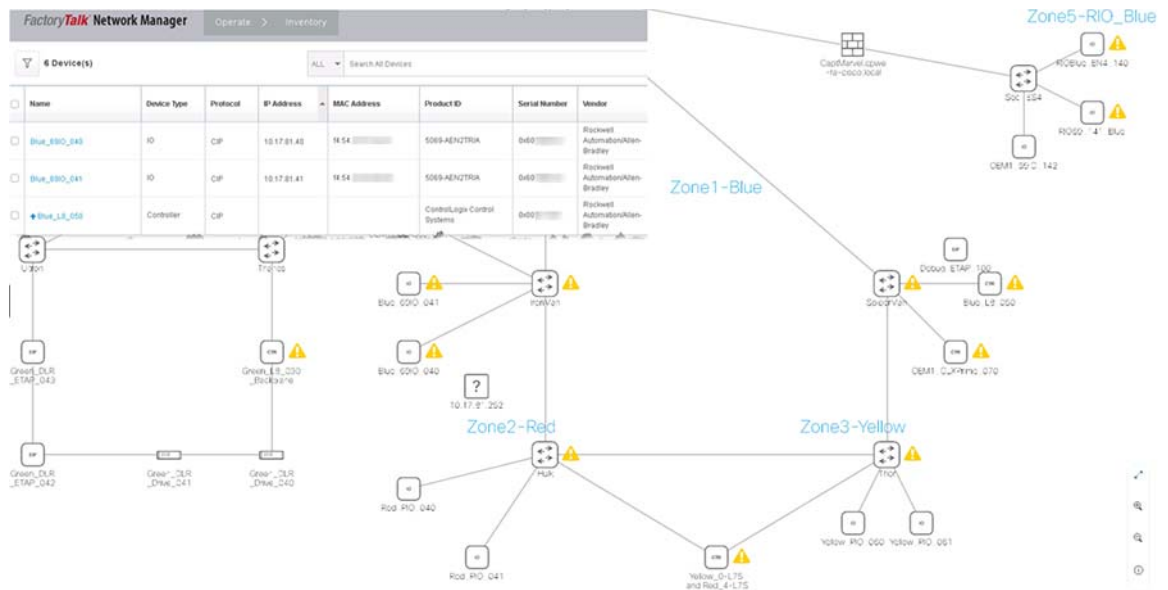
FactoryTalk Linx Browser

The FactoryTalk Linx Browser utility (Figure 2-4) can be used to view whether CIP Security has been enabled or disabled.

- When a node has a shield icon in front of it, that node supports the CIP Security feature.

- When a node does not have a shield icon in front of it, that node does not support the CIP Security feature.

- When the shield icon is gray, the CIP Security feature is disabled (the default).

- When the shield icon is green, the CIP Security feature has been enabled using the FactoryTalk Policy Manager software.

- When the shield icon is yellow, the CIP Security feature is in the process of applying the configuration pushed down by the FactoryTalk Policy Manager software.

The FactoryTalk Linx browser provides a simple user interface to view and navigate an IACS topology and access IACS device properties. This tool provides a standalone version of the network browser component that is shared by other Rockwell Automation software. This browser will share the FactoryTalk Linx drivers that are configured in the FactoryTalk Administration Console. The FactoryTalk Administration Console permits control system engineers with the ability to add and configure new drivers that can also be used by the Console.

Figure 2-4   FactoryTalk Linx Browser Utility
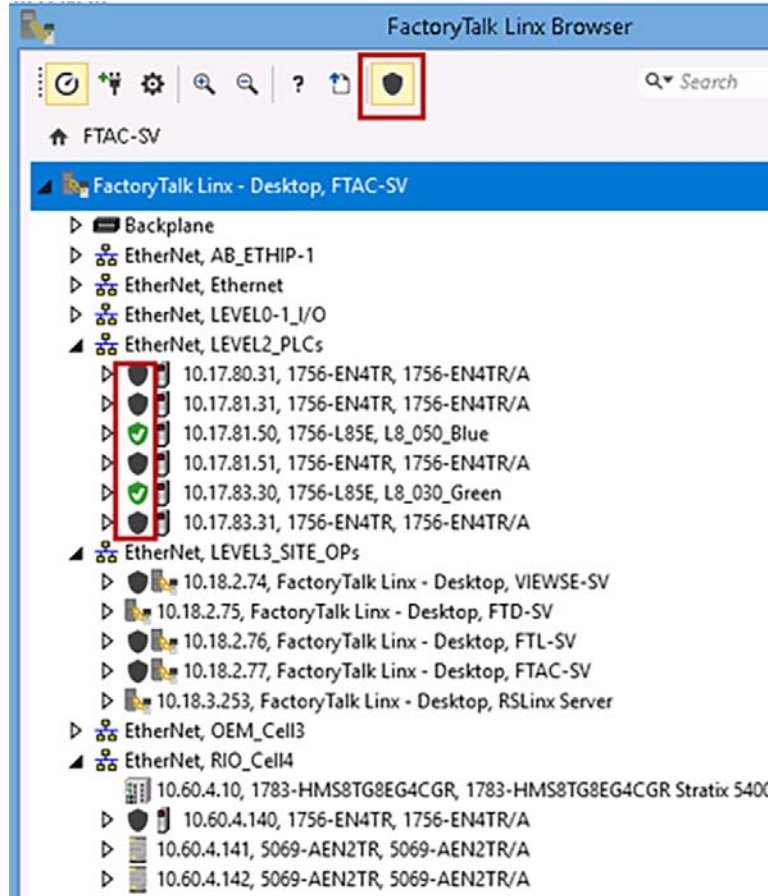
Note   CIP Security IACS devices must be discoverable by FactoryTalk Linx to apply and deploy CIP Security properties. FactoryTalk Linx Browser utility cannot be used to enable/disable the CIP Security properties for products. Use the FactoryTalk Policy Manager software to modify or to enable/disable CIP Security properties on products.

IACS Data Flows

IACS is fed by various upstream and downstream connections that keep it running and provide real-time data to keep systems safe. These north-south traffic flows are typically protected with firewalls securing the network perimeter, however defending the perimeter alone is not enough to help prevent a lateral move. CIP Security properties can assist the industrial security landscape move towards a zero-trust security model by shifting the security perimeter closer the data, limiting the impact of a breach. To successfully apply this concept, it is crucial to understand interactions between IACS devices and manage internal and external data flows. A proper assessment plan should begin with identifying all connections and reviewing the level of risk that they may pose to an IACS (Table 2-5).

- Examine the IACS assets in their information systems and identify information flows that affect the assets.

- Characterize systems and software that are part of the information flow.

- Any connections that pose an unnecessary risk should be reviewed for necessity.

Security is a balance; not every CIP-connected device requires the same level of security, Identify the data with the most critical value. Typically, this is where the most effort to secure data will need to be applied. Also consider there are other industry security standards and regulatory compliance that may be involved, which may be beyond what the organization perceives as the value of any data.

For a successful deployment of CIP Security:

- Validate that all processes or programs are running as expected without CIP Security enabled.

- Identify the types of CIP traffic and data flow that maps to each IACS device or process to the initiator and responder of a CIP connection. Understanding which IACS device initiates a connection and which IACS device accepts the connection will help define conduits for protecting EtherNet/IP communication in different zones. Any EtherNet/IP communication between zones must be through a defined conduit.

Table 2-5   Characterize Assets, Data Flows, and Access Control

Data connections/Access control	Description
IACS data connections	- Public Internet - VPN connections - Server connections - HMI systems - Peer-to-Peer connections - I/O connections - Traffic types: unicast, multicast, broadcast
Access control information	- How are the assets accessed? - Who can copy, move, or modify assets? - What methods can be used to interact with assets? - Do they exit in multiple locations? - What protocols and ports are used to access what applications?
Tools to help identify and document	- Wireshark - IACS device webpage - Microsoft® Visio software - Microsoft Excel® software

Wireshark is a widely-used network protocol analyzer. It is a free and open-source packet analyzer commonly used for network troubleshooting, protocol analysis, software and communications protocol development, and education. The purpose of traffic analysis is to determine who is talking to whom (Figure 2-5).

Figure 2-5   Wireshark Tool

Many IACS devices have a webpage that displays information about the module including the CIP connections established. This is a quick way to determine who is talking to whom. In Figure 2-6 the 1756-EN4TR module with IP Address 10.17.81.51 has ESTABLISHED TCP connections on port 44818 for several IACS devices including 10.17.81.40 and 10.17.81.41 shown in the Wireshark screen capture in Figure 2-5.

Figure 2-6   1756-EN4TR Webpage (TCP Connections page)

Figure 2-7 illustrates common EtherNet/IP communications in an IACS using the CPwE Model:

- **Level 3-Site Operations** will typically see CIP class 3 HMI communications to and from IACS devices up to the plant or site-wide FactoryTalk server.

- **Level 2-Supervisory Control** contains the local management software where engineering workstations (EWS) use CIP class 3 administration communications for uploading/downloading projects to the controllers.

- **Level 1-Control System** containing the controllers instructing the Level 0 IACS devices and gathering data about a particular process. The following types of traffic can occur at this level includes a combination of CIP class 1 (I/O) and CIP class 3 types of traffic:

    – Controllers using CIP class 1 peer-to-peer produced and consumed tags with each other.

    – Controllers using CIP class 3 messaging for HMI data as well as peer-to-peer MSG instructions.

- **Level 0-Process** containing the sensors, actuators, drives, and robots performing the functions of the process. The following types of traffic that can occur at this level includes:

    – Controllers using CIP class 1 I/O connections with I/O and device IACS devices.

    – Controllers using CIP class 3 MSG instructions to exchange data or configure IACS devices.

Note   For details on EtherNet/IP communications, see EtherNet/IP Overview.

Figure 2-7   Topology of CIP Connections
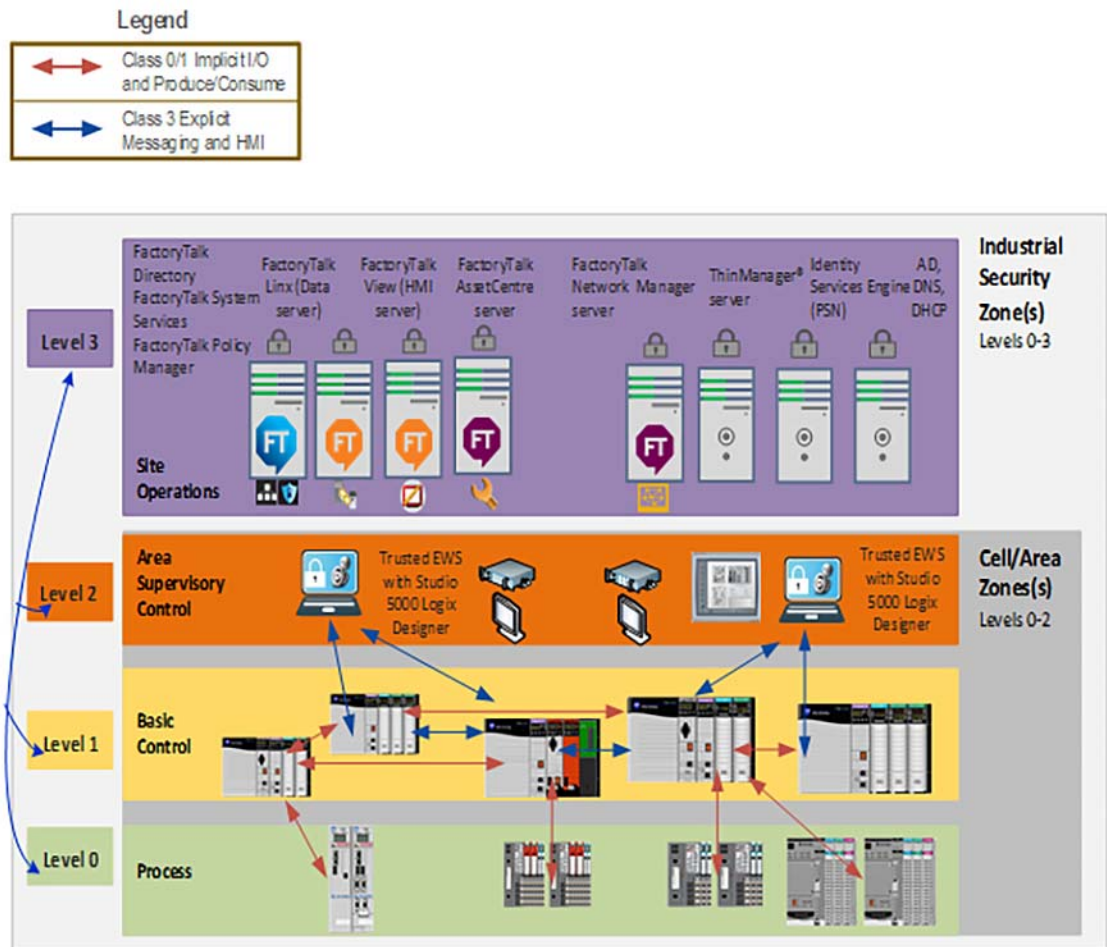
IACS Threats and Countermeasures

For each asset, identify how and where to enforce the policy that governs the asset. Based on the type of protections for the asset, examine the information flows, systems characterizations, and enforcement mechanisms. Identify potential threats (such as threats to confidentiality, threats to integrity, and threats to availability). A common system used for categorization of threats is the Microsoft-developed **STRIDE** model (Table 2-6).

- **S**poofing of user identify
- **T**ampering
- **R**epudiation
- **I**nformation disclosure (privacy breach or data leak)
- **D**enial of Service (DoS)
- **E**levation of privilege

Table 2-6   Identify Threats and Countermeasures

Threat	Example	Countermeasure
Spoofing identity	A smart sensor could be spoofed to send incorrect data	Device authentication
Tampering with data	Data in transit could be intercepted and altered	Message integrity
Repudiation	The ability of having no proof of an entity performing an action to a system	Non-repudiation using digital signature
Information disclosure	Unauthorized viewing of information	Message confidentiality using encryption
Denial of service	Rendering a device unusable	Availability
Elevation of privilege	Unprivileged entity gains privilege access to compromise system	Authorization

Next, create a network diagram and overlay information, asset locations, data flows, enforcement points, and vulnerability (Figure 2-8). Tools like Microsoft Visio, Excel, or ThreatModeling can be used to create the diagram. Another helpful tool to identify threats is the Common Vulnerabilities and Exposures (CVE). The CVE is a program launched in 1999 by MITRE, a nonprofit that operates research and development centers sponsored by the federal government to identify and catalog vulnerabilities in software or firmware into a free list for organizations to improve their security. For more information, see:
https://cve.mitre.org/

Figure 2-8   Network Overlay of Vulnerability and Countermeasure Enforcement Points
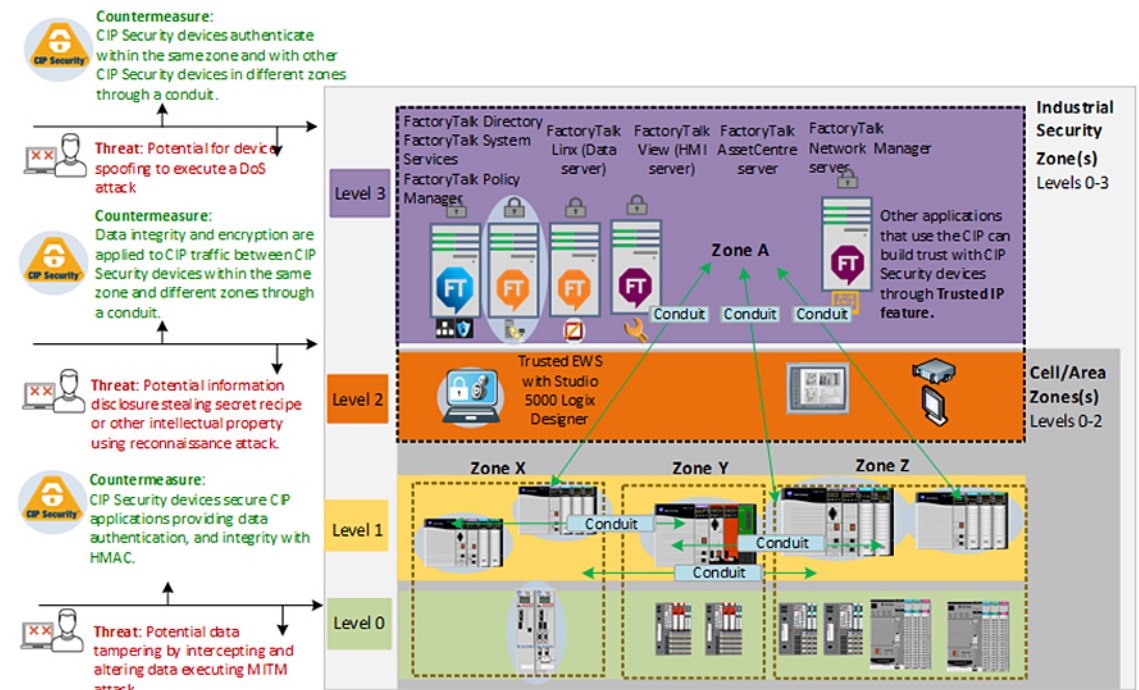
Note   Rockwell Automation IACS devices supporting CIP Security include the following:

- 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 supports CIP Security listed above see Table 2-3.

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

Alignment with ISA/IEC 62443

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in IACS networks. 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.

This section is an overview of the ISA/IEC 62443-3-2 and 3-3 groups in the series which deal with System Security Requirements and Security Levels (SL) (Figure 2-9).

- **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. The principle audience include suppliers of industrial automation and control systems, system integrators, and asset owners.

Figure 2-9   ISA/IEC 62443 Series of IACS Standards

ISA/IEC 62443-3-2 Overview

Zones and Conduits

The CIP Security architecture is based on logical segmentation with zone and conduits following the ISA/IEC 62443-3-2 Zones and Conduits model.

- **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 a 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.

Risk Assessment

As part of the ISA/IEC 62443-3-2, the security risk assessment process can be used to assign security levels to zones and conduits. An assessment provides a picture of the organization's current security posture (current risk state) and what mitigation techniques are needed to get to a preferred state or acceptable risk state. It is recommended to form a multi-discipline team of operations, engineering, IT, and safety representatives to collaborate in the development and deployment of your industrial security policy. Proactively controlling interactions between IACS devices and managing internal and external data flows will help reduce security risks.

Key deliverables for a security assessment include:

- Inventory of authorized and unauthorized devices and software
- Detailed observation and documentation of system performance
- Identification of tolerance thresholds and risk/vulnerability indications

- Prioritization of each vulnerability based on impact and exploitation potential

- Mitigation techniques required to bring an operation to an acceptable risk state

Government entities including the U.S. Department of Homeland Security (DHS) and the U.S. Department of Commerce/National Institute of Standards and Technology (NIST) also reference ISA/IEC 62443 to help with recommendations for conducting security risk assessments. Figure 2-10 shows examples of security risk assessments from DHS.

Figure 2-10   Security Risk Assessment

Base metrics	Risk - Metric value	Metric description
Confidentiality impact	1 - None	There is no impact to the confidentiality of the system.
	2 - Partial	There is considerable information disclosure.
	3 - Complete	There is total information disclosure, resulting in all systems files being revealed.
Integrity impact	1 - None	There is no impact to the integrity of the system.
	2 - Partial	Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.
	3 - Complete	There is a total compromise of system integrity. Complete loss of system protection, resulting in the entire system being compromised.
Availability impact	1 - None	There is no impact to the availability of the system.
	2 - Partial	There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to the Internet.
	3 - Complete	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

Base metrics	Risk - Metric value	Metric description
Access vector	1 - Local	Requires the attacker to have either physical access to the vulnerable system or local account.
	2 - Adjacent network	Requires the attacker to have access to either the broadcast or collision domain of the vulnerable software, for example the local IP subnet.
	3 - Network	The vulnerable software is bound to the network stack and the attacker does not require local network access or local access, for example, remotely exploitable.
Access complexity	1 - High	Specialized access conditions exist.
	2 - Meduim	The access conditions are somewhat specialized.
	3 - Low	Specialized access conditions or extenuating circumstances do not exist.
Authentication	1 - Multiple	Exploting the vulnerability requires an attacker to authenticate two or more times.
	2 - Single	The vulnerability requires an attacker to be logged into the system, for example, command line or desktop sesssion.
	3 - None	Authentication is not required to exploit the vulnerability.

For additional guidance on methods and approach for risk and vulnerability assessments see:

- Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide Department of Homeland Security (DHS):
  https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf

- NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security:
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Security Levels

Designing security into an IACS and establishing repeatable standards across multiple plant-wide or site-wide IACS is a long-term goal. When it comes to new designs (greenfield) or redesigns (brownfield) security lifecycle can be used to streamline the process to achieve this goal. The security lifecycle can be categorized into the following three levels:

- **Achieved Security Level (SL-A)**—The actual level of security for an IACS zone.

- **Target Security Level (SL-T)**—The desired level of security for an IACS zone.

- **Capability Security Level (SL-C)**—The level where a particular IACS zone or component is capable of meeting the security level (SL) rating without additional compensating controls when properly configured and integrated.

With all the necessary assessments completed, develop the SL-T for an IACS zone. During the designing of the IACS zone, select components with the capabilities (SL-C) to meet the requirements of the SL-T. Once the IACS zone is operational, the actual security level can be considered as SL-A. The SL-A can potentially be higher if implemented correctly or lower if implemented incorrectly.

Security levels (SLs) represent a method of defining the level of capabilities to address security for a zone or conduit. It is analogous to the concept of Safety Integrity Levels (SILs) for a safety system. SIL is the measure of the safety of a given process. It provides a way to rate the confidence with which a system can be expected to perform its safety function under normal operation. Though it can yield a similar quantitative result, SLs need to be viewed in their own applicable context. SLs (Table 2-7) are based on combinations of likelihood of a threat event occurrence and an estimated adverse impact on industrial operations. SLs can be used to determine the required level of security for zones and conduits.

Table 2-7   Security Levels

Security Level	Description	Example
SL 1	Low security measures implemented for protection against casual or coincidental access by unauthorized entities	• Misconfiguration via current employee or vendor • Unintentional or accidental
SL 2	Moderate security measures implemented for protection against intentional unauthorized access by entities with simple means with low resources, generic skills, and low motivation	• Misconfiguration via third-party or low-level hacker with basic knowledge of system • Intentional
SL 3	High security measures implemented for protection against intentional unauthorized access by entities using moderate resources, IACS specific skills and moderate motivation	• Damage via high-level hacker • Intentional and industry specific
SL 4	Highest security measures implemented for protection against intentional unauthorized access by entities using sophisticated means with extended resources, IACS specific skills and high motivation	• Economic damage via high-level hacker with means and motive • Aggressive and industry specific

SL concepts can be used to select the IACS devices and countermeasures to be used within a zone and provide the ability to categorize risks for zone or conduits. The Component Requirements (CR) describe the requirements that must be met by secured industrial components. With CR, IACS devices can be assigned a SL value based on its security capabilities. If certain legacy IACS devices do not satisfy a specific CR of the overall zone or System Requirement (SR), then additional security measures should be taken as described in the defense-in-depth concept.

ISA/IEC 62443-3-3 Overview

Foundational Requirements (FRs)

SLs are based on the seven Foundational Requirements (FRs) for security. FRs are accepted security practices interpreted to fit safely and effectively into a control system design, applying a secure development lifecycle process. These fundamental concepts are carefully adapted to address the unique circumstances of security in control systems such as:

- Risks of economic loss

- Environmental damage to personnel injury and death

- Continuous compliance with the physics associated with distributed control of physical objects

- Processes such as casualties of effects of cyber and physical events occurring in physical processes.

The ISA/IEC 62443-3-3 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. FRs include a series of Security Requirements (SRs) describing a number of layered security mechanisms as a baseline. To achieve a specific SL-A value, a system may be required to demonstrate expected outcomes for specific SRs in their respective FRs.

Below are examples of positioning security mechanisms within an IACS network. It includes network segmentation (zones and conduits), technologies like CIP Security, and other management software to be used as building blocks to help bring organizations closer to the desired security level.

FR1: Identification and authentication control (IAC) basic security requires the capability of identifying and authenticating all users (humans, software processes, and devices) before allowing them to access to the IACS system.

- FactoryTalk Security polices and its integration with Microsoft® Active Directory technology can be used to provide centralized management of human access control to the FactoryTalk software utilizing password-based authentication.

  - The expected outcome is the ability to manage human user access to Studio 5000 Logix Designer, the configuration tool used for configuring ControlLogix 5580 IACS devices within the IACS network.

- The CIP Security device identity and authentication property utilize a commonly accepted Public Key Infrastructure (PKI) to distribute digital certificates to help ensure that only trusted EWS with Studio 5000 Logix Designer can access and program trusted IACS controllers within the IACS network.

  - The expected outcome is the ability to enforce only trusted controllers can access and communicate with other trusted IACS devices within the IACS network.

FR4: Data confidentiality (DC) basic security requires the capability to achieve the confidentiality of information on communication channels and in data repositories to help prevent unauthorized disclosure whether at rest or in transit.

- The CIP Security data confidentiality (encryption) property uses proven secure encrypted protocols TLS/DTLS and cipher suites Advanced Encryption System (AES) and Secure Hash Standard (SHA).
  - The expected outcome is to help achieve protection against eavesdropping and unauthorized access of data in transit within the IACS network.

FR5: Restrict data flow (RDF) basic security requires the capability to segment the control system via zones and conduits to limit the unnecessary flow of data.

- An EtherNet/IP network provides many methods for network segmentation.
  - The expected outcome is to have a physical and logical segmentation of IACS networks from non-IACS networks.

- Implement an Industrial Demilitarized Zone (IDMZ) for network segmentation between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone) with redundant high availability security appliances or firewalls as device conduits enforcing data security policies between zones.
  - The expected outcome is to securely allow sharing of IACS data and network services between the two zones without any direct connections to a trusted network (Industrial Zone).

- VLANs, Access Control Lists (ACLs) and Industrial Firewalls (IFWs) provide additional layers of security to help restrict traffic between zones. Managed Stratix IES have the capability of logging and/or sending syslogs to a Security Information and Event Management (SIEM) software.
  - The expected outcome with additional layers of security mechanisms for traffic restrictions is the ability to have multiple opportunities to thwart efforts to pivot in the Industrial Zone while getting real-time alerts when violations occur.

- CIP Security provides segmentation and conduits enforced at the IACS application or device.
  - The expected outcome is the ability to create network micro-segmentation, which is a more granular approach helping prevent lateral movement in the network. The ability to proactively control interactions between IACS devices and manage internal and external data flows will help reduce security risks to acceptable level.

Technology Considerations

EtherNet/IP Overview

Understanding EtherNet/IP is imperative for a successful CIP Security deployment. One crucial factor before deploying CIP Security in the IACS network is first validating that all processes and programs are running as expected without any CIP Security enabled. Next identify the types of IACS traffic and data flow that maps to each IACS device or process to the initiator and responder of a CIP connection will aid in creating appropriate conduits.

Note   CIP Security is the ODVA, Inc. secure extension of CIP. Its security properties cannot be extended to secure communications for other industrial protocols or common Internet protocols.

EtherNet/IP (Figure 2-11) is a multi-discipline, control and information platform for use in industrial environments and time-critical applications. The EtherNet/IP network uses standard Ethernet and TCP/IP technologies and an open, application-layer protocol called the Common Industrial Protocol (CIP).

The open, application-layer protocol makes interoperability and interchangeability of industrial automation and control devices on the EtherNet/IP network a reality for real-time control applications.

EtherNet/IP adheres to the following standards:

*   IEEE 802.3—Standard Ethernet, Precision Time Protocol (IEEE-1588)

*   IETF—Internet Engineering Task Force, standard Internet Protocol (IP)

*   IEC—International Electrotechnical Commission

*   ODVA, Inc.—Global organization that manages the Common Industrial Protocol (CIP)

Figure 2-11   OSI Model for EtherNet/IP
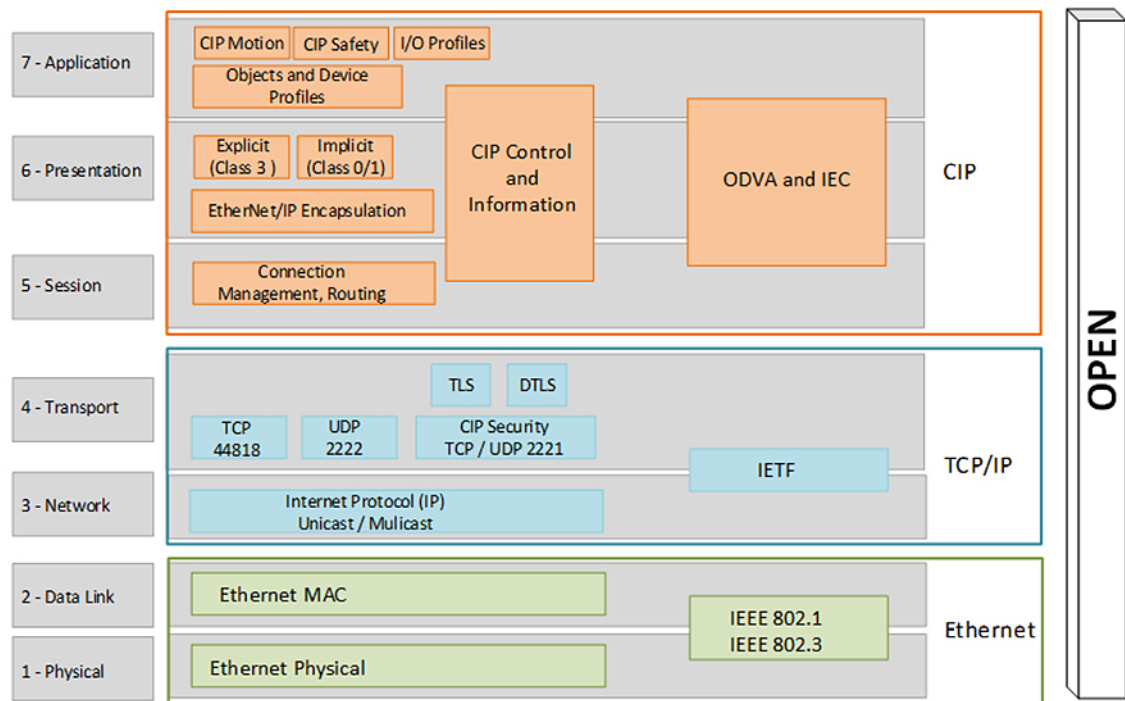
CIP is a message-based, application-layer protocol. It implements a relative path to send a message from the producing IACS devices in a system to the consuming IACS devices. In a CIP connection, the client will initiate the TCP three-way handshake on port 44818 followed by the connection manager Forward_Open request to the server. The server will reply with a connection manager Success: Forward_Open back to the client.

CIP characterizes two forms of messaging: Explicit Message (Class 3) and Implicit Message (Class 1).

Explicit messaging is when a client IACS device initiates a CIP connection to exchange information with a server IACS device on a specific request (MSG instruction). It uses TCP/IP and requires that the memory location of the information to be sent is also defined in the instruction itself.

*   Explicit messages are not time critical and are typically used for data collection.

*   They are transferred across TCP/IP and are unscheduled.

*   They are unicast frames for one-to-one communications.

- Executing an MSG instruction, a program upload, and HMI communications are examples of explicit connection.

In implicit messaging or I/O connections, the I/O IACS device exchanges data and status with the controller either upon a change of state (COS) or at a requested packet interval (RPI). The RPI is the frequency of updates to the controller based on configuration and location of the input IACS device on the network. The I/O IACS device cannot start sending data until the controller requests for it. The I/O IACS device (server) waits until the controller (client) initiates the TCP connection. Once the TCP and Forward_Open connections have successfully completed, then the I/O IACS device can start sending data with the controller

- Implicit or I/O connections are considered time critical and are scheduled to be produced or consumed at a RPI.

- I/O connections from the producer to the consumer are typically sent as UDP unicast frames, while those sent from the target to the originator can be sent as UDP multicast or unicast frames.

The controller can also produce data for other controllers to consume. The produced and consumed data is accessible by multiple controllers either over the backplane or over the EtherNet/IP network. This data exchange conforms to the producer/consumer model.

For an I/O connection to successfully make a CIP connection, the client will initiate the TCP three-way handshake with the destination port 44818 followed by the connection manager Forward_Open request to the server.

Figure 2-12 is a Wireshark screen capture of initial connections with a client IACS scanner 1756-L8xE (10.17.81.51) and a server IACS adapter 5069-AEN2TR (10.17.81.40). Once the CIP connection is established then I/O data can flow using the UDP port 2222 (Figure 2-13).

Figure 2-12   TCP and CIP Connection

Figure 2-13   UDP I/O Connection

The client is a scanner IACS device 1756-L8xE (10.17.81.51) and the server is an adapter IACS device 5069-AEN2TR (10.17.81.40). First the client will initiate the TCP connection to the server using TCP port 44818. Typically, this is triggered when an I/O device is added to the I/O configuration of a controller.

1. **Client** -> Server: SYN

2. Client <- **Server**: SYN, ACK

3. **Client** -> Server: ACK

Once the TCP connection has been established, the client will initiate the CIP connection using TCP port 44818 to the server using Connection Manager.

4. **Client** -> Server: Forward_Open

5. Client <- **Server**: Success: Forward_Open

Once the CIP connection has been established, the client and the server will start exchanging data using UDP port 2222.

6. **Client** -> Server: CIP Data

7. Client <- **Server**: CIP I/O Data

TLS (RFC 5246) and DTLS (RFC 6347)

Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are both network protocols that allow client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Current TLS versions include TLS 1.1, 1.2 and 1.3. CIP Security implemented in Rockwell Automation IACS devices use TLS version 1.2 on TCP/UDP port of 2221. It uses the TLS/DTLS technology to "wrap" around the industrial traffic creating a secure tunnel allowing the EtherNet/IP traffic to flow through it. This allows for the applications like CIP Motion™ and CIP Safety to continue to work the same regardless of the security layer.

TLS is a proven open security standard already being used to minimize potential vulnerabilities in common applications including web browsers, instant messaging, email, and voice over IP in the Enterprise Security Zone. TLS provides three primary services that help ensure the safety and security of data exchanged:

- Authentication

- Encryption

- Integrity

DTLS is based on TLS, but is specifically used for UDP connections instead of TCP connections. Since DTLS is based on TLS, it can use a majority of the cipher suites described for TLS.

Two key protocols work together to provide connection security in the TLS operation (Figure 2-14):

1. The TLS handshake protocol is performed only once to establish a secure connection for both communicating parties. It establishes the following:

   a. Both will negotiate the secure communication's cipher suite (a cipher suite is the collection of cryptographic algorithms that will be used in subsequent phase below).

   b. The root certificate is presented as authentication as the trust anchor from which the whole chain of trust is derived.

   c. The negotiation of the shared (secret) session key is generated then encrypted and sent to the other communicating party for use by the TLS record protocol. The shared (secret) session key is based on the asymmetric public-private key pair from the certificate.

2. After the TLS handshake protocol is complete, the TLS record protocol begins. From this point, the TLS record protocol is responsible for getting the data from applications, fragmenting it to an appropriate size, applying the shared (secret) session key to secure and verify data integrity, then sends it to the network transport layer (TCP/UDP). Optionally, the application data exchange can also use the shared (secret) session key for symmetric encryption of the data. In symmetric encryption, the exact same key is used on both sides of a conversation for both encrypting and decrypting. An example of symmetric algorithm used for encryption is AES 128-bit encryption.

Figure 2-14   TLS Handshake and Record Layers

X.509 Certificate Authentication

X.509 is a key component in the TLS/DTLS protocol. In the X.509 certificate structure, a root certificate is used as the trust anchor from which the whole chain of trust is derived; therefore a trust anchor must be in the possession of the trusting party beforehand to make any further certificate path validation possible. Rockwell Automation IACS devices used a vendor certificate as a root certificate including the unique key pair installed in the IACS device at the time of manufacture to provide device authenticity based on the X.509 standard.

The IACS device vendor certificate is presented as the server certificate with the public key during the TLS handshake to provide IACS device authenticity to the root-level CA (FactoryTalk System Services) but is not used as a basis for trust while being configured with new trust anchors and client certificates. By default, CIP Security IACS devices are configured to trust any commissioning tool that connects to it and configures the security settings. This is called the Trust On First Use (TOFU) model. It is a security model in which a client needs to create a trust relationship with an unknown server. TOFU concept used by SSH programs, where the public key of the peer is not verified, or verified in an out-of-bound way.

Once security properties are configured in zones and conduits in the FactoryTalk Policy Manager commissioning tool and deployed, trust between IACS devices is limited to the new client certificates (digitally signed with the trusted CA's private key) that the tool has provisioned, and the vendor certificate becomes irrelevant.

It is recommended to secure the root-level CA for protection of the signing keys. If the root CA were to be exploited, the security breach would compromise all IACS devices configured within the FactoryTalk system. Here are some security best practices for securing CAs:

- Private key protection
  - Hardware Security Module (HSM) to help protect the Private Key of the CA. HSMs can either be network attached through a private network to the CA, commonly used in virtualized CAs, or can be directly attached to the CA.

- Physical and logical access to the CAs
  - Install in a physically secure environment, which will help protect the Root CA.
  - Access to the CAs should be limited only to the CA administrator of the PKI hierarchy.
  - It is recommended to disable remote access technologies to the CAs such as Remote Desktop Protocol (RDP).
  - Disable CD-ROM auto play and USB ports either in the BIOS or in the virtual machine settings.
  - Keep the CA disconnected to the Internet unless you are performing maintenance tasks.

- Auditing
  - Increase the amount of system logging to support audit requirements.

- CA retrieval should be documented and audited, generally referred to, as a chain of custody.
- Remove unnecessary software/system packages/local and network services.
  - It is recommended not to reuse the computer hosting the Network FactoryTalk Directory (FTD) and FactoryTalk System Services for other applications.

CIP Security Properties

CIP Security defines the concept of Security Profiles. A Security Profile is a set of well-defined capabilities to facilitate device interoperability and end user selection of devices with the appropriate security capability. This section details the key security properties in the EtherNet/IP Confidentiality Profile implemented to mitigate threats.

The EtherNet/IP Confidentiality Profile leverages the open security IETF-standard TLS (RFC 5246) and DTLS (RFC 6347) protocols to help provide the following CIP Security 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 ensure the data has not been tampered with or falsified while in transit with TLS Hash-based Message Authentication Code (HMAC).
- **Data confidentiality (encryption)**—Increase the overall IACS device security posture, message encryption can be enabled to avert unwanted data reading and disclosure.

In addition to CIP Security properties, Rockwell Automation IACS devices currently supporting CIP Security also include the following features:

- **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 port**—Rockwell Automation products that support CIP Security can enable or disable the unsecure HTTP port/protocol 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 based on IP address.
  - Retrofitting ControlLogix 5570-based applications with the latest CIP Security enabled 1756-EN4TR communication module to secure EtherNet/IP communications.

Note   Once CIP Security capable IACS devices are configured and deployed with security properties, RSLinx® Classic cannot browse and discover those IACS devices unless a Trusted IP conduit is configured and deployed. FactoryTalk Linx version 6.11 or higher supports CIP Security and must be used to browse, discover, and go online with IACS devices.

Device Identification and Authentication

IACS device spoofing can occur when a malicious device poses as a legitimate IACS device to send messages with the intent to disrupt operations, thus successfully executing a DoS attack. These types of attacks can render the IACS device inoperable. With the CIP Security device identification and authentication property, communicating entities must provide some information about themselves that is trustworthy and verifiable before data is exchanged.

The CIP Security device identification and authentication property is used to establish and build IACS device trust with the following methods:

- **Pre-Shared keys (PSK)** are used to provide identity based on keys shared in advance among the communicating parties. This represents a more manual method of authentication and typically implemented in small systems. Optionally, the previously shared keys between two parties can be used for encryption and decryption of data.

  Advantages:

  The PSK handshake does not require any certificate parsing and signature verification providing less performance impact on establishing connections, however, the throughput performance is roughly the same as using certificates. PSK can be used to obtain all three security properties: device identification and authentication, data integrity, authentication, and/or data confidentiality for IACS device within the same zone (intra-zone communication) security.

  Considerations to using PSK:

  PSK are generally considered less secure than a certificate just like in human-user passwords, VPN, and Wi-Fi authentications, it may be subject to brute-force and dictionary attacks to learn the PSK. Recovering a compromised PSK is difficult because there is no mechanism to notify IACS devices of a key compromise, except by pushing a new key pair to all IACS devices. An additional limitation with PSK is IACS devices can only ever have one PSK configured, as a result, any conduits required between zones (inter-zone communication) configured with pre-shared key can only use Trusted IP.

- **Certificates** are agreements between communicating parties and a common entity called a Certificate Authority (CA). The CA is a trusted entity that manages and issues security certificates to requesters to prove their identities and public keys that are used for secure communication in an IACS network. Mutual trust is established when communicating parties exchange certificates signed by a common CA. (Figure 2-15). Once the TLS handshake completes and CIP application data exchange begins, there are no public key or certificates involved only symmetric encryption of AES and HMAC with SHA.

  Advantages:

  Certificates can be used to obtain all three security properties: device identification and authentication, data integrity and authentication, and/or data confidentiality for IACS device within the same zone or different zones security. It provides a higher level of complexity in authentication as the key length may be larger than a PSK. The key length in encryption determines the feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. It scales well to larger systems and is easier to maintain as devices get introduced to the network.

  Considerations to using certificates:

  It is recommended to secure the root-level CA for protection of the signing keys. If the root CA were to be exploited, the security breach would compromise all IACS devices configured within the FactoryTalk system.

  FactoryTalk Policy Manager is the commissioning tool graphical user-interface (GUI) used to configure, deploy, and view the system communication security policies.

FactoryTalk System Services is the root-level CA. It is the service that signs and issues client certificates to give assurance for a communicating party's authenticity. It runs as a service in the background to help enable the deployment of CIP Security policies configured in the FactoryTalk Policy Manager commissioning tool.

Figure 2-15   Device Identification and Authentication (Client Certificate Example)
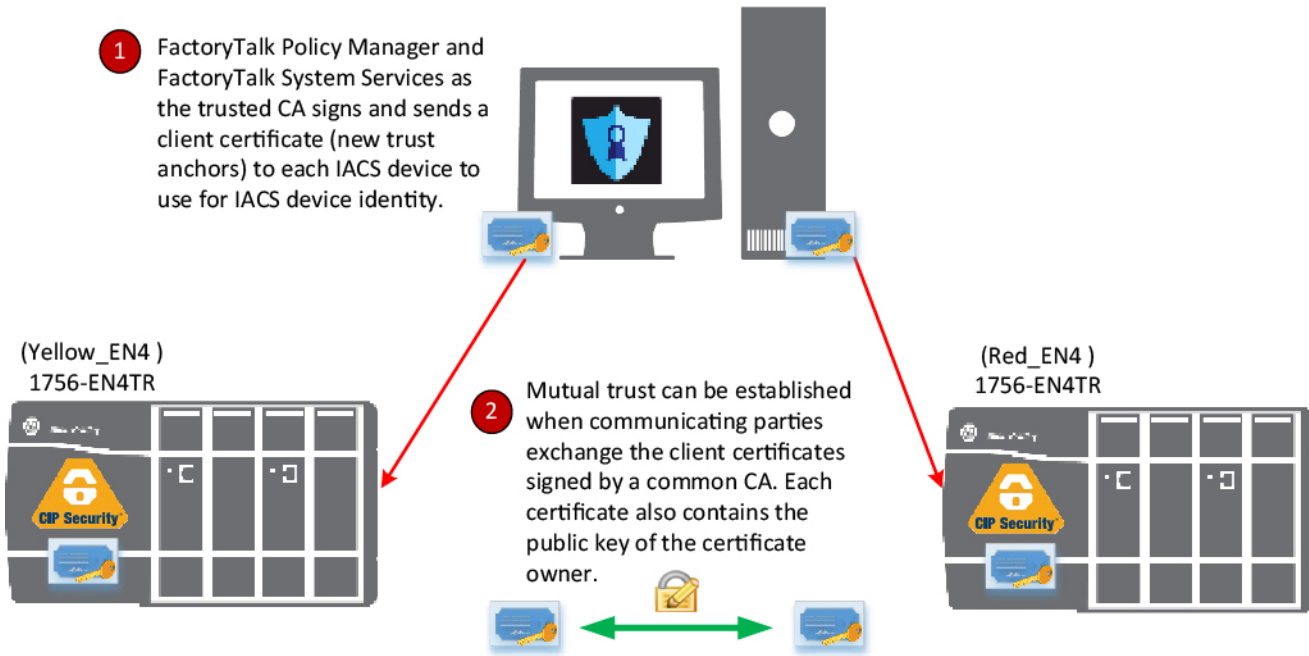
No.	Time	Source	Scr Port	Destination	Dst Port	Protocol	Info
22098	0.081277	Yellow_EN4	55812	Red_EN4	2221	DTLSv1.2	Client Hello
22099	0.053244	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Hello Verify Request
22100	0.000687	Yellow_EN4	55812	Red_EN4	2221	DTLSv1.2	Client Hello
22101	0.000666	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Server Hello
22102	0.000317	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Certificate
22103	0.059569	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Server Key Exchange
22104	0.000001	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Certificate Request
22105	0.000001	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Server Hello Done
22106	0.041588	Yellow_EN4	55812	Red_EN4	2221	DTLSv1.2	Certificate
22110	0.009022	Yellow_EN4	55812	Red_EN4	2221	DTLSv1.2	Client Key Exchange
22111	0.030941	Yellow_EN4	55812	Red_EN4	2221	DTLSv1.2	Certificate Verify
22112	0.000002	Yellow_EN4	55812	Red_EN4	2221	DTLSv1.2	Change Cipher Spec, Finished
22114	0.017726	Red_EN4	2221	Yellow_EN4	55812	DTLSv1.2	Change Cipher Spec, Finished
22118	0.105821	Yellow_EN4	55812	Red_EN4	2221	CIP CM	Connection Manager - Forward Open (Assembly)
22119	0.001047	Red_EN4	2221	Yellow_EN4	55812	CIP CM	Success: Connection Manager - Forward Open
22120	0.008652	Yellow_EN4	55812	Red_EN4	2221	CIP I/O	Connection: ID=0x00014109, SEQ=0000000000, O->T
22125	0.019674	Red_EN4	2221	Yellow_EN4	55812	CIP I/O	Connection: ID=0x002B4AE2, SEQ=0000000000, T->O
22131	0.016613	Yellow_EN4	55812	Red_EN4	2221	CIP CM	Connection Manager - Forward Open (I/O Map) ('Prod
22136	0.001378	Red_EN4	2221	Yellow_EN4	55812	CIP CM	Success: Connection Manager - Forward Open
22139	0.001665	Yellow_EN4	55812	Red_EN4	2221	CIP I/O	Connection: ID=0x0011410A, SEQ=0000000000, O->T
22140	0.002993	Red_EN4	2221	Yellow_EN4	55812	CIP I/O	Connection: ID=0x003B4AE6, SEQ=0000000000, T->O
22142	0.014559	Red_EN4	2221	Yellow_EN4	55812	CIP I/O	Connection: ID=0x003B4AE6, SEQ=0000000001, T->O

386015

Note   In the release of CIP Security, it is required to install FactoryTalk System Services and FactoryTalk Policy Manager software on the computer that hosts the FactoryTalk Network Directory.

For more details see: Additional Resources, page 2-3.

Data Integrity and Authentication

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 enables the sender's 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 (secret) session key to create a keyed hash or HMAC (keyed-Hash Message Authentication Code) to achieve 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 identical, it means that the message has not tampered with and the data is accepted. (Figure 2-16).

Figure 2-16   Data Integrity and Authentication (HMAC Example)
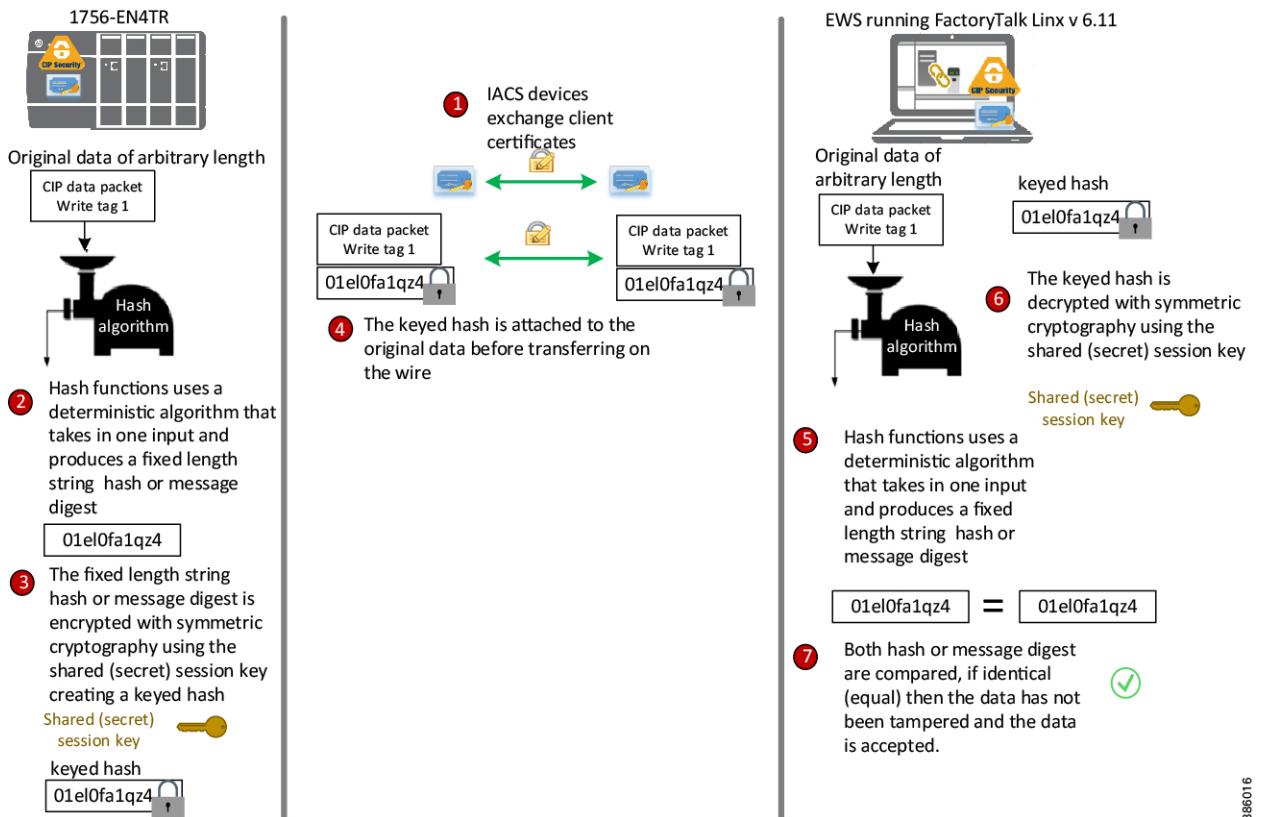
Note   CIP Security data integrity use cases are specific to data in transit and not data at rest. Once the CIP packet is on the wire is where CIP Security comes into play to help ensure data is not altered.

Data Confidentiality (Encryption)

Data sent over a wire can be intercepted allowing for sensitive information such as account credentials, secret recipes, or intellectual property to be stolen. CIP Security employs encryption to help reinforce confidentiality by helping to protect any sensitive or classified information from being stolen.

After the TLS handshake is complete and the session begins. The communicating IACS devices will use a shared (secret) session key to encrypt and decrypt the CIP application data sent to each other. The shared (secret) session key uses symmetric encryption, where the exact same key is used on both sides of a conversation, for both encrypting and decrypting. An example of symmetric algorithm used for encryption is Advanced Encryption System (AES) 128-bit encryption (Figure 2-17).

Advantages:

Encryption can be used to help reinforce confidentiality by helping to protect any sensitive or classified information from being read or stolen. The CIP Security confidentiality property uses symmetric encryption for the IACS application data exchange. This type of encryption is much less computationally intensive than asymmetric cryptography, which is only used for the TLS handshake or initial establishing of the connection.

Considerations to data confidentiality:

The data confidentiality security property is optional as data encryption will impact IACS device performance. Situations exist where a customer makes a reasonable design decision that allows for more risk acceptance to trade for better performance. For zones where network communication does not require the level of security for data encryption, for CIP Motion applications, and I/O connections; Rockwell Automation, Cisco, and Panduit recommend enabling only device and data authentication/integrity without encryption.

Note   CIP Motion application was not tested or validated as part of CPwE CIP Security. See the specific vendor IACS device technical specification or release notes publications for performance and capacity.

Figure 2-17   Data Confidentiality (Encryption)
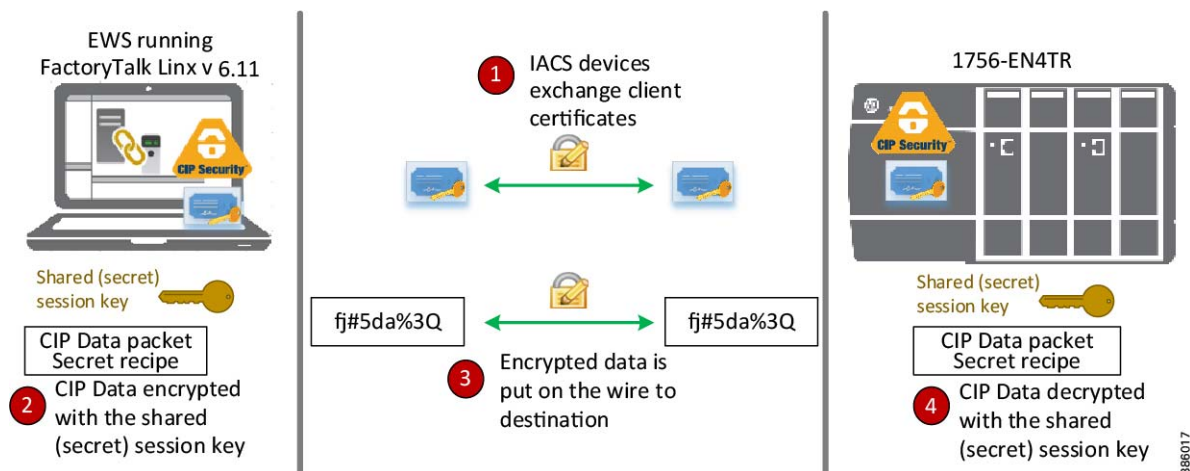
Note   Rockwell Automation devices and software currently supporting CIP Security can enable data confidentiality (encryption) as an optional policy.

Trusted IP Communication

Rockwell Automation devices and software currently supporting CIP Security are still able to interoperate with devices that do not support CIP Security on the same network by using the Trusted IP feature. The feature can be implemented to authorize CIP communication between an IACS device that is capable of CIP Security and one that is not based on IP address.

Advantages:

Trusted IP helps add control on access for legacy IACS and third-party CIP applications where standards and policies are needed for audit or compliance purposes.

Considerations of Trusted IP:

With Trusted IP conduits, there are no mechanisms for device or data identity and authentication or data encryption. Trusted IP feature is essentially a list of IP addresses for known trusted IACS devices or administrator approved CIP applications allowed to access and communicate with CIP Security capable IACS devices.

IACS devices currently supporting CIP Security are still able to interoperate with IACS devices that do not support CIP Security on the network through the standard TCP/UDP ports of 44818 and 2222 depending on which IACS device is initiating the CIP connection.

No additional configuration for a Trusted IP conduit is required in FactoryTalk Policy Manager to allow the EtherNet/IP communication, if the initiator of the CIP connection is from a CIP Security capable IACS device to one that is not or when the IACS devices are placed in the same zone.

A Trusted IP conduit configuration is required in FactoryTalk Policy Manager to allow EtherNet/IP communication between devices in different zones or if the initiator of the CIP connection is from an IACS device with no CIP Security capabilities to one that is capable.

In Figure 2-18, the FactoryTalk Network Manager software does not support CIP Security, however is able to initiate a CIP scan to discover the 1756-EN4TR, which does support CIP Security through the Trusted IP feature.

Figure 2-18   Trusted IP Feature
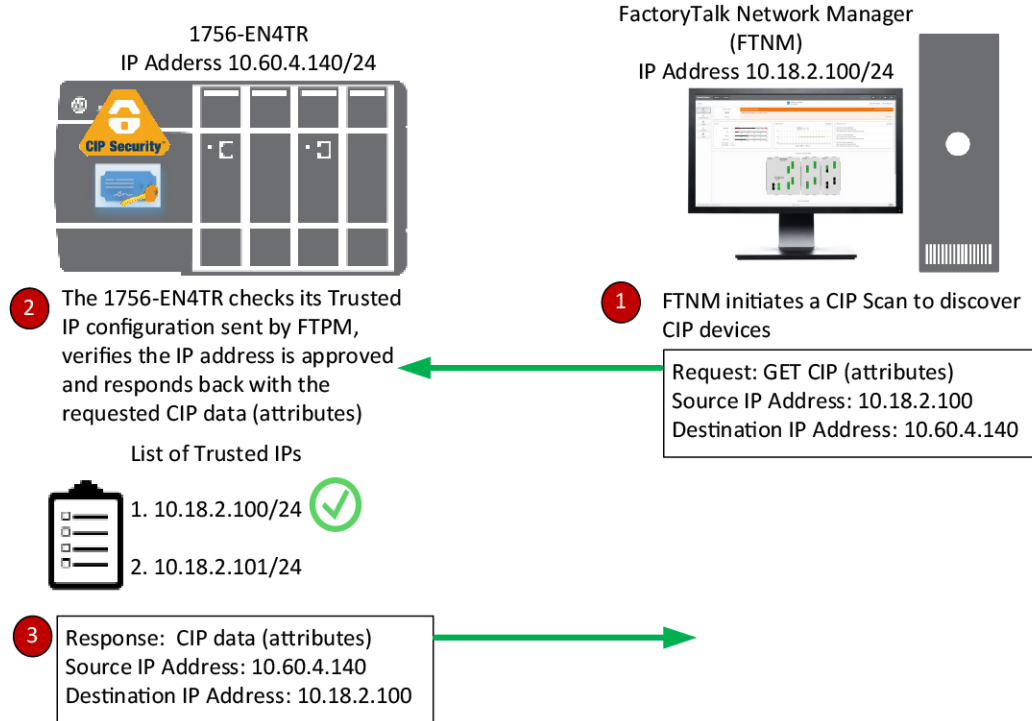
Note   In FactoryTalk Policy Manager, the authentication method of a Trusted IP can be defined on a conduit to allow authorized CIP connections between a CIP Security capable IACS device and one that is not.

CIP Security Limitations

The following are limitations and considerations of the solution from Rockwell Automation to implement CIP Security in an IACS:

- CIP Bridging
- ControlLogix Redundancy Systems (Multicast traffic)
- Network Address Translation (NAT)
- Automatic Device Replacement (ADR)
- RSLinx Classic Software

CIP Bridging

CIP Security cannot be configured or apply protection through a CIP bridge or controller backplane. In Figure 2-19, CIP Security can be applied to the 1756-EN4TR in slot 0, but cannot be applied to the 1756-EN4TR in slot 4 or to the IACS devices in the DLR off of the 1756-EN4TR in slot 4.

Optionally, ControlLogix has a feature called Trusted slot, which can be configured to maintain network segmentation on the local chassis. This feature is not part of CIP Security but native to ControlLogix and can be found on the controller Properties Security tab. The trusted slot feature restricts the communication paths through which certain operations are performed on Logix controllers.

Figure 2-19   CIP Bridging
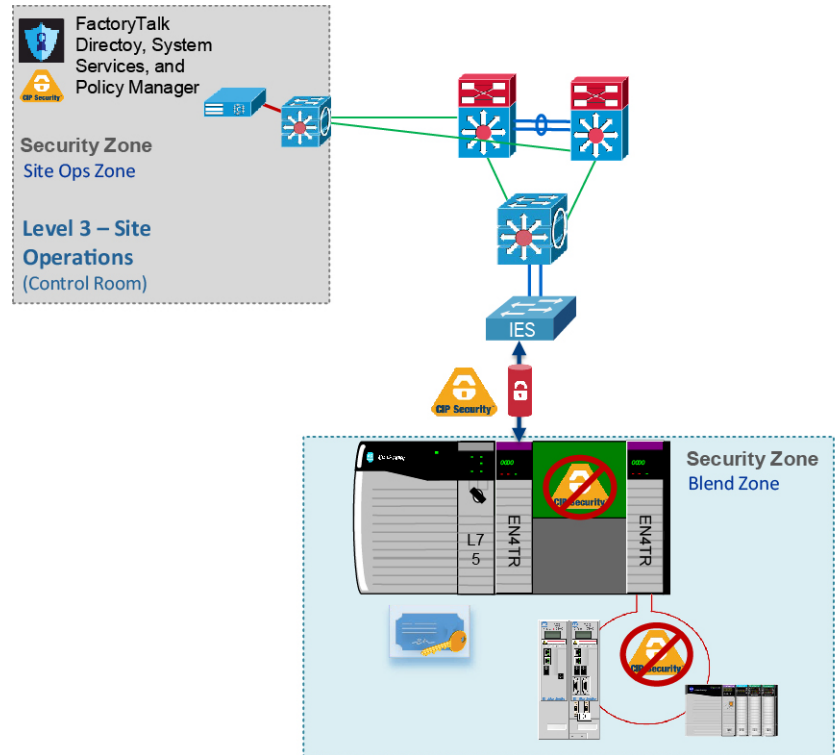
ControlLogix Redundancy Systems (Multicast traffic)

Currently, multicast connections with CIP Security are not supported. As a result, CIP Security cannot be used in a ControlLogix Enhanced Redundancy system or with any CIP multicast applications.

Network Address Translation (NAT)

Note   NAT was not tested or validated as part of CPwE CIP Security. Due to the general complexity of NAT configuration, maintenance, and management, careful consideration and testing is recommended before overlaying CIP Security in an architecture with NAT.

CIP Security is IP-based, meaning if an IACS device is reachable to the computer/server hosting FactoryTalk Policy Manager and FactoryTalk System Services by IP address, then CIP Security can be successfully deployed to that IACS device. Therefore, Network Address Translation (NAT) can be implemented with CIP Security only if the computer/server with FactoryTalk Policy Manager can access the CIP Security IACS device via an IP address.

Automatic Device Replacement (ADR)

The current workflow for an IACS device requiring ADR with CIP Security implementation is to physically replace the IACS device, apply ADR, then redeploy the CIP Security properties to the IACS device from FactoryTalk Policy Manager.

RSLinx Classic Software

RSLinx Classic software does not support CIP Security and cannot be used implement and deploy CIP Security properties to capable IACS devices. Once CIP Security capable IACS devices are configured and deployed with security properties, RSLinx Classic will not be able to browse and discover those IACS devices unless a Trusted IP conduit is configured and deployed. FactoryTalk Linx version 6.11 or higher supports CIP Security and must be used to browse, discover, and used to go online with IACS devices.

Architectural Considerations

Network Segmentation

Network 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. Applying the concepts of defense-in-depth, the Industrial Demilitarized Zone (IDMZ) is the first layer of defense for network segmentation enforcing data security policies between a trusted network (Industrial Zone) and an untrusted network (Enterprise Zone) with redundant high availability security appliances or firewalls. The IDMZ is the network perimeter that acts as a buffer to securely allow sharing of IACS data and network services between the two zones (Figure 2-20).

Figure 2-20   CPwE Plant-wide or Site-wide Zone (IDMZ)
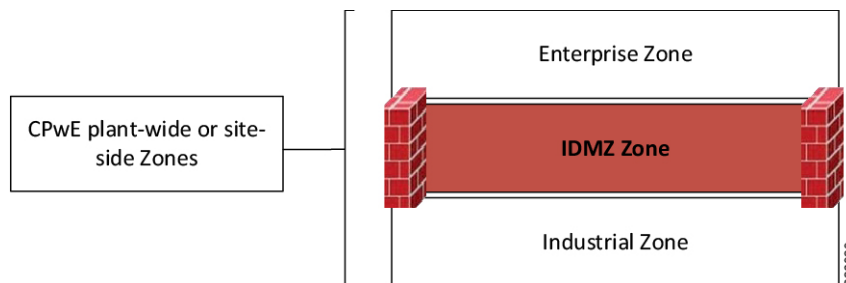
Note   Links to the *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* are provided for further details.

- 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

The second layer of defense is grouping IACS devices by VLANs/subnets with access control lists (ACLs). At a high level, subnets and VLANs are analogous in that they both segment the network. The main differentiator between the two are their functions within the communication stack referenced in the Open Systems Interconnection (OSI) model. VLANs are used at the data link layer with Layer 2 MAC addresses, while subnets are used at the network layer with Layer 3 IP addresses. Large IP networks can be further logically-partitioned into multiple, smaller network segments called subnets. A router is put in place as the

logical and/or physical boundary between subnets. VLANs are a method of creating logically-independent Layer 2 broadcast domains within a large network interconnected through switches, creating smaller connected LANs (Figure 2-21). By utilizing VLANs, differentiated services can be applied to equipment of common capability.

Benefits for VLANs include:

- Functional/Treatment of traffic—Quality of Service (QoS)

- Scalability/Network performance—Smaller broadcast domains

- Security—Smaller domains of trust reducing attack surface

By default, the routing or inter-vlan routing features typically at the Industrial Zone core and distribution Layer 3 network device will permit all traffic between VLANs. Access Control Lists (ACLs) on the Layer 3 network interfaces can be used to restrict traffic, but are limited in capabilities. The ACLs on Layer 3 network devices such as routers or multi-layer switches are not the same as firewall rules; they may have performance impact on traffic and they can become too complex to manage if too many exceptions are required. Layer 3 ACLs are most effective when they are small and used for explicit denies.

To provide more flexibility and simplicity to network segmentation, *Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* uses Cisco TrustSec (CTS) technology to define access policies using security groups. This allows the segmentation of IACS assets using Security Group Tags (SGT) which group the assets regardless of their location in the plant-wide network.

Benefits of Cisco TrustSec (CTS) include:

- CTS uses tags to represent logical group privilege.

- The tag is called an SGT and is used in access policies.

- The SGT is understood and is used to enforce traffic by certain Cisco and Allen-Bradley Stratix switches, routers, and firewalls.

- CTS is defined in three phases: classification, propagation, and enforcement.

Figure 2-21   Group by VLANs
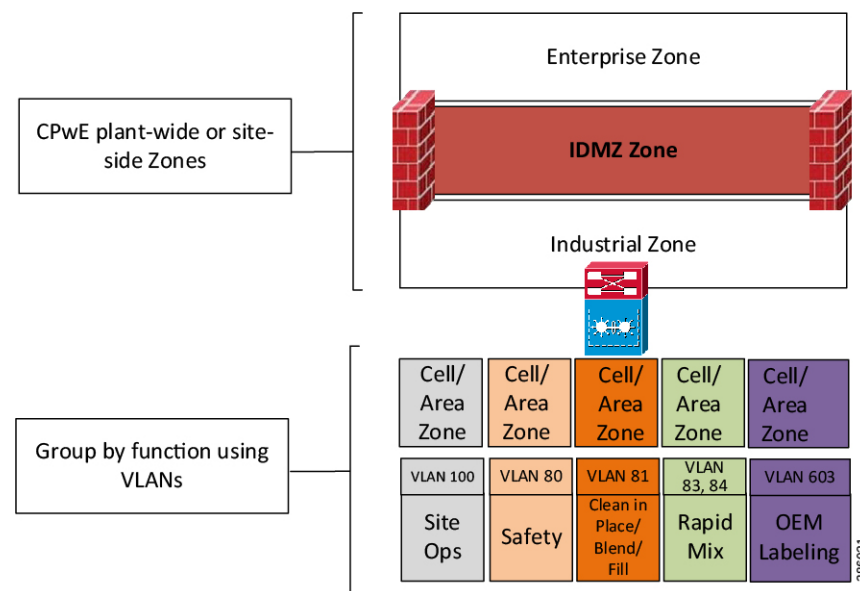
Note   See *Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* are provided for further details.

- 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

CIP Security provides a third layer of defense enforced at the IACS application and device. It creates a network micro-segmentation, which is a more granular approach by helping prevent lateral movement within a zone or between zones. Micro-segmentation reduces an attacker's capability to easily compromise an entire network. A CIP Security architecture within CPwE is composed of multiple zones, which are IACS devices grouped typically based on operation function and security requirements (Figure 2-22).

For brownfield deployments to meet certain security regulations, an organization may have to reconfigure VLANs and readdress IACS devices to meet zoning efforts. This can be highly disruptive to industrial operations. CIP Security allows for a more cost-effective and reliable approach with the ability to create security zones with applicable security properties with minimal redesign to the existing IACS application.

Figure 2-22   CIP Security Zones
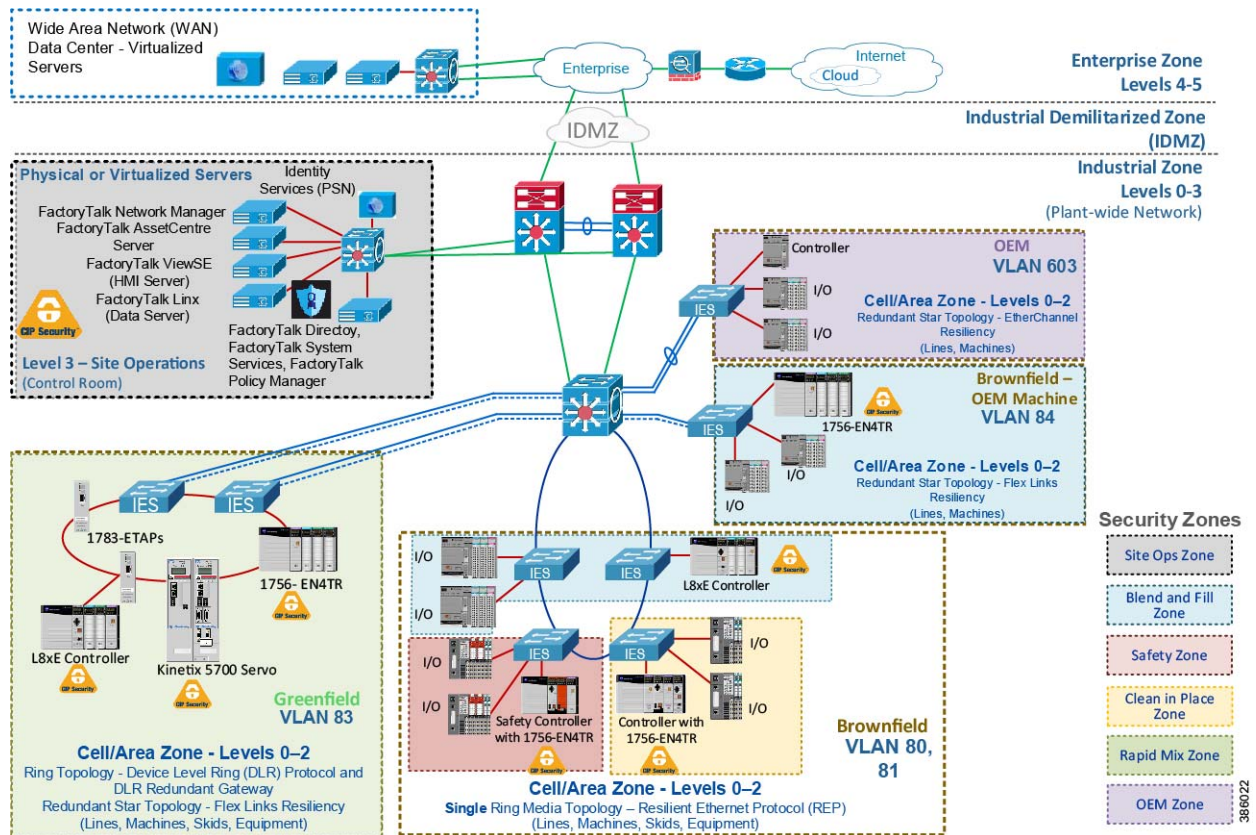
Zones and Conduits

The CIP Security properties to apply in a zone and conduit depends on the requirements identified in the risk assessment and targeted security level. Typically, security properties assigned to zones and conduits can be based on the potential consequences should an attack objective be achieved in that zone. For example, if an operation is interrupted, will it cause financial loss, damage, interruption to the delivery of goods or services essential to the organization's continued success?

Zones are groups to which IACS devices are added. IACS devices are grouped based on operation function and security requirements. A function implies the concept of an individual system or element within a larger system functioning together. CIP Security properties are applied at the zone level, which can be referred to as Intra-zone security and at the conduit level as Inter-zone security. This allows for device identity and authentication and data integrity between IACS devices in the same zone and in different zones.

- Intra-zone consists of CIP Security properties configured on the individual zone and would apply to all devices and CIP application data within that zone but not between other zones. For example, in Figure 2-22 the 1756-L8xE and 1756-EN4TR are in the same Blend and Fill (blue) Zone and configured to uses certificates as device identity and authentication. Even though the two IACS devices are in the same trusted zone, they are still required to exchange certificates for proof of identity. This also allows for data integrity and authentication within the same zone without having to explicitly create a conduit to one another.

    Zones can include a combination of CIP Security capable IACS devices and ones that are not (Table 2-8). IACS devices currently supporting CIP Security are still able to interoperate with IACS devices that do not support CIP Security on the same network through the standard TCP/UDP ports of 44818 and 2222 depending on which IACS device is initiating the CIP connection. IACS devices with CIP Security enabled will use TLS/DTLS version 1.2 on TCP/UDP port of 2221. For additional details, see Trusted IP Communication.

✎
Note   For zones where network communication does not require the level of security for data encryption (for example, CIP Motion applications), Rockwell Automation, Cisco, and Panduit recommend enabling only device and data authentication/integrity without encryption. CIP Motion application was not tested or validated as part of CPwE CIP Security.

Table 2-8   Intra-Zone Security

Zone	IACS devices	Intra-Zone Security Properties
Site Ops Zone (gray)	• FactoryTalk Linx[1] Data Server—OPC data Server • FactoryTalk AssetCentre—IACS inventory and disaster recovery • EWS—Studio 5000 Logix Designer programming • ISE PSN—Endpoint Profiling • FactoryTalk Network Manager—IACS Visibility and Management	• Certificates • Data Integrity • Data Confidentiality
Blend and Fill Zone (blue)	• 1756-L85E[1] • 5069-AEN2TR • 5069-AEN2TR • 1756-EN4TR[1] (remote I/O) • 5069-AEN2TR (remote I/O) • 5069-AEN2TR (remote I/O)	• Certificates • Data Integrity • Data Confidentiality
Safety Zone (red)	• 1756-73S with 1756-EN4TR[1] • 1734-AENTR with safety I/O • 1734-AENTR with safety I/O	• Certificates • Data Integrity
Clean in Place Zone (yellow)	• 1756-L75 with 1756-EN4TR[1] • 1734-AENTR • 1734-AENTR	• Certificates • Data Integrity • Data Confidentiality
Rapid Mix Zone (green)	• 1756-L85E[1] • 1756-EN4TR[1] (I/O)	• Certificates • Data Integrity
OEM Zone (purple)	• 5069-L340ERM • 5069-AEN2TR • 5069-AEN2TR	• Trusted IP

1. For a list of the catalog numbers with the associated firmware versions that currently support CIP Security, see System Components.

• Inter-zone consists of CIP Security properties configured on the individual conduit and would apply to CIP application data traversing between different zones. For example, in Figure 2-23 for FactoryTalk applications defined in the Site Ops Zone (gray) to securely exchange EtherNet/IP data with the Levels 0 - 2 Cell/Area Zones containing CIP Security IACS devices, a conduit must be explicitly configured with the desired security properties from the Site Ops Zone (gray) to each of the following zones:

  – Blend and Fill Zone (blue)

- Clean in Place Zone (yellow)

- Rapid Mix Zone (green)

- Safety Zone (red)

Figure 2-23   Inter-Zone Security
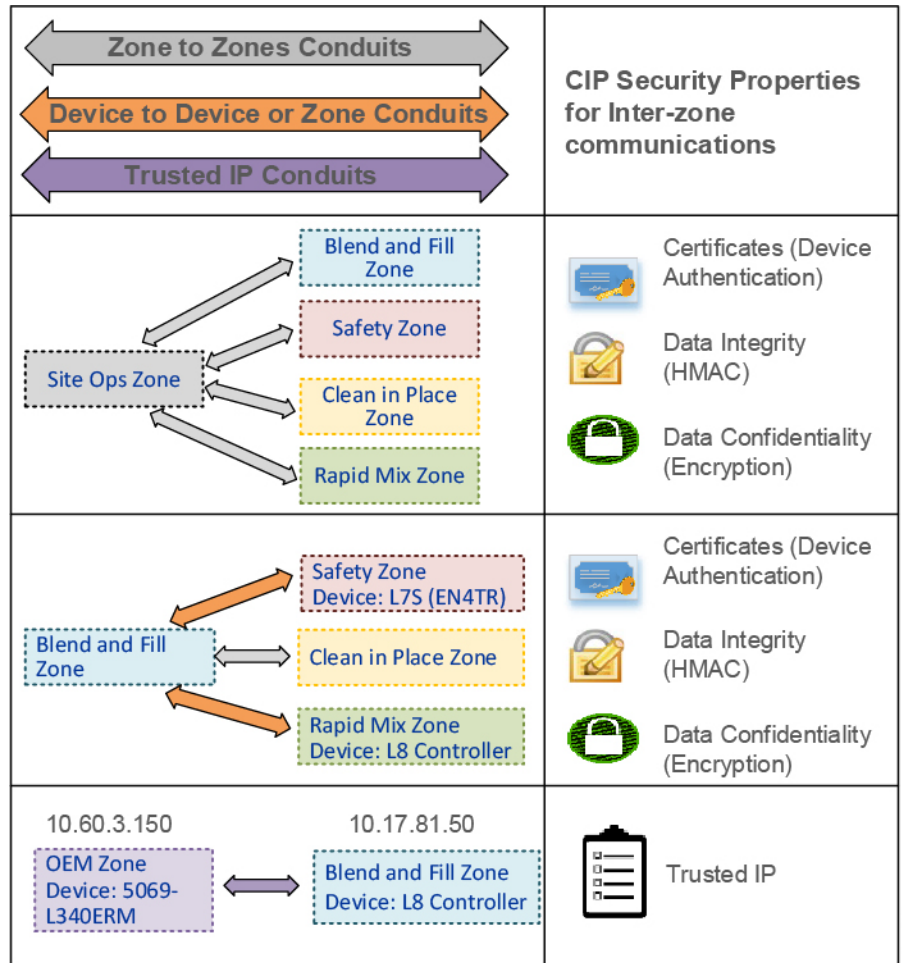
Conduits are used to control access and trusted communication to and from different zones. Any communication between zones must be explicitly configured through a defined conduit. To manage and control communication between zones, conduits can be created and removed as needed on a device-to-device and zone-to-zone basis. This is not a new concept; VPNs are conduits creating a secure tunnel from a source to a destination using negotiated cipher suites.

Types of CIP Security Conduits include:

- Zone to Zone Conduits—This type of conduit is useful for centralized zones like the Level 3-Site Operations and Level 2-Supervisory controls where communications are exchanged to and from the plant-wide or site-wide IACS devices.

- Device to Device Conduit—This type of conduit is useful in situations where certain IACS device control to an operation is identified more critical therefore strict controlled access must be applied with higher security than the other IACS in the same zone.

- Device to Zone Conduit—This type of conduit is useful when controlled access from a single IACS device in a particular zone is required to a group of IACS in another zone.

- Trusted IP Conduit—This type of conduit can be used for CIP connections initiated from legacy IACS devices, third-party applications, or OEM machines that do not support the CIP Security technology to ones that do support it. For example, in Figure 2-23 a Trusted IP conduit must be defined and explicitly created for the OEM Zone CompactLogix 5380 (5069-L340ERM) to send an MSG to the Blend and Fill Zone ControlLogix 5580 (1756-L85E).

Note   Once CIP Security capable IACS devices are configured and deployed with security properties, RSLinx Classic will not be able to browse and discover those IACS devices unless a Trusted IP conduit is configured and deployed. FactoryTalk Linx version 6.11 or higher supports CIP Security and must be used to browse and discover IACS devices.

From the requirements and data flow identified in the threat model and risk assessment, it is recommended to create a security matrix of what communication streams are permitted or denied from zone to zone or IACS devices in different zones (Figure 2-24).

Figure 2-24   IACS Security Matrix

Source \ Destination	Site Ops Zone Devices	Safety Zone Devices	Blend and Fill Zone Devices	Clean in Place Zone Devices	Rapid Mix Zone Devices	OEM Zone Devices
Site Ops Zone Devices	Default - Permit	Permit	Permit	Permit	Permit	Permit
Blend and Fill Zone Devices	Permit	Permit	Default - Permit	Permit	Permit	Permit
Clean in Place Zone Devices	Permit	Permit	Permit	Default - Permit	Permit	Deny
Rapid Mix Zone Devices	Permit	Permit	Permit	Permit	Default - Permit	Deny
Safety Zone Devices	Permit	Default - Permit	Permit	Permit	Permit	Deny
OEM Zone Devices	Permit	Deny	Permit	Deny	Deny	Default - Permit

FactoryTalk System Overview

A FactoryTalk system is composed of software products, services, and hardware devices participating together and sharing the same FactoryTalk Directory and FactoryTalk services. In every FactoryTalk System, one computer must be designated as the FactoryTalk Directory server (FTD). The FTD is the centerpiece of the FactoryTalk Services Platform, providing a central lookup service for all products participating in an application. The role of the FTD in the Rockwell Automation environment is analogous to the role of a Domain Controller in the Microsoft Windows environment.

There are currently two types of FactoryTalk Directories:

- A Local FactoryTalk Directory (Local FTD) is typically used in a single (standalone) computer system. The Local FTD may or may not be connected to a Local Area Network (LAN).

- A Network FactoryTalk Directory (Network FTD) is designed primarily for use with a multiple (distributed) computer system, and it is normally connected to a LAN. Any other computers in the FactoryTalk system such as FactoryTalk View Site Edition (SE) and FactoryTalk Transaction Manager are clients to the designated Network FTD.

Note   FactoryTalk Live Data clients such as FactoryTalk View, FactoryTalk Transaction Manager, FactoryTalk Alarm and Events, FactoryTalk Linx Gateway, etc. rely on FactoryTalk Live Data service to manage connections between FactoryTalk products and data servers that are part of a FactoryTalk application. FactoryTalk Live Data handles and facilitates reading and writing values from and to OPC-DA servers as well as Live Data servers on behalf of these client software products. This type of communication uses various static and dynamic ports beyond the EtherNet/IP TCP 44818 and UDP 2222. It is recommended to implement the Microsoft Windows IPsec functionality to provide security services for IP network traffic between these client software products. In addition to IPsec, network traffic generated by the FactoryTalk View products and their components can be protected by SSL/TLS. For example, both FactoryTalk View SE and FactoryTalk ViewPoint support communication over HTTPS. For more details, see the Rockwell Automation Knowledgebase article QA46277 - "Deploying FactoryTalk Software with IPsec" (https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1090456).

A typical CIP Security implementation will be with a single Network FTD system. A Network FTD provides services to a group of hosts, with most FactoryTalk software utilizing the network directory as the Local FTD has little architecture options since it serves only the host upon which it is installed.

As a recommended best practice, the FactoryTalk Directory should be installed on an independent computer to allow the following:

- System Start-up—Most of the FactoryTalk software products rely on the various services provided by the FTD, the lowest risk scenario is to have it available as these products are initializing.

- Patching/Upgrading—Patching an FTD hosted on a dedicated computer translates to minimum system downtime, as it is not affecting the operation of other FactoryTalk components while rebooting.

- Securing and limiting physical access to computer hardware—Put measures in place to limit operator access and to protect your hardware systems. It is essential to limit operator access to the hardware running Windows operating systems and FTD. An operator with access to the power switch and bootable media could have direct access to the underlying file system and could potentially circumvent many of the security measures described in this document.

FactoryTalk Services Platform includes built-in security user groups (Figure 2-25) used to define user privileges for FactoryTalk Policy Manager. FactoryTalk user or Windows-linked user accounts created in FactoryTalk Administration Console can be added to the built-in security groups to grant specific rights in FactoryTalk Policy Manager. Table 2-9 lists the access rights for the built-in security user groups in FactoryTalk Policy Manager.

Figure 2-25   FactoryTalk Services Platform built-in Security User Groups
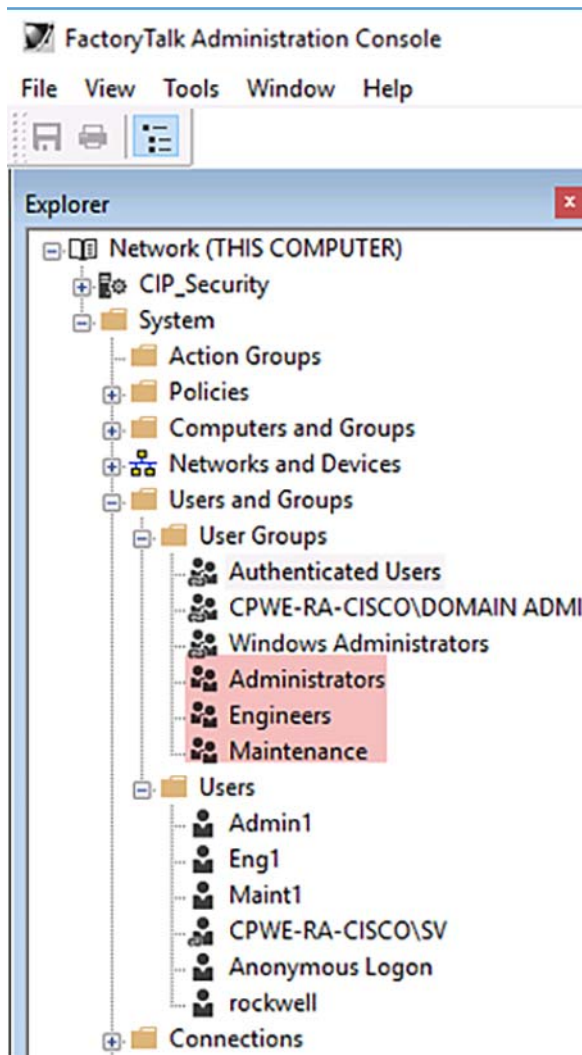
Table 2-9   Built-in Security User Access in FactoryTalk Policy Manager

Access Right	Built-in Security Group	Permissions
View-Only	• Administrators • Engineers • Maintenance	All security policy items are read-only or may not appear on the FactoryTalk Policy Manager main menu bar: • Adding/creating Zones, Conduits, and Devices • Deleting Zones, Conduits, and Devices • Editing Zones, Conduits, Device Properties, and Port Properties • Discover Devices, Add Range, and Replace Device Global settings for editing Model name and Certificate Setting are grayed out for read-only access. The **Help** option is active and can be accessed on the main menu bar.
Deploy	• Administrators • Engineers • Maintenance	The security policy can be deployed to devices. Devices can be replaced in the security model. Security policy items and global settings are read-only. • **Deploy** is active on the main toolbar. • **Replace Device** is active on the Zone toolbar. • **Replace Device** is active on the Device toolbar.
Edit	• Administrators	All controls are active and all security policy items and global settings can be modified. • Adding/creating Zones, Conduits, and Devices • Deleting Zones, Conduits, and Devices • Editing Zones, Conduits, Device Properties, and Port Properties • Discover Devices, Add Range, and Replace Device • Deploy security model

CIP Security Solution Use Cases

The solution use cases in Table 2-10 are addressed by CPwE CIP Security.

Table 2-10 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

Warning It is recommended to schedule downtime or maintenance window when deploying a CIP Security model to an IACS network. Before a deployed security policy becomes active, communications must be reset to all configured IACS devices, resulting in a short loss of connectivity. This will also allow time for any troubleshooting if needed.

The workflow for onboarding, deleting, and replacing CIP Security capable IACS devices can be found in Chapter 3, "CPwE CIP Security Configuration."

Use Case 1—CIP Security Protection with Zone to Zone Conduit

The recommended initial deployment of the CIP Security is to secure communication from the Level 3-Site Operations FactoryTalk Applications Zone(s) to each Levels 0-2 Cell/Area Zone(s) with CIP Security IACS devices. Typically, the Site Operations Zone contains the site-wide servers to each IACS Cell/Area Zone containing the controls and area supervisory assets. This is ideal since most threats originate from high in the 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. 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 accepted.

In this use case, 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 2-26). Once CIP Security capable IACS devices are configured and deployed with security

properties, RSLinx Classic will not be able to browse and discover those IACS devices unless a Trusted IP conduit is configured and deployed. FactoryTalk Linx version 6.11 or higher supports CIP Security and must be used to browse and discover IACS devices.

Retrofitting the 1756-EN4TR communication module in existing ControlLogix 5570 chassis to secure EtherNet/IP communications allows for a cost-effective and reliable approach to designing security into an existing network. The Safety Zone (red) and the Clean in Place Zone (yellow) used the CIP Security capable 1756-EN4TR communication module in the local ControlLogix 5570 chassis to secure EtherNet/IP communications with other zones.

Figure 2-26   Use Case 1—CIP Security Zone to Zone Conduit
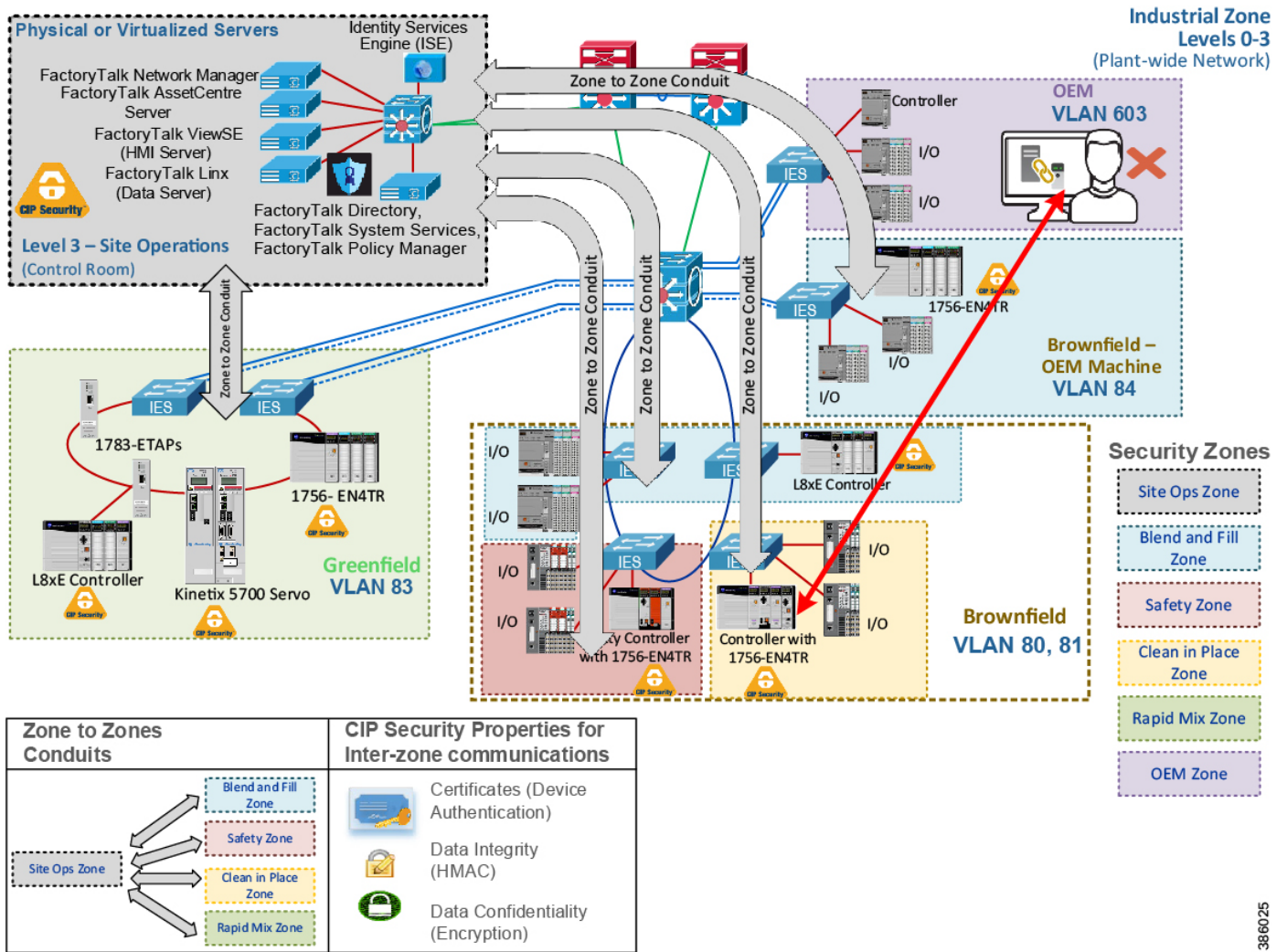
In Figure 2-27 the webpage of the local 1756-EN4TR with IP Address 10.17.81.51 shows the TCP connections after the CIP Security deployment. It has ten ESTABLISHED TCP connections, seven from trusted unsecured connections using port 44818 and three from trusted secure connections using port 2221. The local 1756-EN4TR is also both the client for some connections and a server for other connections.

Furthermore, it has accepted and ESTABLISHED an unsecured TCP connection from an untrusted IACS device Remote Address: 10.18.2.71 on Remote Port: 60422. In this scenario, the local 1756-EN4TR excludes the IACS device IP Address: 10.18.2.71 in its CIP Security configuration, therefore it is able to deny CIP connections, which can be seen in the Wireshark screen capture in Figure 2-28. This deny action will result

in the IACS device's (Remote Address: 10.18.2.71) ability to browse the backplane of the local 1756-EN4TR module therefore thwarting unwanted attempts of going online, uploading, or downloading to the local controller. Additionally, Studio 5000 Logix Designer will deny untrusted attempts with a popup Error: 0x032F: Ingress rule deny non-secure.

Figure 2-27   1756-EN4TR Webpage (TCP Connections Page)

Figure 2-28   1756-EN4TR Denies Untrusted IACS Device
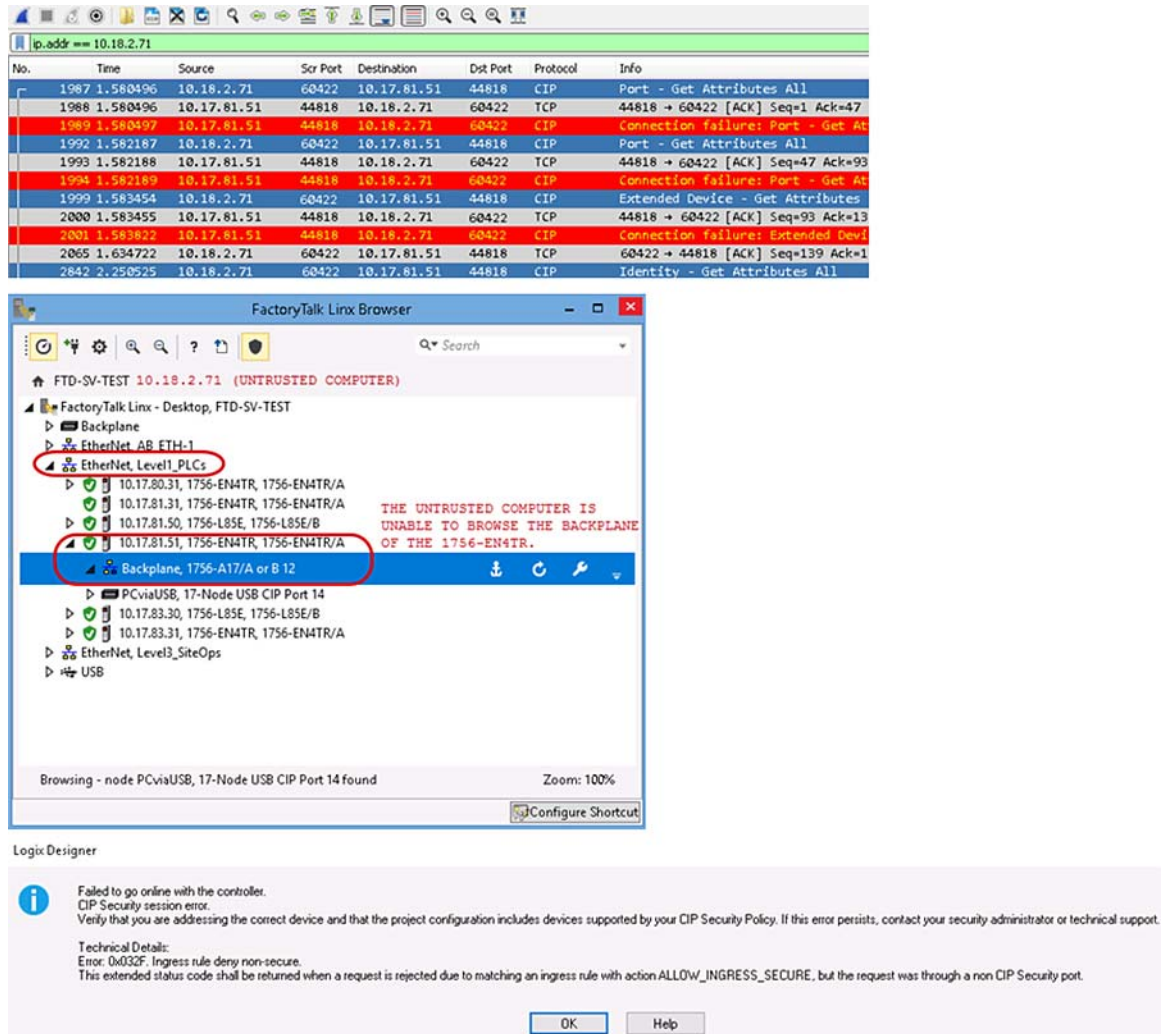
Use Case 2—CIP Security Protection with Device to Device or Zone Conduits

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 east-west traffic flow for EtherNet/IP communications between IACS devices in different zones (Figure 2-29), for example ControlLogix to ControlLogix message instructions (MSG) will use data integrity to confirm data was not altered in transit and optionally enable data confidentiality to help protect intellectual property with the help of the TLS network protocol. Rockwell Automation, Cisco, and Panduit recommend using device and data authentication/integrity without encryption for CIP Motion or I/O applications.

Note CIP Motion application was not tested or validated as part of CPwE CIP Security. See the specific vendor IACS device technical specification publication for performance and capacity.

OEMs can seamlessly integrate CIP Security IACS devices into a customer's plant-wide architecture. The OEM would test and qualify the skid/machine with the required CIP Security properties enabled. Before shipping the skid/machine, CIP Security must be completely cleared using the FactoryTalk Policy Manager commissioning tool software. The OEM could provide documentation and guidance in terms of what options to select for reasonable performance. It would be up to the end user to apply security. See Removing the CIP Security Policy from an IACS Device in Chapter 3, "CPwE CIP Security Configuration."

Figure 2-29   Use Case 2—CIP Security Device to Device or Zone Conduit

In Figure 2-30 the two 1756-L85Es named Blue and Green are communicating using an MSG. Green is reading a tag named Read_L8_String from Blue. In the following Wireshark screen capture, the value being passed in the tag is the string 'SECRETRECIPE11'. Even with the CIP Security data integrity in place to verify the data was not altered in transit, without data confidentiality (encryption), intellectual property and even passwords are sent in plaintext making it available for anyone running Wireshark on the network to capture and steal sensitive information.

Figure 2-30   Unencrypted MSG between Two 1756-L85Ess

In Figure 2-31 the same two 1756-L85Es are now communicating using CIP Security data integrity and data confidentiality (encryption) enabled. Green can read the tag value as 'SECRETRECIPE111' because it has the correct shared secret key to decrypt. The Wireshark screen capture now shows the payload of the two 1756-L85Es as encrypted and unreadable without the correct shared secret key to decrypt.

Figure 2-31   Encrypted MSG between Two 1756-L85Es
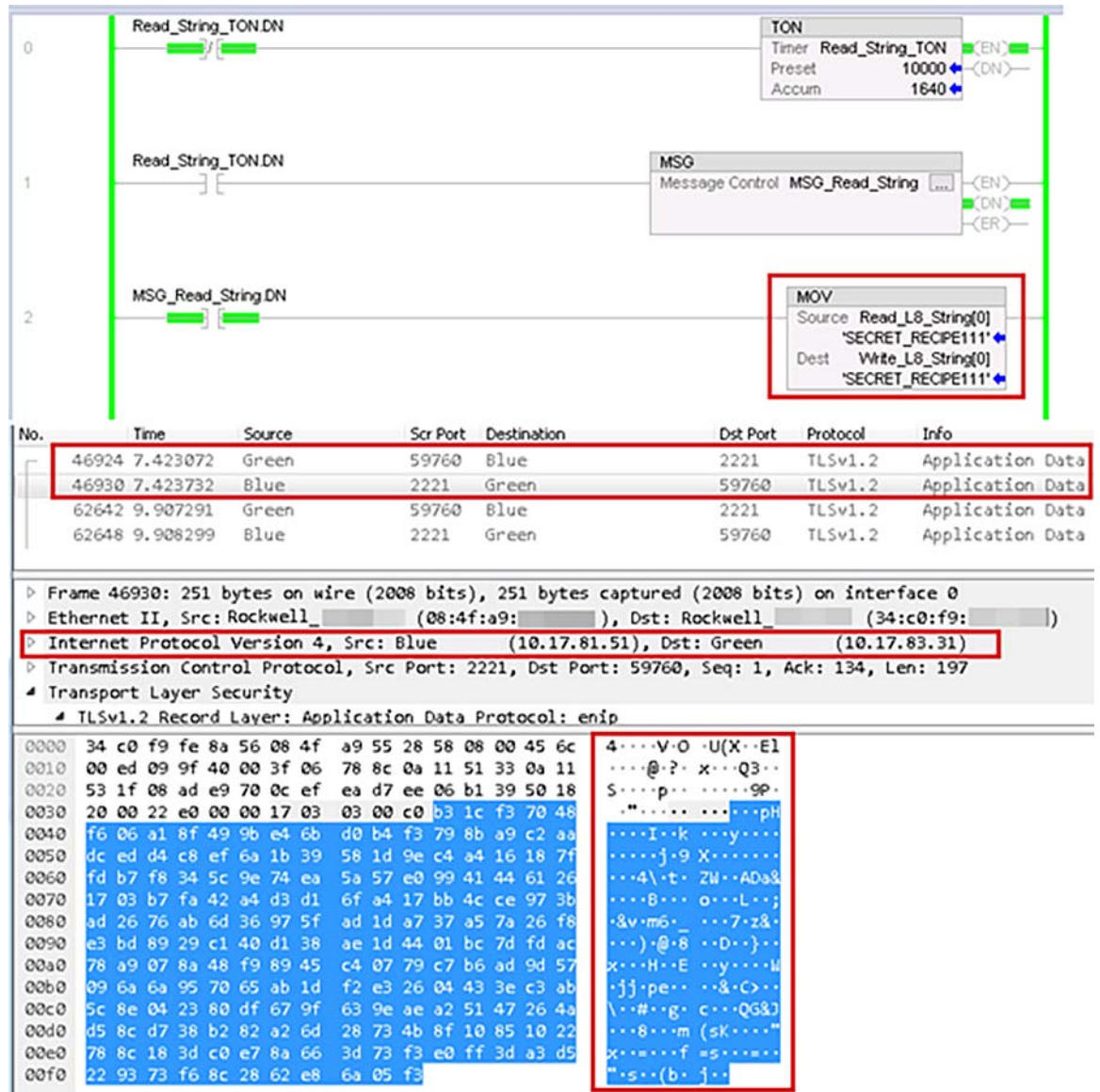
Use Case 3—CIP Security Protection with Trusted IP Conduits

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 network by using the Trusted IP feature. The feature can be implemented to authorize CIP communication between an IACS device that is capable of CIP Security and one that is not based on IP address. The security properties of the Trusted IP conduit cannot be extended to secure communications for other industrial protocols like Modbus or common Internet protocols like ICMP.

For IACS applications, use FactoryTalk Policy Manager to create Trusted IP conduits for trusted IP addresses in EtherNet/IP communications between non-CIP Security IACS devices and applications to CIP Security IACS devices. Essentially, the tool deploys two kinds of Trusted IP conduits, an explicitly defined Trusted IP conduit and an implied Trusted IP through a secure CIP Security enabled conduit.

Explicitly Defined Trusted IP Conduit

When a zone contains all non-CIP Security capable IACS devices like the OEM Zone (purple) and an IACS belonging to that zone, it must initiate a CIP connection to an IACS device with CIP Security capability in another zone. Then an explicitly defined Trusted IP conduit must be configured in the Conduits component page of FactoryTalk Policy Manager. In Figure 2-32 a Trusted IP conduit must be defined and explicitly created for the OEM Zone (purple) CompactLogix 5380 (5069-L340ERM) to send an MSG to the Blend and Fill Zone (blue) ControlLogix 5580 (1756-L85E).

Implied Trusted IP Conduit

When a zone like the Site Ops Zone (gray) contains an inter-mix of CIP Security capable IACS devices and ones that are not, the non-CIP Security capable IACS devices will have a yellow triangle information icon displayed next to them in the tool. When a zone to zone or device conduit is created with CIP Security enabled, for example the Site Ops Zone (gray), the CIP Security capable IACS devices will implicitly trust the non-CIP Security capable IACS devices using the Trusted IP capability. The non-CIP Security capable IACS devices will not be able to use any of the CIP Security properties configured on the zone or the conduits for communication. Additionally, it is no need to create a second conduit for the Site Ops Zone (gray) specifically for the Trusted IP capability to the non-CIP Security capable IACS devices. As an example, in Figure 2-33 FactoryTalk Network Manager is an application that does not support CIP Security. However, it can initiate CIP connections to other zones through a CIP Security enabled zone to zone conduit and therefore their IP addresses are implicitly trusted by CIP Security enabled IACS devices in other zones.

Figure 2-32   Use Case 3—Rockwell Automation CIP Security Trusted IP Conduits
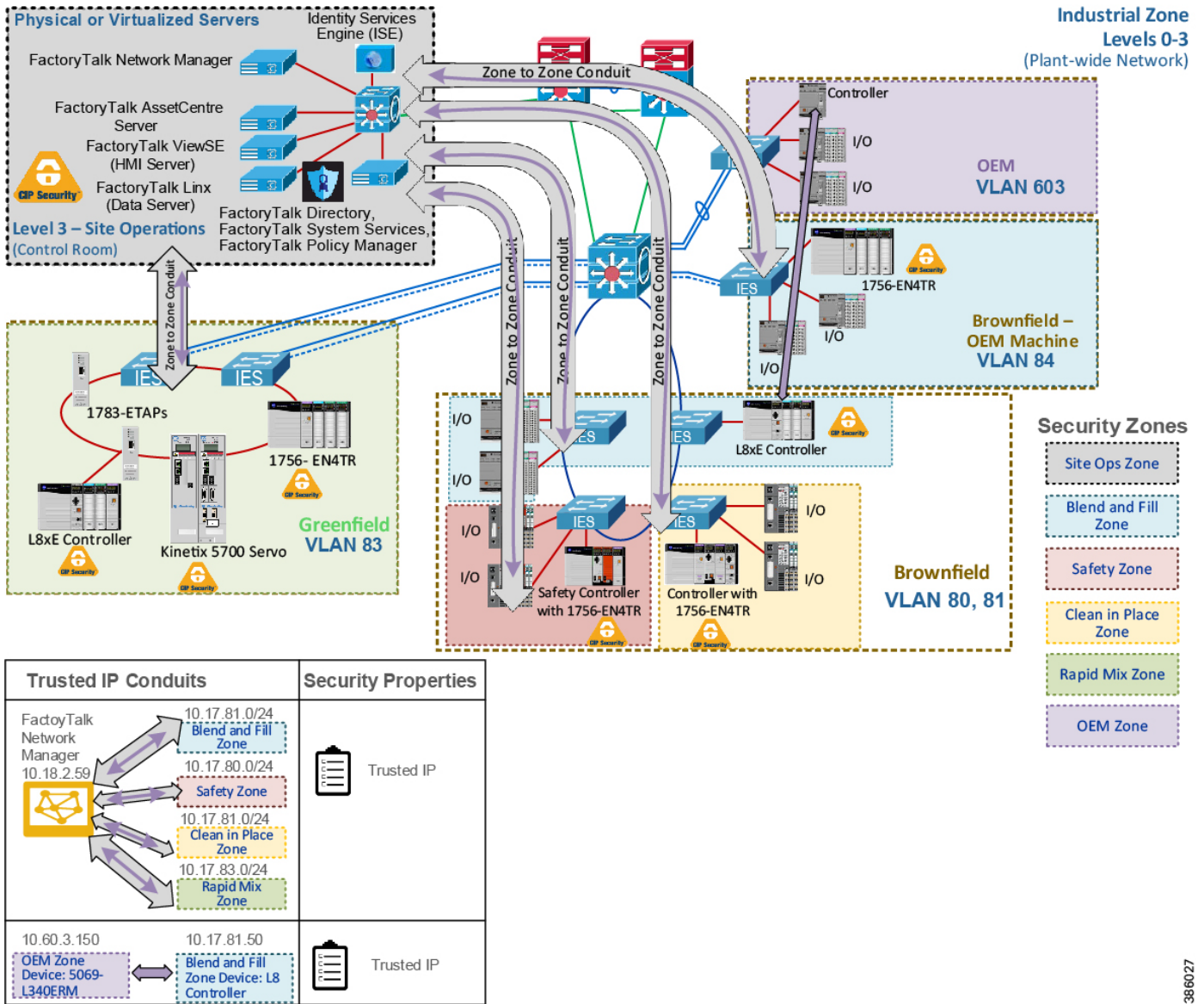
Figure 2-33   CIP Connections to Other Zones through a CIP Security Enabled Zone to Zone Conduit

CPwE CIP Security Configuration

This chapter describes how to configure CIP Security Zones and Conduits within the CPwE architecture based on the design considerations and recommendations of Chapter 2, "CPwE CIP Security Design Considerations." The included configurations have been verified during reference architecture testing.

This chapter is not intended to provide step-by-step procedures to configure the network infrastructure devices such as routers, firewalls, or IES due to the variability in network architectures. Presumably, the network IACS devices will have end-to-end connectivity to the computer or server hosting the Network FTD, which also has the FactoryTalk System Services, and FactoryTalk Policy Manager installed on it. However, this chapter discusses specific items related to FactoryTalk applications and IACS devices and their interaction with CIP Security. This section includes the steps required to properly configure and deploy CIP Security features in FactoryTalk Policy Manager to help achieve secure EtherNet/IP communications in an IACS.

Note The client/server terminology is commonly used with TCP and TLS/DTLS connections and originator/target for CIP connection. However, for simplicity of this document, the terms client/server will be generalized and used throughout this document when discussing the behavior associated with a connection of an IACS device. The client initiates a connection and the server listens for and accepts a connection.

Overview

FactoryTalk Policy Manager is the commissioning tool GUI used to configure, deploy, and view the system communication for CIP Security properties. When a user logs in to the tool, the menu divides the system security policy into different components. Use these components to design security models that control the permissions and usage of IACS devices within the system.

- Zone component—Groups of IACS devices.
- Conduit component—Communication routes between components.
- Device component—Computers, controllers, modules, HMI panels, and drives.
- Deleted Devices component—Delete IACS device that is no longer needed. After an IACS device is deleted it will be listed in the Deleted Devices table until the next time the model is deployed.

A fully configured instance with zones, devices, and conduits along with their respective CIP Security properties inside FactoryTalk Policy Manager is referred to a security model.

FactoryTalk Policy Manager depends on FactoryTalk System Services for certificate services, policy deployment, and authentication. FactoryTalk System Services is the service that signs and issues client certificates to give assurance for a communicating party's authenticity. It runs as a service in the background to help enable the deployment of the CIP Security model configured in the FactoryTalk Policy Manager commissioning tool.

The CPwE CIP Security model consisted of multiple zones and conduits with a mix of intra-zone and inter-zone security properties applied based on functional and security requirements obtained from the security risk assessment process. Each organization's functional and security requirements will vary based on their own security risk assessments.

The CPwE CIP Security model security zones containing various VLANs (Figure 3-1).

- 0-Site Operations Zone

- 1-Blue (Blend/Fill) Zone

- 2-Red (Safety) Zone

- 3-Yellow (Clean in Place (CIP)) Zone

- 4-Green (Rapid Mix) Zone

- 5-OEM (Packaging) Zone

- 6-Support EWS Zone

Note   The numerical values [0-6] shown before the zone name are locally significant and only used in the security model configuration for better organization of the zones for publication purposes.

Table 3-1 contains the following IACS devices and Zone Properties for each zone in the CPwE CIP Security model.

- 0-Site Operations and 6-Support EWS Zones combines functional zones Levels 3-2 IACS devices:

    - **Level 3 Site Operations** contains the assets that are critical to monitoring and controlling the plant-wide or site-wide industrial operations. Data flow will typically be class 3 HMI communications to and from IACS devices.

    - **Level 2 Supervisory control** contains the local management software where Engineering workstations (EWS) use class 3 CIP administration communications for uploading/downloading projects to the controllers.

- 1-Blue (Blend/Fill), 2-Red (Safety), 3-Yellow (Clean in Place (CIP)), 4-Green (Rapid Mix), and 5-OEM (Packaging) Zones combines functional zones Levels 0-1 IACS devices. These areas are critical to help ensure that industrial operations continue. Typically, class 0/1 and 3 types of traffic can occur at these levels.

    - **Level 1 Control system** contains the controllers instructing the Level 0 IACS devices and gathering data about a particular process.

    - **Level 0 Process** contains the sensors, actuators, drives, and robots performing the functions of the process.

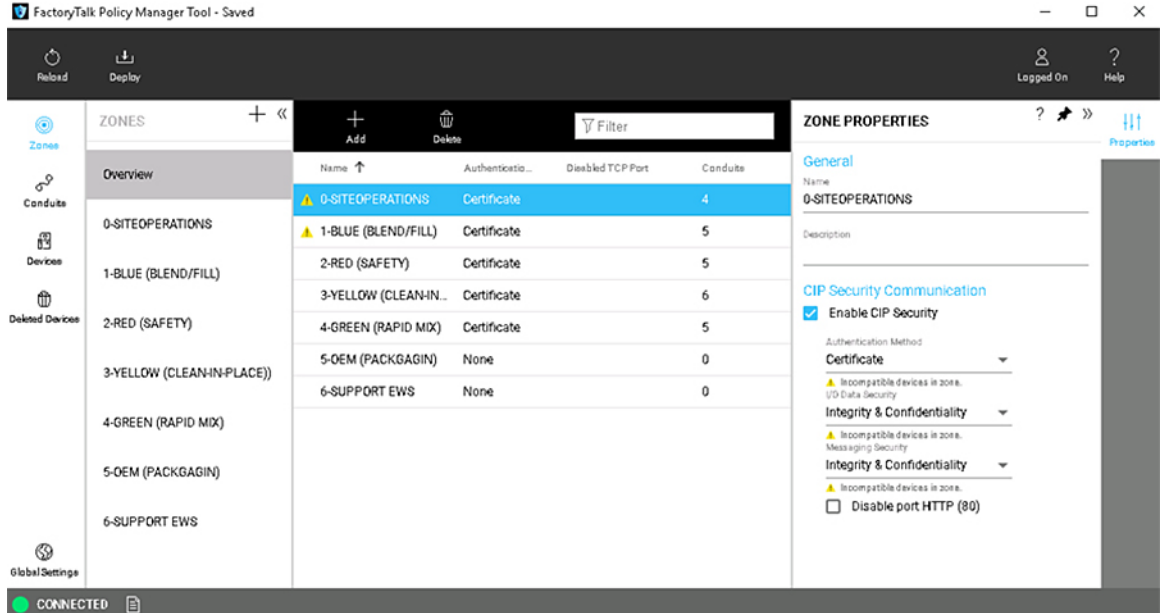Figure 3-1   Zones in the CPwE CIP Security Model

Table 3-1 contains the following IACS devices and Zone Properties for each zone in the CPwE CIP Security model. Intra-zone security properties are the policies configured on the individual zone and would apply to all IACS devices and CIP application data within that zone but not between other zones. Each zone is applied with the security properties based on functional and security requirements obtained from conducting a security risk assessment.

Table 3-1   CPwE CIP Security Model IACS Devices and Zone Properties

Zone	IACS Devices	Intra-Zone Security Properties
0-Site Operations	• FactoryTalk Linx[1] Data Server - OPC data Server • FactoryTalk AssetCentre[1] - IACS inventory and disaster recovery • EWS - Studio 5000 Logix Designer[1] programming • ISE PSN -Endpoint Profiling • FactoryTalk Network Manager - IACS Visibility and Management	• Certificates • Data Integrity • Data Confidentiality
6-Support EWS	• Maintenance EWS with only RSLinx Classic and Studio 5000 Logix Designer installed	• Trusted IP

Table 3-1   CPwE CIP Security Model IACS Devices and Zone Properties (continued)

Zone	IACS Devices	Intra-Zone Security Properties
1-Blue (Blend and Fill)	• 1756-L85E[1] • 5069-AEN2TR • 5069-AEN2TR • 1756-EN4TR[1] (remote I/O) • 5069-AEN2TR (remote I/O) • 5069-AEN2TR (remote I/O)	• Certificates • Data Integrity • Data Confidentiality
2-Red (Safety Zone)	• 1756-73S with 1756-EN4TR[1] • 1734-AENTR with safety I/O • 1734-AENTR with safety I/O	• Certificates • Data Integrity
3-Yellow (Clean in Place (CIP))	• 1756-L75 with 1756-EN4TR[1] • 1734-AENTR • 1734-AENTR	• Certificates • Data Integrity • Data Confidentiality
4-Green (Rapid Mix)	• 1756-L85E[1] • 1756-EN4TR[1] (I/O)	• Certificates • Data Integrity
5-OEM (Packaging)	• 5069-L340ERM • 5069-AEN2TR • 5069-AEN2TR	• Trusted IP

1. The following catalog numbers with the associated firmware versions currently support CIP Security. See System Components in Chapter 2, "CPwE CIP Security Design Considerations" for a complete list.

When CIP Security is enabled, only IACS devices within zones or an explicitly configured conduit are capable of establishing communications with other IACS devices in the security model. Conduits control access to and from different zones. Any CIP communication between zones must be through a defined conduit. Other IACS devices not in the same zone or explicitly configured with a conduit will be blocked.

Figure 3-2 shows the CPwE CIP Security model conduits. CIP Security properties will also be applied at the conduit component for inter-zone communications. The security properties applied are based on functional and security requirements obtained from the security risk assessment process. Each organization's functional and security requirements will vary based on their own security risk assessments.

Figure 3-2   Conduits in the CPwE CIP Security Model

Defined Conduits	Zone	⟷	Zone	Conduit CIP Security Properties
Conduit 1	0-Site Operations All host IP addresses in this zone		1-Blue (Blend and Fill) Zone All host IP addresses in this zone	• Authentication Method: Certificate • I/O Data Security: Integrity & Confidentiality • Messaging Security: Integrity & Confidentiality
Conduit 2	0-Site Operations All host IP addresses in this zone		2-Red (Safety Zone) All host IP addresses in this zone	
Conduit 3	0-Site Operations All host IP addresses in this zone		3-Yellow (Clean in Place (CIP)) All host IP addresses in this zone	
Conduit 4	0-Site Operations All host IP addresses in this zone		4-Green (Rapid Mix) Zone All host IP addresses in this zone	

Defined Conduits	Device or Zone	⟷	Device or Zone	Conduit CIP Security Properties
Conduit 5	1-Blue (Blend and Fill) Zone All host IP addresses in this zone		2-Red (Safety Zone) **Device:** 1756-L73Safety with 1756-EN4TR	• Authentication Method: Certificate • I/O Data Security: Integrity & Confidentiality • Messaging Security: Integrity & Confidentiality
Conduit 6	1-Blue (Blend and Fill) Zone All host IP addresses in this zone		3-Yellow (Clean in Place (CIP)) **Device:** 1756-L75 with 1756-EN4TR	
Conduit 7	1-Blue (Blend and Fill) Zone All host IP addresses in this zone		4-Green (Rapid Mix) Zone All host IP addresses in this zone	
Conduit 8	2-Red (Safety Zone) **Device:** 1756-L73Safety with 1756-EN4TR		3-Yellow (Clean in Place (CIP)) **Device:** 1756-L75 with 1756-EN4TR	• Authentication Method: Certificate • I/O Data Security: Integrity & Confidentiality • Messaging Security: Integrity & Confidentiality
Conduit 9	2-Red (Safety Zone) **Device:** 1756-L73Safety with 1756-EN4TR		4-Green (Rapid Mix) Zone All host IP addresses in this zone	
Conduit 10	3-Yellow (Clean in Place (CIP)) **Device:** 1756-L75 with 1756-EN4TR		4-Green (Rapid Mix) Zone All host IP addresses in this zone	• Authentication Method: Certificate • I/O Data Security: Integrity & Confidentiality • Messaging Security: Integrity & Confidentiality

Defined Conduits	Device or Zone	⟷	Device or Zone	Conduit CIP Security Properties
Conduit 11	6-Support EWS **Device:** Maintenance EWS with RSLinx Classic and Studio 5000 Designer 10.18.3.245		1-Blue (Blend and Fill) Zone All host IP addresses in this zone	• Authentication Method: Trusted IP • I/O Data Security: None • Messaging Security: None
Conduit 12	6-Support EWS **Device:** Maintenance EWS with RSLinx Classic and Studio 5000 Designer 10.18.3.245		2-Red (Safety Zone) Zone All host IP addresses in this zone	• Authentication Method: Trusted IP • I/O Data Security: None • Messaging Security: None
Conduit 13	6-Support EWS **Device:** Windows 10 EWS with Studio 5000 Designer 10.18.2.59		3-Yellow (Clean in Place (CIP)) Zone All host IP addresses in this zone	• Authentication Method: Trusted IP • I/O Data Security: None • Messaging Security: None
Conduit 14	6-Support EWS **Device:** Maintenance EWS with RSLinx Classic and Studio 5000 Designer 10.18.3.245		4-Green (Rapid Mix) Zone All host IP addresses in this zone	• Authentication Method: Trusted IP • I/O Data Security: None • Messaging Security: None
Conduit 15	5-OEM (Packaging) **Device:** 5069-L340ERM 10.60.3.150		1-Blue (Blend and Fill) **Device:** 1756-L85E 10.17.81.50	• Authentication Method: Trusted IP • I/O Data Security: None • Messaging Security: None
Conduit 16	5-OEM (Packaging) **Device:** 5069-L340ERM 10.60.3.150		3-Yellow (Clean in Place (CIP)) **Device:** 1756-L75 with 1756-EN4TR 10.17.81.31	• Authentication Method: Trusted IP • I/O Data Security: None • Messaging Security: None

Note   Non-CIP Security capable IACS devices can be added to the security model. These IACS devices will have a yellow triangle information icon displayed next to them in the center Content pane and the same icon stating *Incompatible devices with zone* beneath each security configuration option. These IACS devices will not receive CIP Security policy themselves. However, the CIP Security capable IACS devices will implicitly add the IP address of the non-CIP Security capable IACS devices to their Trusted IP list so that communication between the IACS devices can occur.

⚠️ *Incompatible devices in zone*.

Planning and Component Considerations

Implementing a CIP Security model requires preparation and planning before deployment. At a minimum, gather this information:

- **Number of zones**—When planning for security in a new system (greenfield) or redesign of an existing system (brownfield), the first step is to break the system into different zones and define conduits connecting these zones where necessary.

- **Security requirements for each zone and conduit**—Once a zone model of the system is established each zone and conduit is assigned a SL-T, based on a consequence analysis, which describes the desired security assurance for the respective zone or conduit. Determine the security requirements for the communication in the intra-zone and inter-zones:

    - Device identity/authentication

    - Data integrity/authentication

    - Data confidentiality (encryption)

    - Trusted IP

- **IACS devices assigned to each zone**—IACS devices are the modules, drives, controllers, HMI panels, computers, and servers that work together to create an IACS network. FactoryTalk Policy Manager will allow adding IACS devices and software that do not support CIP Security in the security model. However, they are not able utilize any of the CIP Security properties including device or data identity/authentication and encrypting communications.

    Next describe the functionality that should be provided by assets in a zone and the connections between zones to meet the security objectives. If certain legacy IACS devices do not satisfy a specific CR of the overall zone or SR, then additional security measures should be taken as described in the defense-in-depth concept.

- **Required data flows and define trust relationships between conduits**:

    - Zones and zones or IACS devices

    - IACS devices to IACS devices

    - Trusted IP

FactoryTalk Policy Manager Configuration

Step 1   Validate all communication, processes, and programs are running as expected without CIP Security enabled, including:

- Controller programs

- I/O connections

- MSG executions

- HMI displays

Verify the computer hosting FactoryTalk Policy Manager has successful communications to all required IACS devices, which include but is not limited to:

- Ping

- Tracert (Microsoft Windows), Traceroute (Cisco IOS, e.g., Allen-Bradley IES)

- Successfully discovered in FactoryTalk Linx Browser utility or FactoryTalk Linx in the Administration Console.

Note   CIP Security IACS devices must be discoverable by FactoryTalk Linx to apply and deploy CIP Security properties. FactoryTalk Linx Browser utility cannot be used to modify, enable, or disable the CIP Security properties on IACS devices. Use the FactoryTalk Policy Manager software to modify, enable, or disable CIP Security properties.

Step 2   Log in and navigate to FactoryTalk Policy Manager.

FactoryTalk Policy Manager Tool user accounts for login can be created in FactoryTalk Administration Console as FactoryTalk user or Windows-linked users. Specific access rights in FactoryTalk Policy Manager can be implemented in built-in security groups in FactoryTalk Administration Console.

Note   FactoryTalk Policy Manager must be able to connect to FactoryTalk System Services to log in successfully. If the error message `FactoryTalk System Services Cannot Be Reached` appears after launching FactoryTalk Policy Manager, it means FactoryTalk System Services is not running. Select EXIT POLICY MANAGER to close the error message.

To resolve this error, attempt to start FactoryTalk System Services.

- Go to the Windows Services snap-in (services.msc).
- In the services list, scroll down to the FactoryTalk System Services item.
- Right-click FactoryTalk System Services and select Start.

Table 3-2 provides a reference to the FactoryTalk Policy Manager navigation shown in Figure 3-3.

Table 3-2   FactoryTalk Policy Manager Navigation

Item	Description
1 (top main menu bar)	FactoryTalk Policy Manager top main menu bar. Displays the actions available for the items: • **Reload**—Reloading the model synchronizes FactoryTalk Policy Manager and FactoryTalk System Services and refreshes the display of possible conflicts so that they can be addressed before deployment. • **Deploy**—Deploys the security model to configured IACS devices. • **Logged on or logged off**—Used for user login or off. • **Help**—Online help includes overview, screen, and release notes for the product. The Help contains these basic components: Concepts, Procedures, and Properties referenced.
2 (left navigation bar)	FactoryTalk Policy Manager left navigation bar. Use this bar to move between the different components of the security model. Also use to access **Global Settings**.

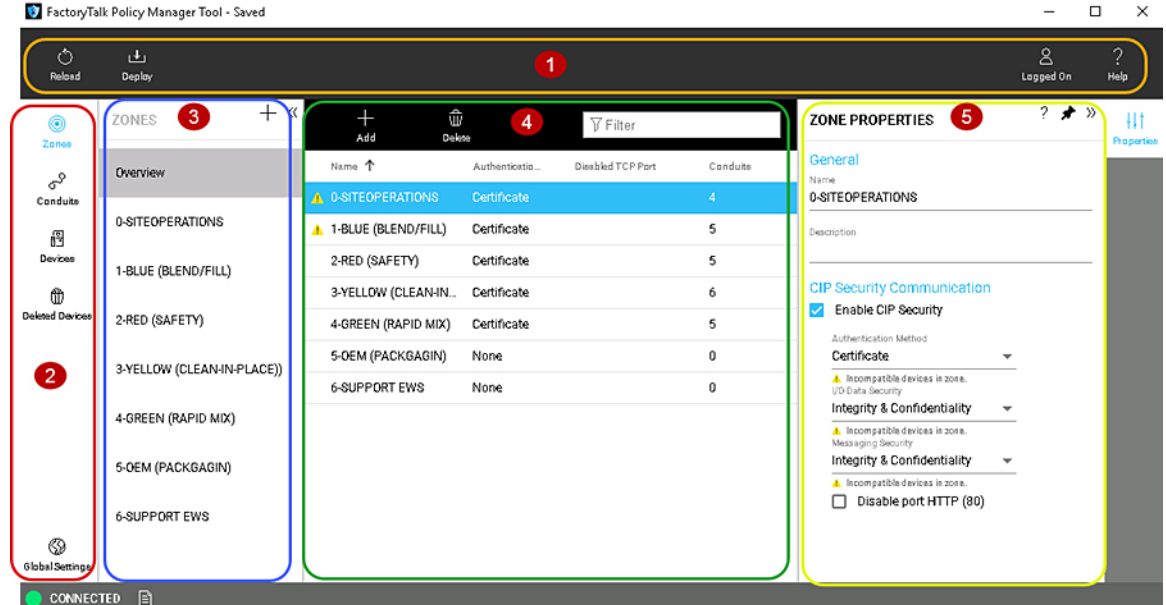Table 3-2   FactoryTalk Policy Manager Navigation (continued)

Item	Description
3 (left Zones list pane)	Displays the zones configured in the model. Select a zone to edit the devices in the zone. Use the Zones list to quickly edit zone properties or delete zones. **Note** The other components Devices, Conduits, and Deleted Devices do not have a separate list pane.
4 (center Content pane)	Displays the items that can be configured. Contains the FactoryTalk Policy Manager toolbar that contains the actions available for the items. Action items will vary between components. • **Add [+]**—Add a zone or conduit. • **Discover Devices**—IACS devices can be discovered by querying the network. • **Add Device [+]**—IACS devices can be added manually by catalog number or as a generic device. • **Add Range <…>**—A range (group) of IACS devices that are not CIP Security capable, can be incorporated into the security model using a trusted IP range. • **Replace Device**—Replace an IACS device. • **Delete**—Delete a zone, conduit, or IACS device. Actions that are not displayed on the toolbar can be viewed by clicking the More actions icon (vertical ellipsis).
5 (right Properties pane)	Properties panes are available for zones and devices, and automatically shows the port properties for the last device configured. For conduits properties panes, it will display the properties of the last conduit configured.

Figure 3-3   FactoryTalk Policy Manager Navigation


Step 3   Add Zones.

Zones identify a group of logical or physical IACS devices to which security settings are applied. IACS devices are added to zones.

Zones establish the rules for data integrity, data confidentially, and the authentication method used to authenticate trusted IACS devices. Once an IACS device is added to a zone, it will use the security properties configured on the zone for intra-zone communications with other IACS devices within that zone.

To add a zone to the security model follow the steps below (Figure 3-4)

1. The left navigation bar contains the components for selection, to select the Zones component, click Zones.

    – Zones component

    – Conduits component

    – Devices component

    – Deleted Devices component

2. Once the Zones component is selected, the left **ZONES** list pane will automatically appear and display an overview of the exiting zones. To create a Zone, click the + icon in the **ZONES** list pane. A new Zone 1 will appear under the **ZONES** list pane and the **ZONE PROPERTIES** pane will appear on the right side of the tool.

3. To configure or edit zones in the **ZONES** list, click to select the desired zone, then click the edit pencil icon in that zone.

4. The **ZONE PROPERTIES** pane will appear on the right side of the tool. Complete the configurations in the **ZONE PROPERTIES** pane according to the security requirements for intra-zone EtherNet/IP communications. See editable configuration fields in Table 3-3.

FactoryTalk Policy Manager Configuration

Figure 3-4   Add a Zone to the Security Model
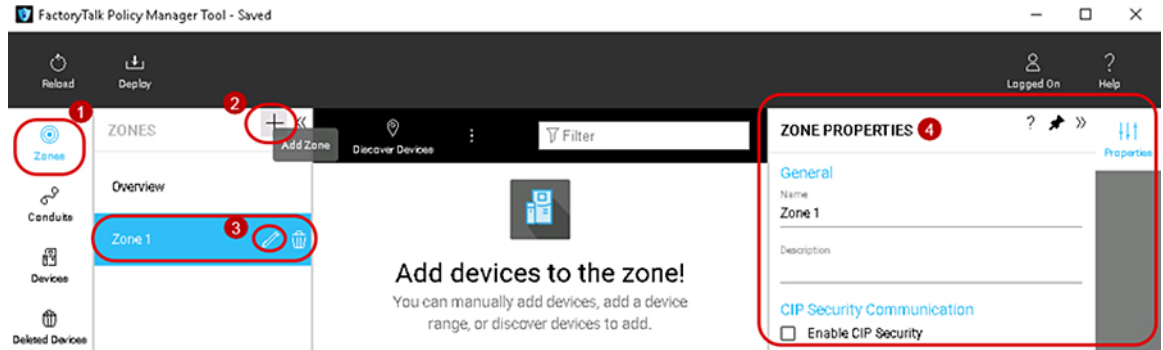
The ZONE PROPERTIES pane includes the editable configuration fields shown in Table 3-3.

Table 3-3   Zone Properties

Zone Property	Description
General area	The settings under the General area define the Name and Description of the zone.
Name	Assign a name to the zone.
	It is recommended to assign a human-readable functional name to the zones.
Description (Optional)	Description of the zone.
CIP Security Communication area	The settings under the CIP Security Communication area relate to how the devices within the same zone (intra-zone communication) communicate with each other.
Enable CIP Security checkbox	When the Enable CIP Security checkbox is selected, additional security configuration options become available for configuration for the selected zone.
(Optional)	The security configurations selected in this area will apply to all IACS devices and the EtherNet/IP communications established with one another in the selected zone (intra-zone communication).
	Note: Non-CIP Security capable IACS devices can be added to a zone with CIP Security enabled. These IACS devices will have a yellow triangle information icon displayed next to them in the center Content pane and the same icon stating *Incompatible devices with zone* beneath each security configuration option. These IACS devices will not receive CIP Security policy themselves, but the CIP Security capable IACS devices will implicitly add the IP address of the non-CIP Security capable IACS devices to their Trusted IP list, so that communication between the IACS devices can occur. ⚠️ *Incompatible devices in zone*.

Table 3-3   Zone Properties (continued)

Zone Property	Description
Authentication Method security configuration (drop down)	Select how the zone verifies the identity of assigned IACS devices in that zone. The options allowed for this field are in bold. **Certificate** A digital certificate is an electronic representation of an identity. A certificate binds the identities public key to its identifiable information, such as name, organization, email, username, and/or a device serial number. If selected, a certificate will be used by IACS devices in the zone to authenticate with one another. Certificate is selected by default when CIP Security is enabled. **Pre-shared Key** A pre-shared key is a secret that is shared among trusted entities. FactoryTalk Policy Manager can create a key that can be shared among IACS devices in the selected zone. • To generate a pre-shared key, select **Auto-generate key**. • To view the key, select **Show Key**. **Note:** Non-CIP Security capable devices do not use any authentication method. If non-CIP Security capable devices are present in a zone when Certificate or Pre-shared Key is selected, a yellow triangle information icon stating *Incompatible devices with zone* will be displayed beneath the Authentication Method option. ⚠ *Incompatible devices in zone.*
I/O Data Security configuration (drop down)	Select the type of security check to perform on the input and output data or Class 0/1 data. The options allowed for this field are in bold. **Integrity Only** Checks whether data was altered and whether the data was sent by a trusted entity. Altered and/or untrusted data is rejected. Selected by default when CIP Security is enabled. **Integrity & Confidentiality** Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data. **None** No I/O Data Security is selected. Even when no I/O Data security is configured, only defined IACS devices within the zone or from an explicitly configured conduit are capable of establishing I/O data communications with those IACS devices. Other IACS devices not in the same zone or explicitly configured with a conduit will be blocked. **Note:** Non-CIP Security capable IACS devices do not use any I/O Data Security method. If non-CIP Security capable IACS devices are present in a zone, a yellow triangle information icon stating *Incompatible devices with zone* will be displayed beneath the I/O Data Security option. ⚠ *Incompatible devices in zone.*

Table 3-3   Zone Properties (continued)

Zone Property	Description
Messaging Security configuration (drop down)	Select the type of security check to perform on messages Class 3 data. The options allowed for this field are in bold. **Integrity Only** Checks whether data was altered and whether the data was sent by a trusted entity. Rejects altered and/or untrusted data. Selected by default when CIP Security is enabled. **Integrity & Confidentiality** Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data. **Note:** Non-CIP Security capable IACS devices do not use any Messaging Security and cannot provide data integrity checking. If non-CIP Security capable IACS devices are present in a zone, a yellow triangle information icon stating *Incompatible devices with zone* will be displayed beneath Messaging Security option. ⚠ *Incompatible devices in zone*.
Disable port HTTP (80) checkbox (Optional)	When the Disable port HTTP (80) checkbox is selected, the web browser for CIP Security capable IACS devices in the selected zone will become disabled. Disabling the port HTTP (80) at the zone level will allow a quick and easy way to disable for all group of IACS devices. For granularity, Disable port HTTP (80) checkbox is also offered in the PORT PROPERTIES. This will allow the web browser to be disabled for an individual IACS device instead for all IACS devices in the zone. **Note:** Non-CIP Security IACS capable devices cannot disable the web browser port HTTP (80). If non-CIP Security capable IACS devices are present in a zone, a yellow triangle information icon stating *Incompatible devices with zone* will be displayed beneath Disable port HTTP (80) option when selected. ⚠ *Incompatible devices in zone*.

Step 4   Add devices.

IACS devices are the modules, drives, controllers, HMI panels, computers, and servers that work together to create a FactoryTalk system. They can be added to the security model in the Zones component or the Devices component. They can also be added manually or discovered by querying the network.

IACS devices added directly into a Zones component and will comply with security properties configured for the zone in the **ZONE PROPERTIES** pane. When added directly into the Devices component, they will be initially unassigned but can be easily moved to a zone using the **PORT PROPERTIES** pane.

Note   To add IACS devices using the **Discover Devices** button, the CIP Security IACS devices must be discoverable by FactoryTalk Linx.

To add a Discovered Device to a Zones component in the security model follow the steps below (Figure 3-5).

1. In the FactoryTalk Policy Manager left navigation bar, click **Zones** to select the Zones component.

2. Once the Zones component is selected, the left **ZONES** list pane will appear and display an overview of the exiting zones. Click the desired zone in the **ZONES** list pane.

3. Click the **Discover Devices** button in the center Content pane, to open the **Discover Devices** window with FactoryTalk Linx.

   Use the **Discover Devices** button to traverse the FactoryTalk system and find IACS devices. Discovery can be useful for populating a list of devices or for checking that the devices added to the list manually are accurately identified.

4. To select multiple IACS devices in the **Discover Devices** window, click to select a device then **hold down the SHIFT key** and click to select more IACS devices.

5. Once one or more desired IACS devices are selected, the **ADD** button will become enabled and add those devices to the desired zone.

Figure 3-5   Add an IACS Device to a Zone Using the Discovered Device Feature
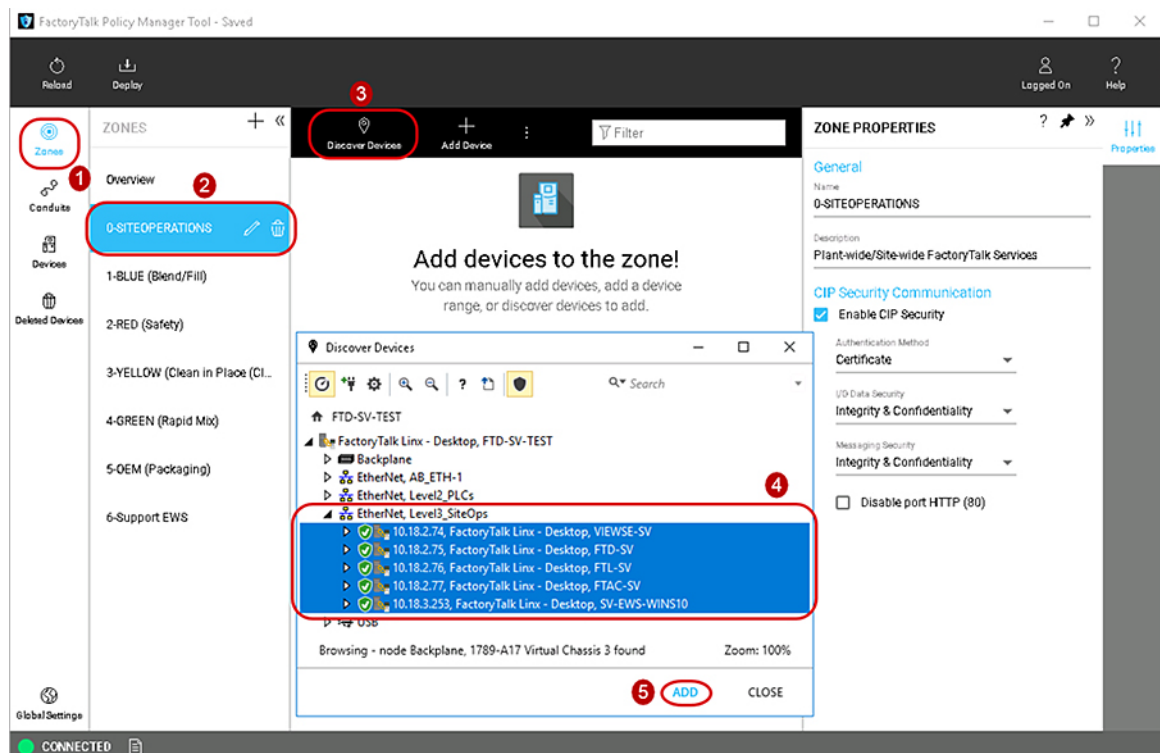
To manually add an IACS device to the Devices component in the security model follow the steps below (Figure 3-6)

1. In the FactoryTalk Policy Manager left navigation bar, click **Devices** to select the Devices component.

2. Click the **Add Device** [+] button located in the center Content pane, to open the **Select Catalog Number** window.

   Use the **Add Device** [+] button to manually add an IACS device to the current Devices component by selecting **Generic Device** or the catalog number of an IACS device. IACS devices added using the manual method requires the computer hosting FactoryTalk Policy Manager. This will achieve successful communications to the manually added IACS device.

3. In the **Select Catalog Number** window, select either **Generic Device** or the catalog number of an IACS device.

   The **Generic Device** allows for adding IACS devices such as computers Windows Server 2016 hosting the networking management software FactoryTalk Network Manager.

4. Once the desired IACS device has been selected, click **OK**.

The **Select Catalog Number** window will only allow the selection of one IACS device. If more IACS devices are required to be manually added, repeat steps 1-4 of this section.

Figure 3-6   Manually Add an IACS Device to Devices Component
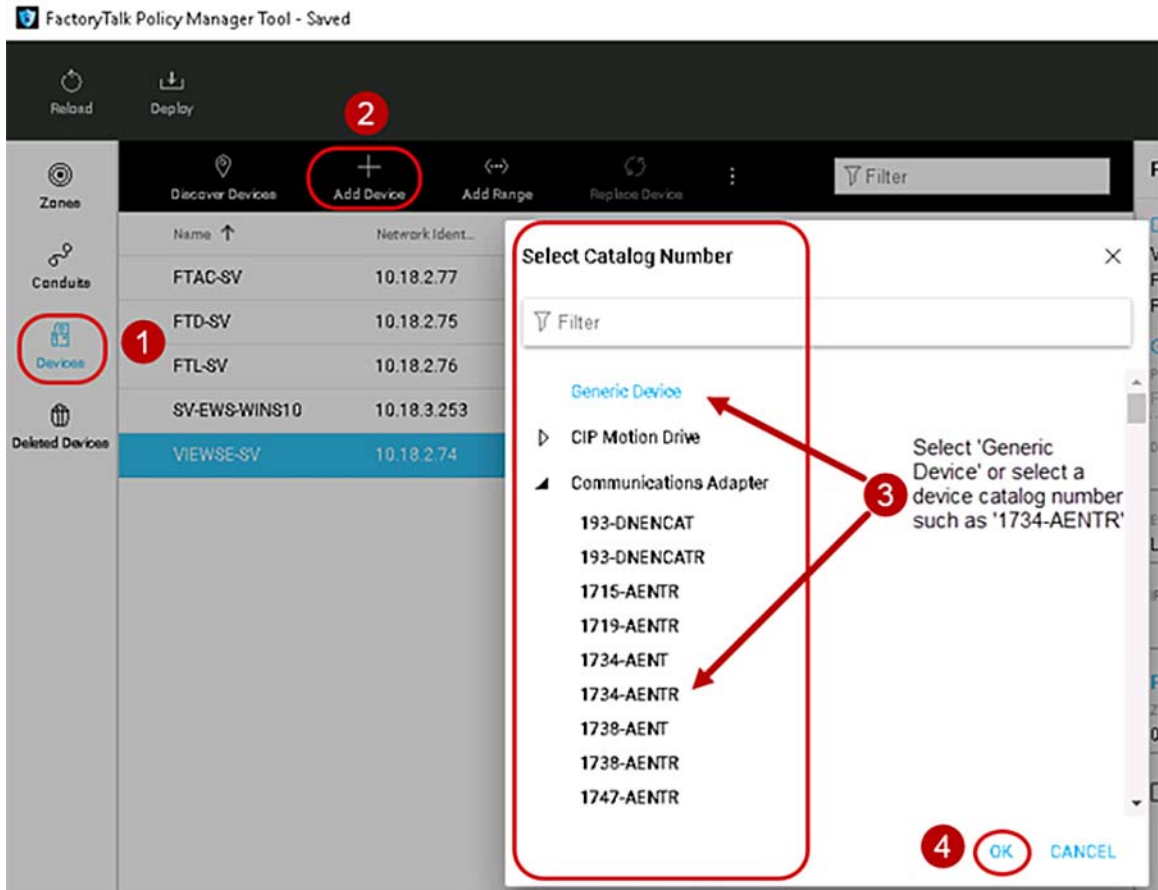

Step 5   Verify and update the Device Properties.

1. The first time a device is added using either methods discovered or manually added to the Zones or Devices components, the **DEVICE PROPERTIES** pane will automatically appear on the right-hand side of the tool (Figure 3-7).

2. The **DEVICE PROPERTIES** pane will always appear on the right side of the tool and is used to add/edit pertinent information about the IACS device. See editable configuration fields in Table 3-4.

✎

Note   If an administrator navigates away to another component or IACS device, then reselects the desired IACS device in the center **Content** pane, it will now automatically appear in the **PORT PROPERTIES** to the right of the tool instead of the **DEVICE PROPERTIES**. The administrator can easily bring up the **DEVICE PROPERTIES** pane by selecting the pencil icon next to the **Device** field in the **PORT PROPERTIES** pane (Figure 3-8).

Figure 3-7   Device Properties in FactoryTalk Policy Manager
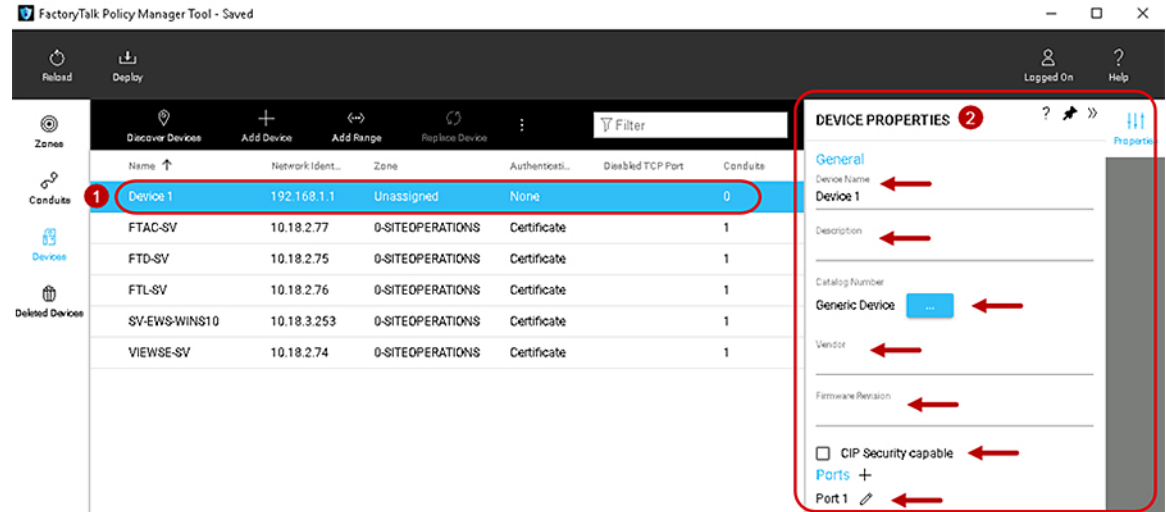
The DEVICE PROPERTIES pane includes the editable configuration fields shown in Table 3-4.

Table 3-4   Device Properties

Device Property	Description
General area	The settings under the General area define the Device Name and Description of the IACS device.
Device Name	Assigns a Name to the IACS device.
	Note: The selection of Generic devices are automatically named **Device <*number*>**. IACS devices selected by catalog number will appear with the catalog number. IACS devices that are discovered will appear with the Device Name as it appears in the FactoryTalk Linx. In all three cases the Device Name field can be edited to by the administrator.
Description (Optional)	Description of the IACS device.
	Note: The selection of Generic devices descriptions are blank. IACS devices selected by catalog number or discovered may have an existing description. In all three cases the Description field can be edited to by the administrator.
Catalog Number	Opens the **Select Catalog Number** window by selecting the ellipsis [...] and choosing the catalog number for the IACS device from the list.
	Note: The selection of Generic devices are automatically given the Catalog Number of Generic Device. IACS devices selected by catalog number will appear with the catalog number. Devices that are discovered will appear with the catalog number as it appears in the FactoryTalk Linx. This is not a free-form field and can only be the **Select Catalog Number** window.

Table 3-4   Device Properties (continued)

Device Property	Description
Vendor (Optional)	Name of the IACS device manufacturer **Note:** If a Rockwell Automation catalog number was provided, this setting is completed by default and cannot be modified.
Firmware Revision (Optional)	Choose the applicable firmware revision. **Note:** If a Rockwell Automation catalog number was provided, this setting is completed by default and will provide a drop-down of available firmware revision numbers for modification.
CIP Security capable checkbox (Optional)	Enable CIP Security capable if the IACS device supports CIP Security. **Note:** CIP Security is associated with the Catalog Number and Firmware Revision properties. When both values are known the CIP Security capable setting is automatically enabled or disabled and cannot be modified.
Ports	Select the pencil icon next to **Ports** to toggle back to the **PORT PROPERTIES** pane to configure port properties, such as the port name, description, IP address, and zone assignment.

Step 6   Verify and Update the Port Properties.

A port represents a physical socket of an IACS device that allows communication with another IACS device using CIP Security. FactoryTalk Linx and IACS devices identified by catalog number have only a single port associated with IP addresses, ports, and protocols. IACS devices that have a specific catalog number have a predefined number of ports with assigned protocols. If an IACS device does not have a catalog number FactoryTalk Policy Manager adds it as a Generic Device. When a security policy model includes generic devices, configure the number of ports on the IACS device.

1. Whether devices were discovered or manually added to the Zones or Devices components, the **PORT PROPERTIES** pane can be accessed by clicking and selecting the device in the center **Content** pane. (Figure 3-8).

2. The **PORT PROPERTIES** pane will always appear on the right side of FactoryTalk Policy Manager and is used to add pertinent information about the IACS device. See editable configuration fields in Table 3-5.

Figure 3-8   Port Properties in FactoryTalk Policy Manager
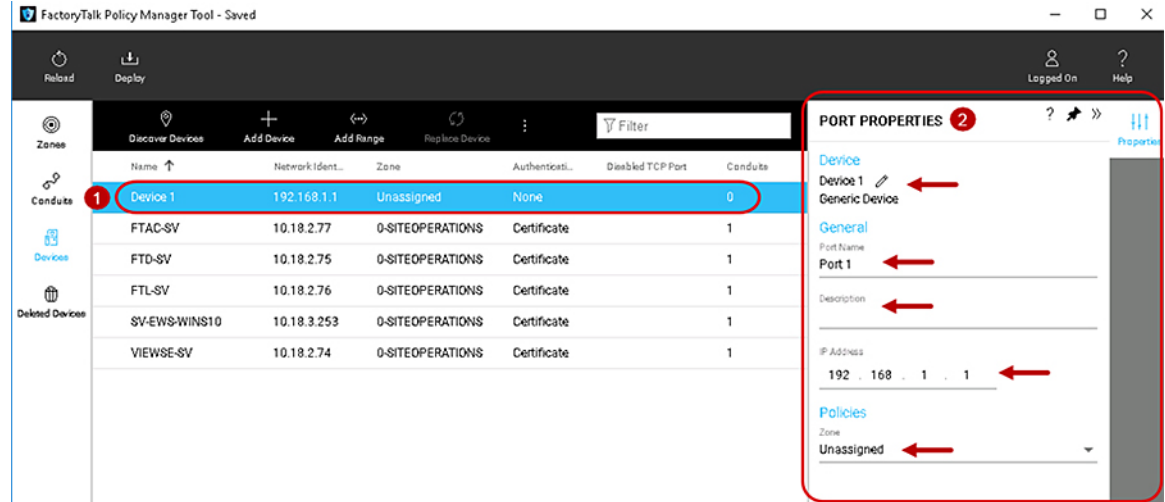
The PORT PROPERTIES pane includes the editable configuration fields shown in Table 3-5.

Table 3-5   Port Properties

Port Property	Description
Device	Select the pencil icon next to **Device** to toggle back to the **DEVICE PROPERTIES** pane to configure IACS device properties, such as the device name, description, vendor, catalog number, and to enable CIP Security on the IACS device.
General area	The settings under the General area relate to network port properties for the selected IACS device.
Port Name	If the IACS device was added as a Generic Device, edit the port name by selecting the Port Name field and typing a new name.
	If the IACS device was added with the Catalog Number or Discovered Devices button, the Port Name field is automatically populated with Port 1 and cannot be modified.
Description (Optional)	Type a description of the port.
EtherNet Driver Name **Note:** This field only appears for CIP Security capable IACS devices.	Type the name of the EtherNet driver for the device. The name of the Ethernet driver used for communications. Example: AB-ETH-1 **Note:** The default EtherNet Driver name is added through discovery of an associated EtherNet driver in FactoryTalk Linx but can be modified by an administrator.
IP Address	Enter the IP address of the IACS device. The IP address of the Ethernet port.
Policies area	The settings under the Policies area relate to security port properties for the selected IACS device.

Table 3-5   Port Properties (continued)

Port Property	Description
Zone	The Zone drop-down field will display the name of the zone to which the port is assigned. The drop-down allows reassigning the port to any of the zones created in the Zones component and Unassigned. **Note:** Selecting the Unassigned from the Zones drop-down field will remove the selected port from the zone it was previously assigned to as well as the CIP Security properties: Authentication Method, I/O Data Security, and Messaging Security.
Disable port HTTP (80) checkbox (Optional) **Note:** This field only appears for CIP Security capable IACS devices.	When the Disable port HTTP (80) checkbox is selected, the web browser for CIP Security capable IACS devices will become disabled. **Note:** If the Disable port HTTP (80) checkbox is checked and grayed out, then the IACS device has been assigned to a zone that already has the Disable port HTTP (80) checkbox checked and enabled.

Step 7   Add Conduits.

Conduits create trusted communication pathways outside of zones. Conduits require two endpoints, such as:

- Two different zones for a zone to zone conduit.
- Two IACS from different zones for a device to device conduit.
- A zone and an IACS device from another zone for a zone to device conduit.

Endpoints can be either a zone or an IACS device. Conduits must adhere to these rules:

- Each combination of endpoints must be unique.
- Duplicate conduits are not permitted.
- One of the endpoints must be CIP Security capable.
- If one endpoint is a zone, the other endpoint cannot be a device within that zone.

Conduits support two authentication methods:

- Trusted IP—Assigns a trust relationship to an asset based on its IP address.
- Certificate—Establishes the identity of the IACS device by using a certificate from a trusted authority. This enables configuration of integrity and confidentiality options for communication over the conduit using the public key associated with the certificate.

Note Non-CIP Security capable IACS devices can be added to a zone with CIP Security enabled. These IACS devices will have a yellow triangle information icon displayed next to them in the center Content pane. These IACS devices will not be able to use certificate for communication for the conduits. When a conduit is created for the zone to another zone with the authentication method of certificate, the CIP Security capable IACS devices will implicitly trust the non-CIP Security capable IACS devices using Trusted IP.

To add a conduit in the security model, follow the steps below (Figure 3-9).

1. The left navigation bar contains the components for selection. To select the Conduits component, click **Conduits**.

- Zones component

- Conduits component

- Devices component

- Deleted Devices component

2. Once the Conduits component is selected, the center **Content** pane will display a toolbar that contains the actions available and an overview of the Conduits concepts. To create a conduit, click the **Add** [+] icon in the center **Content** pane toolbar.

3. The **CONDUIT PROPERTIES** pane will appear on the right side of the tool.

4. In the **CONDUIT PROPERTIES** pane, configure or edit **Endpoint 1** for the conduit by selecting the first **Select an endpoint** field ellipsis [...].

5. The **Select Endpoint** window will appear.

6. Select either a zone or expand a zone to select an IACS device as the first endpoint of the conduit.

7. Once the desired endpoint is selected, the OK button will become enabled. Click **OK**.

8. Return to the **CONDUIT PROPERTIES** pane, configure or edit Endpoint 2 for the conduit by selecting the second **Select an endpoint** field ellipsis [...], and perform the same steps in 6 and 7 to select a second endpoint of the conduit. Remember to adhere to the conduit rules when selecting the second endpoint.

9. Complete the endpoint configuration for Conduit 1 in the **CONDUIT PROPERTIES** pane by clicking **NEXT**.

10. Once the endpoints have been configured, the conduit CIP Security Communication area will appear in the **CONDUIT PROPERTIES** pane (Figure 3-10). CIP Security Communication area will have the configuration options for how endpoints will apply security for communication in the conduit. See editable configuration fields in Table 3-6.

FactoryTalk Policy Manager Configuration

Figure 3-9   Add a Conduit to the Security Model
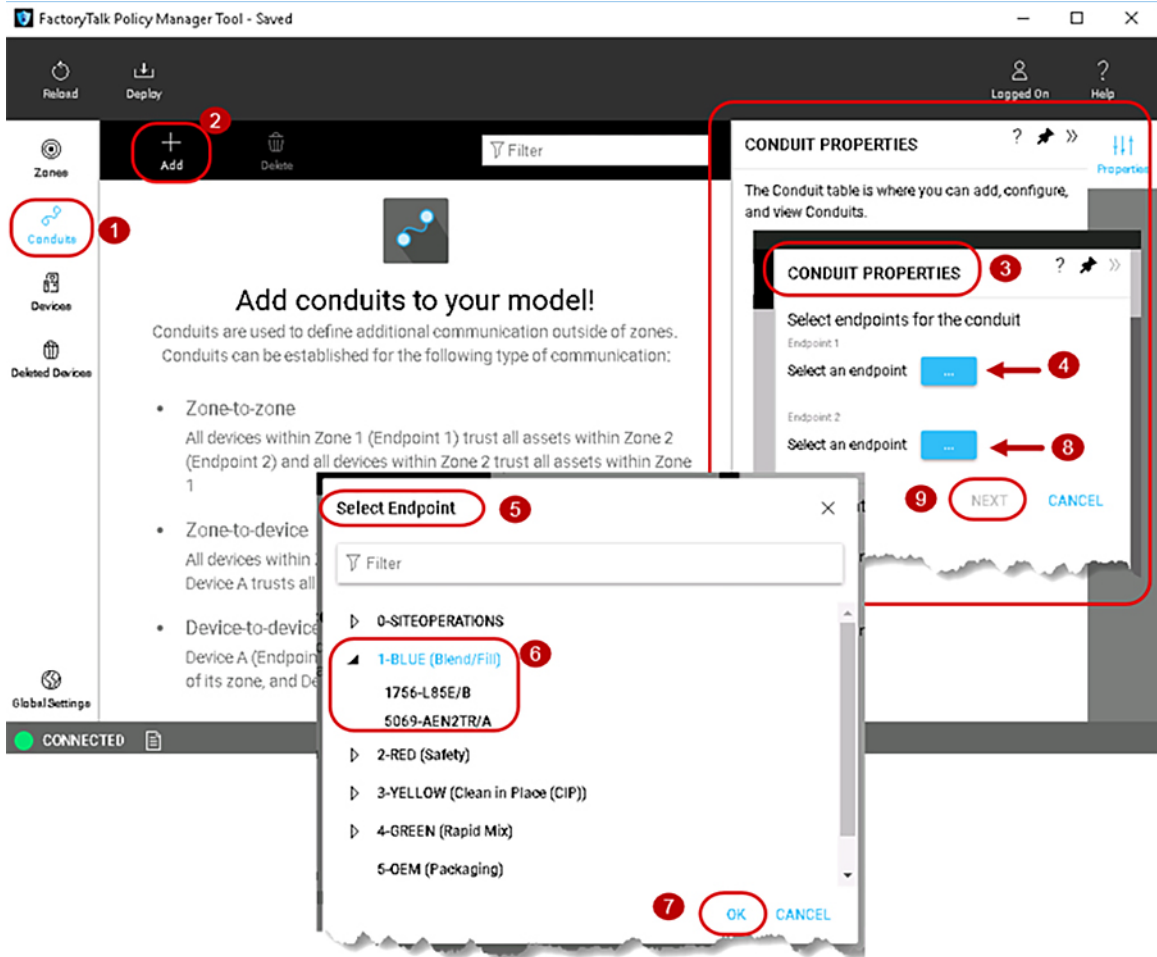
Figure 3-10   Conduit Properties in the Security Model
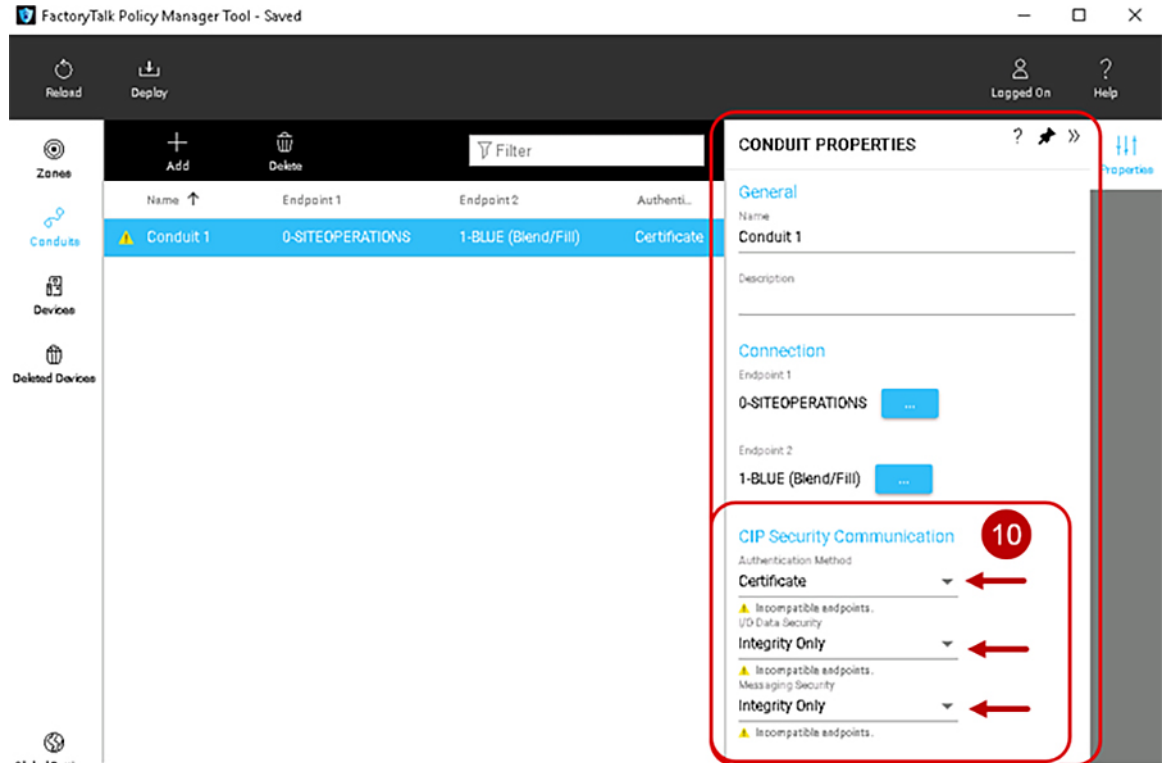
Table 3-6   Conduit Properties

Conduit Property	Description
General area	The settings under the General area relate to network port properties for the selected IACS device.
Name	Name for the conduit.
Description (Optional)	Description for the conduit.
Connection area	The settings under the Connection area allow for endpoint selection.
Endpoint 1	The first endpoint of the conduit.
Endpoint 2	The second endpoint of the conduit.
CIP Security Communication	The settings under the CIP Security Communication area relate to how the defined endpoints (inter-zone communication) communicate with each other.

Table 3-6   Conduit Properties (continued)

Conduit Property	Description
Authentication Method security configuration (drop down option)	Select how the endpoint1 verifies the identity of endpoint2. The options allowed for this field are in bold. **Trusted IP** IACS devices and zones are trusted for communications based on their IP address. No additional security checks are performed. **Certificate** A digital certificate is an electronic representation of an identity. IACS devices and zones are trusted by presenting a certificate that establishes their identity. With the certificate setting selected, configure the I/O Data Security and Messaging Security settings. **Note:** Pre-shared Key is not an option because IACS devices can only ever have one PSK configured. As a result, any conduits required between zones (inter-zone communication) configured with a pre-shared key can only use Trusted IP.

Table 3-6   Conduit Properties (continued)

Conduit Property	Description
I/O Data Security configuration (drop down option)	Select the type of security check to perform on the input and output data or Class 0/1 data. The options allowed for this field are in bold. **Integrity Only** This option checks if the data was altered. If detected, rejects altered data. **Integrity & Confidentiality** Checks integrity and encrypts the data so the corresponding decryption key is required to read the data. Rejects altered and/or untrusted data. **None** With this option, no security checks are performed on input and output data. **Note:** Non-CIP Security capable IACS devices do not use any I/O Data Security method. If non-CIP Security capable IACS devices are present in a zone, a yellow triangle information icon stating *Incompatible devices with zone* will be displayed beneath the I/O Data Security option. ⚠️ *Incompatible devices in zone.*
Messaging Security configuration (drop down option)	Select the type of security check to perform on messages Class 3 data. The options allowed for this field are in bold. **Integrity Only** This option checks if the data in the message was altered. If detected, rejects altered data. **Integrity & Confidentiality** This option checks if the data in the message was altered and that the message was sent by a trusted entity. Rejects the data if it was altered or if it originated from an untrusted entity. **Note:** Non-CIP Security capable IACS devices do not use any Messaging Security and cannot provide data integrity checking. If non-CIP Security capable IACS devices are present in a zone, a yellow triangle information icon stating *Incompatible devices with zone* will be displayed beneath Messaging Security option. ⚠️ *Incompatible devices in zone.*

Step 8   Deploy security model.

After the zones, conduits, and devices have been configured, the security policy model can be deployed. It is recommended to schedule downtime or maintenance window when deploying a CIP Security model to an IACS network. Before a deployed security policy becomes active, communications must be reset on configured IACS devices, resulting in a short loss of connectivity. The schedule downtime or maintenance window will also allow time for any troubleshooting if needed.

Before deploying a security model, make sure that all devices are operational and have network access.

There are two deployment options for security policy model deployment:

- **During deployment**—Option of resetting the communication as part of deployment.

  When this option is selected, the communication port will be closed and reopened on the IACS device during the deployment process. Similar to resetting the network card on a computer, the IACS device stays functional but is disconnected from the network for a few moments. Using this option applies the new policy to the IACS device and deploys it simultaneously.

- **After deployment**—Deploying the changes without resetting the communication channel so that the reset can occur at another time than the deployment process.

  When this option is selected, the security policy settings will be deployed to the IACS device but are not in effect. The communications ports must be reset before the security policy will be used. This option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function.

Once the model is deployed and communications reset on IACS devices, those IACS devices will only accept communications from other IACS devices in the same zone or using conduits configured to enable communications with other security zones or devices.

If changes are made to the security model in FactoryTalk Policy Manager after it is deployed, an asterisk (*) will appear next to the IACS device, indicating that the configured policy has not been deployed to that IACS device.

To deploy the security model, use the following steps (Figure 3-11)

1. In the FactoryTalk Policy Manager top main menu bar, click **Deploy**.

2. In the **Deploy** window that appears, under the section **Choose when to reset device communication ports included in this model:** make a deployment selection:

   – **During deployment**—Immediate resetting of the IACS device(s) communication ports as part of deployment.

   – **After deployment**—No resetting of one or more IACS devices communication ports at the time of the deployment. The security policy settings will be deployed to the IACS device but are not in effect until the communications ports are reset on the IACS device.

Note   Before a deployed security policy becomes active, communications must be reset on the port of the configured IACS devices.

3. Once a deployment method has been selected, the **DEPLOY** button will become enabled for selection. Click the **DEPLOY** button.

Figure 3-11   Deploy the Security Model
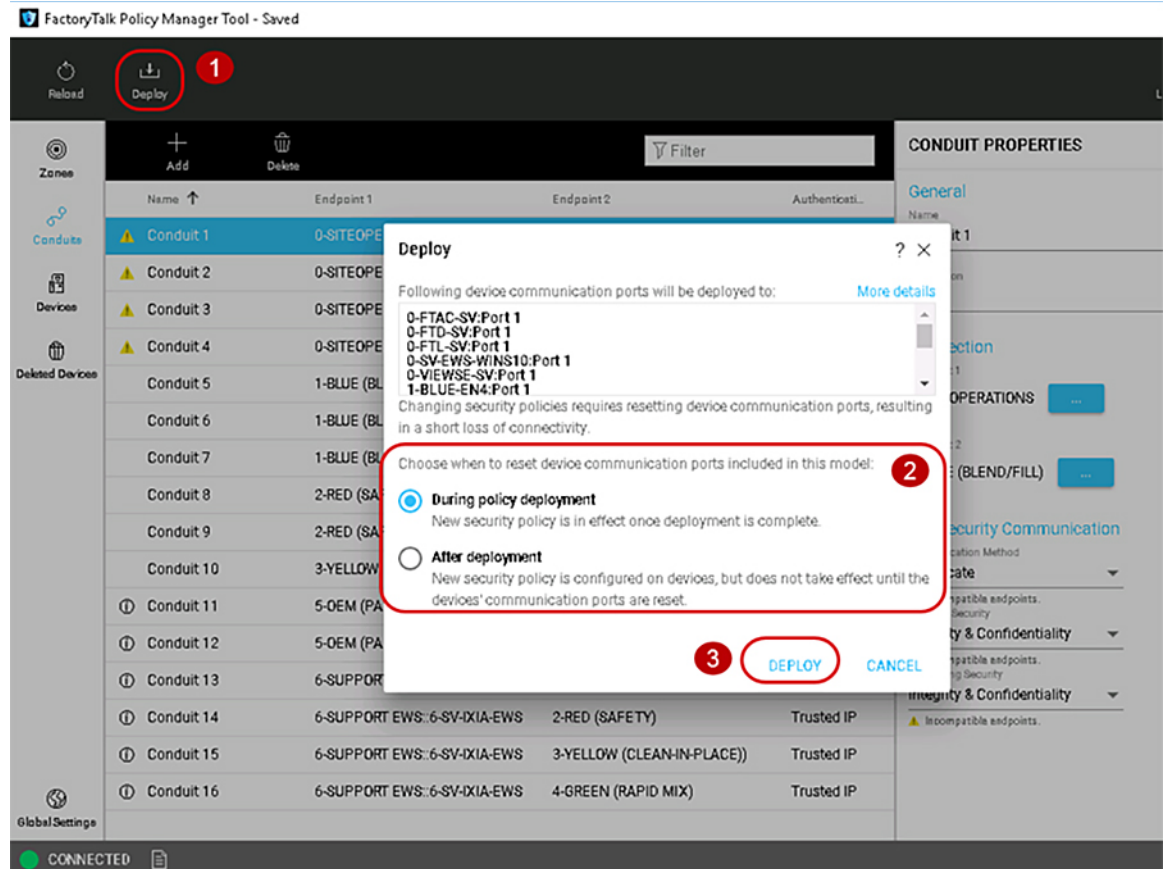
The deployment process may take several minutes to complete depending on the size of the network. Once deployment is complete a summary report is provided listing the successes, failures, and errors encountered during the process.

Warning   If the deployment process is interrupted or stopped during deploy, this can leave the system in an unexpected state. Communications between IACS devices could be permanently interrupted requiring module factory reset.

See the **Results** pane for displayed updates with the results of the deployment as it occurs and complete a summary report (Figure 3-12).

1. The **Results** pane will automatically appear after **DEPLOY** has been selected.

2. If the **Results** pane does not appear, at the bottom of the tool next to the **CONNECTED**, press the paper icon to bring up the **Results** pane.

3. In the body of the **Results** pane, review the result of the deployment on each item in the model. The possible results are:

   – Configuration complete. No issues identified.

   – Configuration complete. Warnings identified.

   – Configuration not complete. Error identified.

4. Select the save icon to save the **Results** pane output for reference, reporting, or other record keeping requirements.

5.   Select the down arrow icon to minimize the **Results** pane.

Figure 3-12   Results of the Deployment of the Security Model
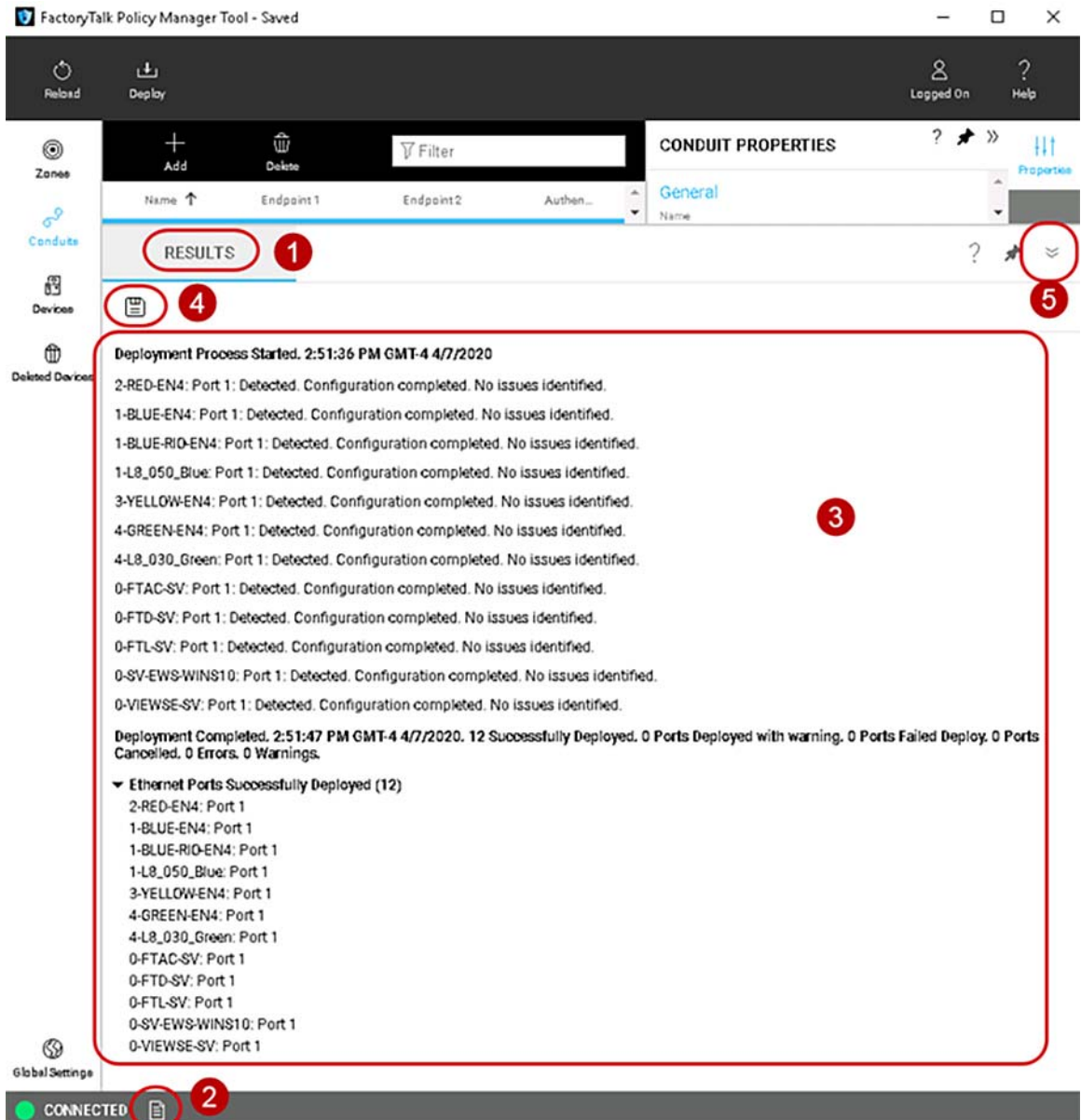
Removing the CIP Security Policy from an IACS Device

If the security model has been deployed and the IACS device communications have been reset the IACS device is constrained by the security policy. Deleting the IACS device from the model does not remove the security configuration. Even if FactoryTalk Policy Manager and FactoryTalk System Services are uninstalled, the security policy configured for the IACS device is still in effect.

To remove CIP Security properties from an IACS device, use the **PORT PROPERTIES** pane in the security model and follow the steps below (Figure 3-13). The steps described in this section are the recommended method to remove any CIP Security configurations on an IACS device. It also assumes the CIP Security enabled IACS device still has successful communications with the computer hosting FactoryTalk Policy Manager and FactoryTalk System Services.

1. The **PORT PROPERTIES** pane can be accessed in either the **Zones** or **Devices** components.

2. Select the desired IACS device for removing of CIP Security properties by clicking the IACS device from the center **Content** pane.

3. The **PORT PROPERTIES** pane will appear on the right side of FactoryTalk Policy Manager. The settings under the **Policies** area in the **Zone** drop-down field will display the name of the current zone to which the IACS device port is assigned. In the drop-down reassign the port to **Unassigned**. Selecting the **Unassigned** from the **Zones** drop down field will remove the selected port from the zone it was previously assigned to as well as the CIP Security properties: Authentication Method, I/O Data Security, and Messaging Security.

4. In the FactoryTalk Policy Manager top main menu bar, click **Deploy**.

5. (Optional) The **Deploy** window will appear. Select the **More details** link to view the **Deployment Details** popup window.

   The **Deployment Details** window will verify one or more IACS devices and the new CIP Security properties that will be set on the next deployment of the security model. Click **CLOSE** to go exit the **Deployment Details** window (Figure 3-14).

6. In the **Deploy** window that appears, under the section **Choose when to reset device communication ports included in this model:** make a deployment selection:
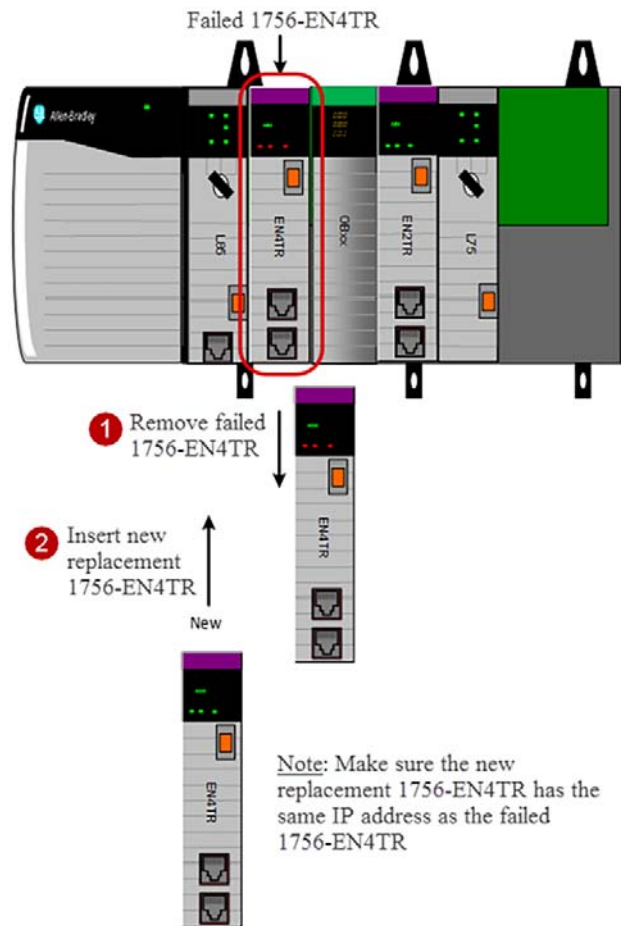
   – **During deployment**—Immediate resetting of one or more IACS devices communication ports as part of deployment.

   – **After deployment**—No resetting of the IACS device(s) communication ports at the time of the deployment. The security policy settings will be deployed to the IACS device but are not in effect until the communications ports are reset on the IACS device.

7. Click the **DEPLOY** button to start the deployment.

Verify in the **Results** pane for a successful deployment of all IACS device ports.

FactoryTalk Policy Manager Configuration

Figure 3-13   Remove the CIP Security Policy from an IACS Device
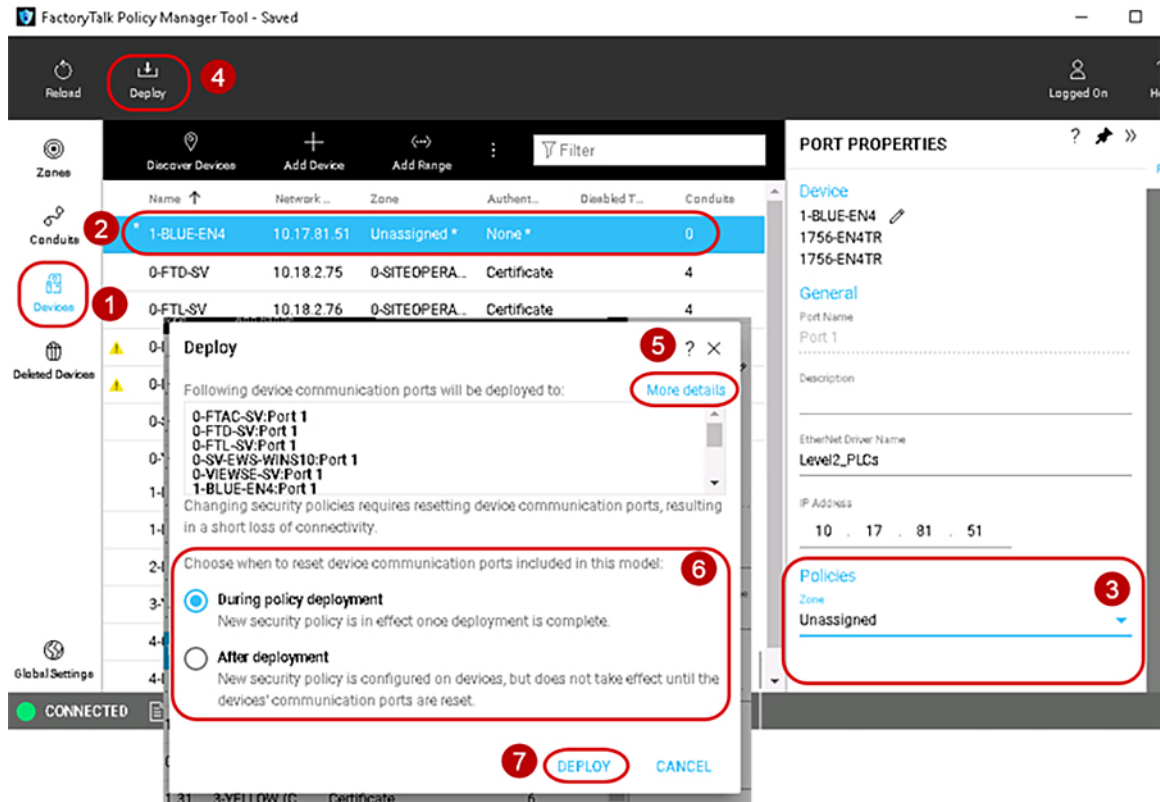
Figure 3-14   Deployment Details Window

If the CIP Security enabled IACS device can no longer communicate with the computer hosting FactoryTalk Policy Manager and FactoryTalk System Services use the following methods:

- Use the FactoryTalk Administration Console to remove the CIP Security policy configuration from FactoryTalk Linx, then return to FactoryTalk Policy Manager to delete the device with FactoryTalk Linx and redeploy the model to the other IACS devices to update their trust models. Figure 3-15 details the steps:

1. Open the **FactoryTalk Administration Console** application and make sure the **Explorer** pane is visible.

2. At the bottom of the **Explorer** pane, click **Communications** tab.

3. Right click the top instance **FactoryTalk Linx - Desktop, <computer name>** and select **Properties** from the menu.

4. The **Device Properties** window will appear. Select the **CIP Security** tab.

5. Select the **Reset CIP Security** button. A popup window will appear to confirm.

6. Click **OK** on the **Device Properties** window to close.

- For the 1756-EN4TR and the 1756-L85E, use the factory reset method documented in the user manuals found in Additional Resources in Chapter 2, "CPwE CIP Security Design Considerations."

Figure 3-15   FactoryTalk Administration Console Removal of CIP Security
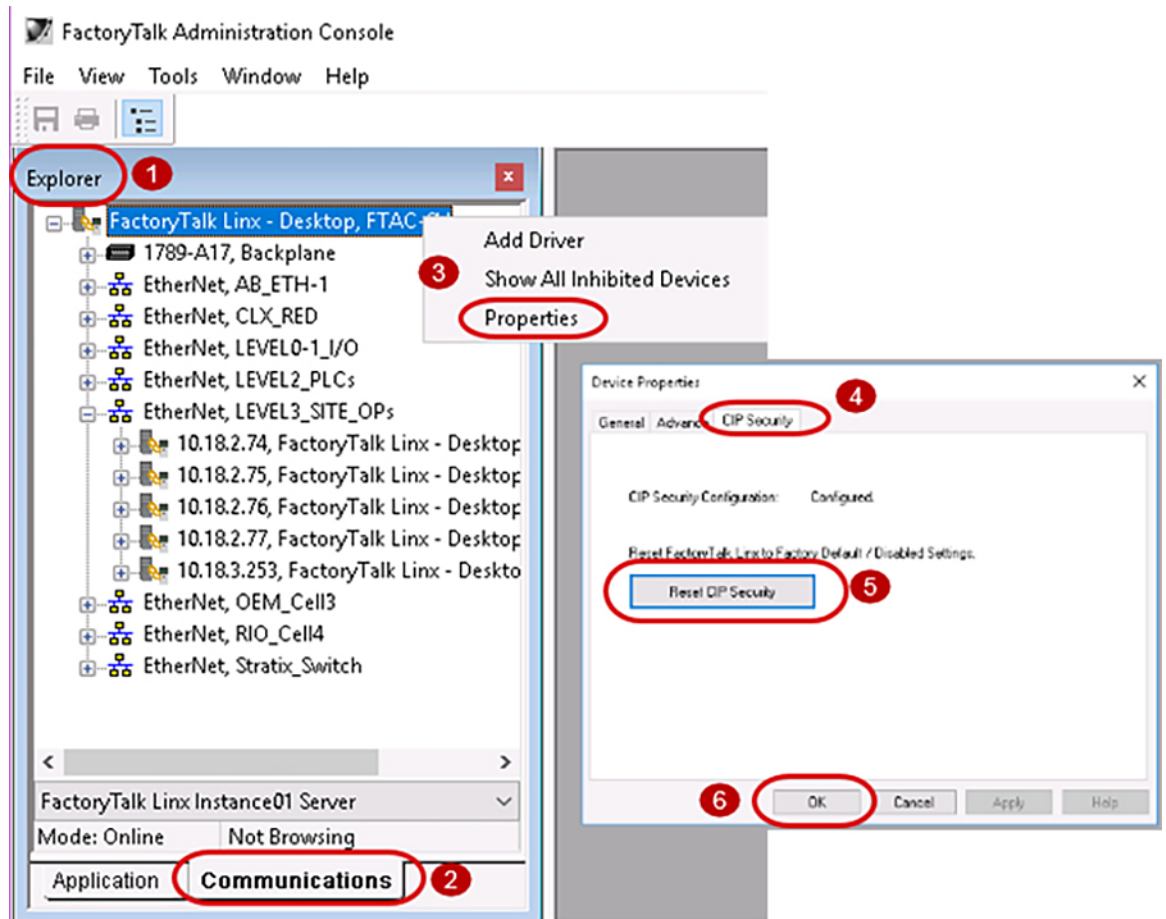
Replacing an IACS Device in the Security Model

Replacing an IACS device is used when an IACS device that has already been configured and enabled for CIP Security has failed or needs to be rotated out for maintenance. Device replacement button enables the identity and the security configuration of the previous device to be assigned to the replacement IACS device. The communications port on an IACS device must be reset after replacement to apply the security policy settings.

To replace an IACS device, use the **Replace Device (↻)** button in the security model. Follow the steps below (Figure 3-16):

1. Physically remove the failed IACS device from the network.

2. Physically insert the new replacement IACS device into the network.

   Make sure the new replaced IACS device has the same IP address as the failed IACS device.

3. In the FactoryTalk Policy Manager too, the **Replace Device (↻)** button can be accessed in either the **Zones** or **Devices** components.

4. In the **Zones** component, select the Zone in which the failed IACS device resides.

5. Select the desired IACS device for replacement by clicking the IACS device from the center **Content** pane.

6. In the center **Content** pane toolbar, click the **Replace Device (↻)** button.

7. In the FactoryTalk Policy Manager top main menu bar, click the **Deploy** button.

8. The **Deploy Configuration to Replaced Device** window will display a list of device communication ports that will also be updated to trust replaced device.

   (Optional) Select the **View full details of deployed security configuration** link to view details of device communication ports that will be updated to trust the replaced device popup window.

9. In the **Deploy Configuration to Replaced Device** window under the section **Choose when to reset device communication ports included in this model:** make a deployment selection:

   During deployment—Immediate resetting of the IACS devices communication ports as part of deployment.

   After deployment—No resetting of the IACS devices communication ports at the time of the deployment. The security policy settings will be deployed to the IACS device but are not in effect until the communications ports are reset on the IACS device.

10. Click the **DEPLOY** button to start the deployment.

Verify in the **Results** pane for a successful deployment of all IACS device ports.

Figure 3-16   Replace Failed IACS Device in Network

FactoryTalk Policy Manager Configuration

Verifying and Troubleshooting the Deployment

This chapter provides an overview of some of the verification and troubleshooting tools that can be used to complete the verification and any troubleshooting of the CIP Security deployment. It also provides a basic overview of Wireshark and webpages for the 1756-L8xE and 1756-EN4TR to help with basic verification and troubleshooting. However, it does not specifically prescribe action items as a result of the troubleshooting steps due to the fluidity of the deployment and potential architectural differences.

Web Browser Verification

Identify the TCP Connections

Many IACS devices have a webpage that display information about the module including the CIP connections established. This is a quick way to determine TCP connections between IACS before FactoryTalk Policy Manager deploys the security model. The webpages of the 1756-L8xE and 1756-EN4TR can help identify the initiator and responder of a CIP connection. This will help define conduits for protected EtherNet/IP communication in different zones. Any EtherNet/IP communication between zones must be through a defined conduit.

Note   The client/server terminology is commonly used with TCP and TLS/DTLS connections and originator/target for CIP connection. However, for simplicity of this document, the terms client/server will be generalized when discussing the behavior associated with a connection of an IACS device. The client initiates a connection and the server listens for and accepts a connection. For more details, see EtherNet/IP Overview in Chapter 2, "CPwE CIP Security Design Considerations."

The 1756-L8xE and 1756-EN4TR have a similar folder structure in the webpage navigation. The TCP Connections page, TLS Connections page, and the DTLS Connections page are provided in both the 1756-L8xE and 1756-EN4TR.

Figure 4-1 shows the webpage of the local 1756-EN4TR with IP Address 10.17.81.51 TCP connections before CIP Security deployment. It has two sets of ESTABLISHED TCP connections because the local 1756-EN4TR is the client for some connections and a server for other connections.

1. The first set of connections shows the local 1756-EN4TR with IP Address 10.17.81.51. It has initiated and ESTABLISHED TCP connections to several IACS devices (Remote Address) on the Remote (destination) port 44818.

2. The second set of connections show the local 1756-EN4TR with IP Address 10.17.81.51. It has accepted and ESTABLISHED TCP connections on its local port of 44818 from several IACS devices (Remote Address) on random Remote (destination) port numbers.

Figure 4-1   1756-EN4TR Webpage (TCP Connections page) before CIP Security
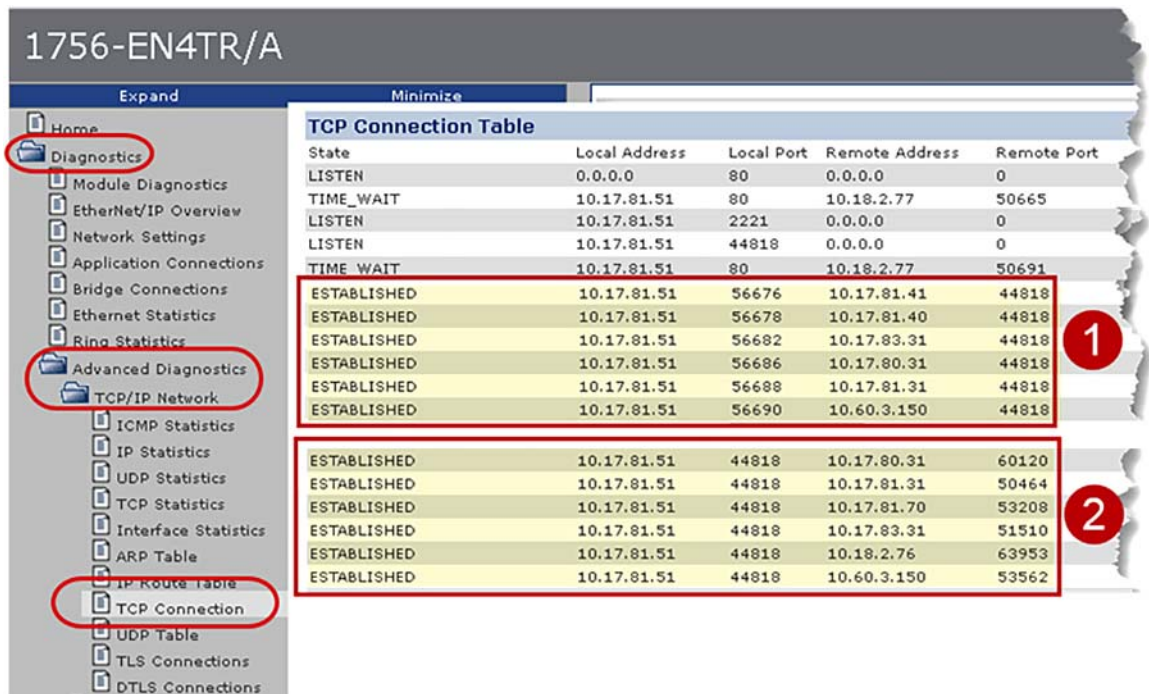
In Figure 4-2 the webpage of the local 1756-EN4TR with IP Address 10.17.81.51 shows the TCP connections after the CIP Security deployment. It has four sets of ESTABLISHED TCP connections because the local 1756-EN4TR module is the client for some connections and a server for other connections.

1. The first set of connections shows the local 1756-EN4TR with IP Address 10.17.81.51. It has initiated and ESTABLISHED secured TCP connections to one IACS devices (Remote Address) on the Remote (destination) port 2221.

2. The local 1756-EN4TR with IP Address 10.17.81.51. It has accepted and ESTABLISHED TCP secured connections on its local port of 2221 from several IACS devices (Remote Address) on random Remote (destination) port numbers.

3. The local 1756-EN4TR with IP Address 10.17.81.51. It has initiated and ESTABLISHED unsecured TCP connections to several IACS devices (Remote Address) on the Remote (destination) port 44818.

4. The local 1756-EN4TR with IP Address 10.17.81.51. It has accepted and ESTABLISHED TCP unsecured connections on its local port of 44818 from several IACS devices (Remote Address) on random Remote (destination) port numbers.

Note   The Remote Address IACS devices using the TCP connection to port 44818 after CIP Security has been deployed are the IACS devices that do not support the CIP Security feature. The local 1756-EN4TR currently supports CIP Security and can interoperate with IACS devices that do not support CIP Security on the network on the standard TCP/UDP ports of 44818 and 2222. For more details, see Trusted IP Communication in Chapter 2, "CPwE CIP Security Design Considerations."

Figure 4-2   1756-EN4TR Webpage (TCP Connections page) after CIP Security

Identify the TLS Connections

Once the security model has been successfully deployed, the webpages of the 1756-L8xE and 1756-EN4TR can help identify the cipher suite configured between the client and the server IACS device. TLS connections are the class 3 explicit messaging such as MSG instruction and CIP administration.

In Figure 4-3 the webpage of the local 1756-EN4TR with IP Address 10.17.81.51 has three ESTABLISHED TLS connections:

1. Remote IP: 10.17.83.31 (Green_EN4TR)

- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

  Each cipher suite has a unique name that is used to identify it and to describe the algorithmic contents of it. Each segment in a cipher suite name represents another algorithm or protocol. The meaning of this name is:

  - TLS defines the protocol used in the cipher suite

  - Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) is used for the key exchange

- – Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the authentication
- – Advanced Encryption Standard with 128-bit key in Cipher Block Chaining mode (AES 128 CBC) is used for the encryption
- – Secure Hash Algorithm 256 (SHA256) is used for the hash
- • Connection side: Server

  This means the local 1756-EN4TR with IP Address 10.17.81.51 has accepted the TLS connection from the IACS Remote IP: 10.17.83.31 (Green_EN4TR).

2. Remote IP: 10.18.2.76 (FactoryTalk Linx Data Server)

- • Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- • Connection side: Server

3. Remote IP: 10.17.80.31 (Red_EN4TR)

- • Cipher Suite: TLS_ECDHE_ECDSA_WITH_NULL_SHA256

  The meaning of the cipher suite applied is:

  - – TLS defines the protocol used in the cipher suite
  - – ECDHE used for the key exchange
  - – ECDSA used for the authentication
  - – NULL means no encryption is used
  - – SHA256 used for the hash

- • Connection side: Client

  This means the local 1756-EN4TR with IP Address 10.17.81.51 has initiated the TLS connection to the IACS Remote IP: 10.17.80.31 (Red_EN4TR).

Figure 4-3   1756-EN4TR Webpage (TLS Connections Page)
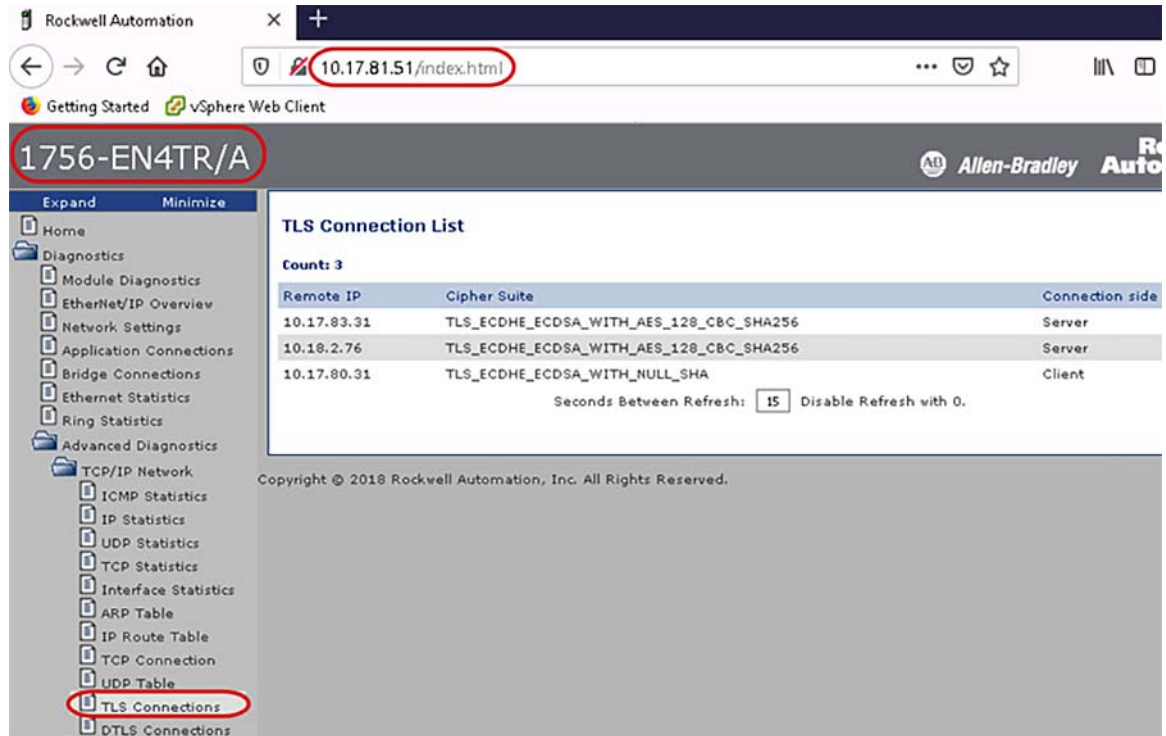
Identify the DTLS Connections

Once the security model has been successfully deployed, the webpages of the 1756-L8xE and 1756-EN4TR can help identify the cipher suite configured between the IACS devices. DTLS connections are the class 0/1 implicit messaging such as I/O connections and produced/consume connections.

In Figure 4-4 the webpage of the local 1756-EN4TR with IP Address 10.17.81.51 has seven ESTABLISHED DTLS connections. The following description explains the two connections to the same Remote IP IACS device Remote IP: 10.17.83.31.

1. Remote IP: 10.17.83.31 (Green_EN4TR)

- Cipher Suite: TLS_ECDHE_ECDSA_WITH_NULL_SHA256

    The meaning of applied cipher suite is:

    - TLS defines the protocol used in the cipher suite

    - ECDHE used for the key exchange

    - ECDSA used for the authentication

    - NULL means no encryption is used

    - SHA256 used for the hash

- Connection side: Server and Client

This means the local 1756-EN4TR with IP Address 10.17.81.51 is the server and the client for the DTLS connection from the client and server IACS Remote IP: 10.17.83.31 (Green_EN4TR). The IACS application being used is produced/consume between the two 1756-EN4TRs. The local 1756-EN4TR is producing data for the Green_EN4TR to consume and inversely the Green_EN4TR is also a producer of another set of data for the local 1756-EN4TR to consume.

Figure 4-4   1756-EN4TR Webpage (DTLS Connections Page)
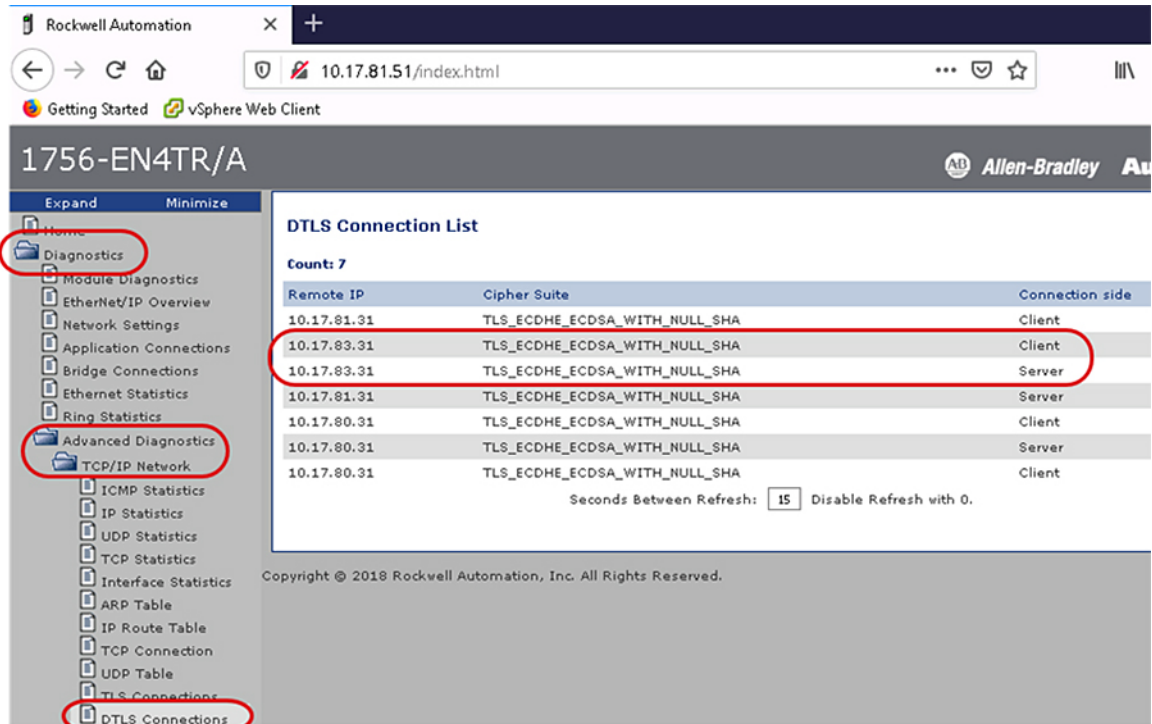
Identify the Confidentiality Connections

The webpages of the 1756-L8xE and 1756-EN4TR can help identify the active bridge connections between the IACS devices and what CIP Security properties are being used for the connection. The Bridge Connections page displays the type of CIP messaging either class 3 explicit message or class 0/1 implicit message along with the CIP Security property applied in the Confidentiality column.

Figure 4-5 shows the webpage of the local 1756-EN4TR with IP Address 10.17.81.51 active bridge connections after the CIP Security deployment. It has three sets of active connections:

1. The first row shows a class 3 active connection from an IACS device identified as Link Addr: 10.17.83.31 (Green_EN4TR). Encrypted is displayed in the Confidentiality column, concluding this connection is using all three CIP Security properties: device authentication, data integrity and confidentiality.

2. The second row shows a class 1 active connection to an IACS device identified as Link Addr: 10.17.81.31 (Yellow_EN4TR). Authenticated is displayed in the Confidentiality column, concluding this connection is using only two of the CIP Security properties: device authentication, and data integrity.

3. The third row shows a class 0 active connection to a server identified as Link Addr: 10.17.81.41 (5069-I/O device). None is displayed in the Confidentiality column, concluding this connection is not using any of the CIP Security properties.

Figure 4-5   1756-EN4TR Webpage (Bridge Connections Page) after CIP Security

Wireshark Verification

Identify the Initial Deployment of CIP Security

Wireshark is a widely used network protocol analyzer. It is a free and open-source packet analyzer commonly used for network troubleshooting, protocol analysis, software and communications protocol development, and education. The purpose of traffic analysis is to determine who is talking to whom.

In the initial release of the CIP Security feature in Rockwell Automation products, the ODVA PUSH method is used for CIP Security provisioning. In this method, the initial deployment of the CIP Security model sets the configuration tool (FTPM/FTSS) as the client initiating the connection and the IACS device as the server in a TLS handshake. Figure 4-6 captures the initial deployment of CIP Security from the computer hosting FactoryTalk Policy Manger (FTPM) and FactoryTalk System Service (FTSS) to a 1756-L85E (Blue_L85E).

1. A reliable TCP connection is needed for communication between the two IACS devices. The TCP connection is established on the secure port 2221. The client is the FTPM/FTSS computer and the server the Blue_L85E.

- **Client** -> Server: SYN

- Client <- **Server**: SYN, ACK

- **Client** -> Server: ACK

2. A secure TLS connection is created for the TLS handshake protocol. The client is the FTPM/FTSS computer and the server the Blue_L85E.

- **Client** -> Server: CLIENT_HELLO

   The client sends a message to the server, asking for an encrypted session, which includes:

   – The highest TLS version supported by the client.

   – Ciphers supported by the client. The ciphers are listed in order of preference.

   – Data compression methods that are supported by the client.

   – The session ID. If the client is starting a new TLS session, the session ID is 0.

- – Random data that is generated by the client for use in the key generation process.

- Client <- **Server**: SERVER_HELLO

  The server sends a SERVER_HELLO command to the client, which includes:

  - – The TLS version that will be used for the TLS session.

  - – The cipher that will be used for the TLS session.

  - – Data compression method that will be used for the TLS session.

  - – The session ID for the TLS session.

  - – Random data that is generated by the server for use in the key generation process.

- Client <- **Server**: CERTIFICATE

  The server responds with their server certificate, which includes the server public key in it. The server is the 1756-L85E and the certificate it sends is the born on certificate or vendor certificate as a root certificate-see—see Figure 4-7.

- Client <- **Server**: SERVER_KEY_EXCHANGE

  This message is optional and sent when the public key that is present in the server's certificate is not suitable for key exchange or if the cipher suite places a restriction requiring a temporary key. This key is used by the client to encrypt Client Key Exchange later in the process. The 1756-L85E does not use its born on certificate or vendor certificate as a basis for trust when it is being configured with new trust anchors and certificates. Once security has been set up by FactoryTalk Policy Manager, trust is limited to the trust anchors that the tool has provisioned, and the vendor certificate becomes irrelevant.

- Client <- **Server**: SERVER_HELLO_DONE

  The server sends the SERVER_DONE command. This command indicates that the server has completed this phase of the TLS handshake and is awaiting the client's response.

- **Client** -> Server: CLIENT_KEY_EXCHANGE

  Using all data generated in the handshake thus far, both will perform the following:

  - – The client generates the pre-master secret "random value" for the session, encrypts it with the server's public key (obtained from the server's certificate) and sends the encrypted pre-master secret to the server. The pre-master secret is a random value generated by the client and encrypted with the server public key. The pre-master key's length can vary depending on the algorithm used during key exchange. This along with the client and server random number is used to create the master secret. If the server can decrypt the message using the server's private key and can create the master secret locally, then the client is assured that the server has authenticated itself.

  - – The server uses its private key to decrypt the pre-master secret.

  - – Both the client and the server use the pre-master key and performs a series of steps to compute and generate the same master secret locally. The master secret is then used to derive a shared secret key/session key for symmetric encryption and MAC. The master secret is of fixed-length value.

  - – Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity.

- **Client** -> Server: CHANGE_CIPHER_SPEC

  The client sends a message to the server informing it that future messages from the client will be encrypted with the session key and indicates that its portion of the handshake is finished.

- Client <- **Server**: CHANGE_CIPHER_SPEC

The server sends a verification message to the client, which has the HMAC for data integrity and encrypted by shared secret key. It also indicates that its portion of the handshake is finished.

The TLS handshake is now complete and the session begins. The client and the server use the shared secret key to encrypt and decrypt the data they send to each other and to validate its integrity.

3. At this point, both client (FTPM/FTSS computer) and server (Blue_L85E) have successfully completed the TLS handshake. Application data is then exchanged using the symmetric encryption and HMAC. In symmetric encryption, the exact same key is used on both sides of a conversation, for both encrypting and decrypting. The application data packets exchanged set the initial configurations deployed in the FactoryTalk Policy Manager security model to the CIP Security capable IACS devices. During this time, application data packets are exchanged to set the appropriate CIP Security objects including the CIP Security object, the certificate management object (CMO) and EtherNet/IP Security object. It also includes the provisioning of the client certificate or new trust anchors for the CIP Security devices in that security model. The client (FTPM/FTSS computer) instructs the server (Blue_L85E) to create a certificate signing request (CSR), which includes the server creating a public/private key pair. The private key stays on the server and is never shared with the client or any other IACS devices. The client reads the CSR, digitally signs it then sends it back as a client certificate, which will be used as device authentication.

Figure 4-6   Initial Deployment of CIP Security

Figure 4-7   CIP Security Vendor Certificate

Identify Class 3 Explicit Communication with CIP Security

After the initial security model has been deployed, each CIP Security capable IACS device will have their respective client certificates signed by a mutual CA, which is the FTPM/FTSS computer. The client certificate will serve as the IACS device's proof of authentication. Certificates are agreements between communicating parties and a common entity called a Certificate Authority (CA). The CA is a trusted entity that manages and issues security certificates to requesters to prove their identities and public keys that are used for secure communication in an IACS network. Mutual trust is established when communicating parties exchange certificates signed by a common CA.

Figure 4-8 captures two 1756-L85Es exchanging client certificates then establishing a CIP connection for a class 3 explicit message. The 1756-L85E (Blue_L85E) is the client and the 1756-L85E (Green_L85) is the server. It follows the same client and server data flow as the initial deployment except after both IACS devices are finished with the TLS handshake, they will perform the CIP Connection Manager Forward_Open request all on the secure CIP TCP Port 2221.

Figure 4-8   Class 3 Explicit Messaging CIP Security

Figure 4-9 displays the client certificate the 1756-L85E (Green_L85) is presenting to the 1756-L85E (Blue_L85E). The client certificate contents are much different from the vendor certificate. The issuer contents displays the information set in the FactoryTalk Policy Manager Global settings.

Figure 4-9   CIP Security Client Certificate

Identify Class 0/1 Implicit Communication with CIP Security

Figure 4-10 captures a 1756-L85E and 1756-EN4TR exchanging client certificates then establishing a CIP connection for a class 0/1 implicit message. The 1756-L85E (Blue_L85E) is the client and the 1756-EN4TR (Red_EN4TR) is the server. It follows the same client and server data flow as the initial deployment except after both IACS devices are finished with the DTLS handshake, they will perform the CIP Connection Manager Forward_Open request all on the secure CIP TCP Port 2221.

Figure 4-10   Class 0/1 Implicit Messaging CIP Security

Deployment Troubleshooting

In FactoryTalk Policy Manager, after deployment, review the Results tab for the result of the deployment on each item in the model. The possible results are:

- Configuration complete. No issues identified.
- Configuration complete. Warnings identified.
- Configuration not complete. Error identified.

The Online Help in the FactoryTalk Policy Manager top main menu bar includes a reference of the possible errors and warning along with descriptions encountered during deployment.

Reloading the model synchronizes FactoryTalk Policy Manager and FactoryTalk System Services and refreshes the display of possible conflicts so that they can be addressed before deployment. The Reload button is in the FactoryTalk Policy Manager top main menu bar.

Verify the computer hosting FactoryTalk Policy Manager has successfully communications to all required IACS devices. This includes but not limited to: ping, tracert, can be browsed in FactoryTalk Linx Browser utility or FactoryTalk Linx in the Administration Console.

CIP Security IACS devices must be discoverable by FactoryTalk Linx to apply and deploy CIP Security properties. FactoryTalk Linx Browser utility cannot be used to modify, enable or disable the CIP Security properties on IACS devices. Please use the FactoryTalk Policy Manager software to modify, enable or disable CIP Security properties.

Deleting the IACS device from the model does not remove the security configuration. Even if FactoryTalk Policy Manager and FactoryTalk System Services are uninstalled the security policy configured for the IACS device is still in effect on that IACS device. The recommended steps to remove any CIP Security configurations on an IACS device are detailed in Removing the CIP Security Policy from an IACS Device in Chapter 3, "CPwE CIP Security Configuration."

References

This appendix includes the following reference sections:

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing—Converged Plantwide Ethernet
  http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures—Converged Plantwide Ethernet
  http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page
- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf
- Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

- OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide:
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td018_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/OEM/WP/CPwE-5-1-OEM-WP/CPwE-5-1-OEM-WP.html

- Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide:
  - 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

- Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide:
  - 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:
  - 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-DIG.html

- Cloud Connectivity to a Converged Plantwide Ethernet 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

- Deploying Network Security within a Converged Plantwide Ethernet Architecture:
  - 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 Scalable Time Distribution within a Converged Plantwide Ethernet Architecture:
  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td016_-en-p.pdf
  - Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html

- Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide:
    - Rockwell Automation site:
      http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf
    - Cisco site:
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/4-0/Resiliency/DIG/CPwE_resil_CVD.html
- Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture:
    - Rockwell Automation site:
      https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf
    - Cisco site:
      https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/PRP/DIG/CPwE-5-1-PRP-DIG.html
- Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide:
    - Rockwell Automation site:
      https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf
    - Cisco site:
      http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Other References

- CIP Security with Rockwell Automation Products Application Technique
  https://literature.rockwellautomation.com/idc/groups/literature/documents/at/secure-at001_-en-p.pdf
- ODVA, CIP Security
  https://www.odva.org/Technology-Standards/Common-Industrial-Protocol-CIP/CIP-Security
- ODVA, Overview of CIP Security
  https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00319R1_CIP_Security_At_a_Glance.pdf
- Stratix Managed Switches User Manual
  http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

Acronyms and Initialisms

Table B-1 lists the acronyms and initialisms commonly used in CPwE documentation.

Table B-1   Acronyms and Initialisms

Term	Description
1:1	One-to-One
AAA	Authentication, Authorization, and Accounting
AD	Microsoft Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
ADR	Automatic Device Replacement
AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
AIA	Authority Information Access
AMP	Advanced Malware Protection
ASDM	Cisco Adaptive Security Device Manager
ASIC	Application Specific Integrated Circuit
ASR	Cisco Aggregation Services Router
BYOD	Bring Your Own Device
CA	Certificate Authority
CDP	CRL Distribution Points
CIP^{TM}	ODVA, Inc. Common Industrial Protocol
CLI	Command Line Interface
CoA	Change of Authorization
CoS	Class of Service
CPwE	Converged Plantwide Ethernet
CR	Component Requirement
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CRR	Cyber Resilience Review
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager

Table B-1   Acronyms and Initialisms (continued)

Term	Description
CTS	Cisco TrustSec
CTL	Certificate Trust List
CUR	Coarse Update Rate
CVD	Cisco Validated Design
CVE	Common Vulnerabilities and Exposers
DACL	Downloadable Access Control List
DC	Data confidentiality
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIG	Design and Implementation Guide
DLR	Device Level Ring
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name System
DoS	Denial-of-service
DPI	Deep Packet Inspection
DSRM	Directory Services Restoration Mode
DTLS	Datagram transport layer security
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EIGRP	Enhanced Interior Gateway Routing Protocol
EMI	Enterprise Manufacturing Intelligence
EoIP	Ethernet over IP
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
FIB	Forwarding Information Base
FIFO	First-In First-Out
FTD	FactoryTalk Directory
FTNM	FactoryTalk Network Manager
FTPM	FactoryTalk Policy Manager
FTSS	FactoryTalk System Service
FPGA	Field-Programmable Gate Array
FQDN	Fully Qualified Domain Name
FR	Foundational Requirement
FVRF	Front-door Virtual Route Forwarding
GRE	Generic Routing Encapsulation
GUI	Graphical user interface
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
HSM	Hardware Security Module
HSRP	Hot Standby Router Protocol
HTTP	Hypertext transfer protocol
HTTPS	Secure hypertext transfer protocol

Table B-1   Acronyms and Initialisms (continued)

Term	Description
IAC	Identification and authentication control
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zones
IEC	International Electrotechnical Commission
IES	Industrial Ethernet Switch (Allen-Bradley Stratix)
IGMP	Internet Group Management Protocol
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
I/O	Input/Output
IoT	Internet of Things
IP	Internet Protocol
IPDT	IP Device Tracking
ISA	International Society of Automation
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISE	Cisco Identity Services Engine
ISR	Integrated Service Router
IT	Information Technology
LBS	Location Based Services
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation
MITM	Man-in-the-middle
MLS	Multilayer Switching QoS
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MQC	Modular QoS CLI
MSE	Mobile Service Engine
MSG	Class 3 explicit message instruction
MSS	Maximum Segment Size
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NHRP	Next Hop Routing Protocol
NIST	National Institute of Standards and Technology
NMT	Network Management Tool
NOC	Network Operation Center

Deploying CIP Security within a Converged Plantwide Ethernet Architecture

Table B-1   Acronyms and Initialisms (continued)

Term	Description
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAC	Programmable Automation Controller
PAN	Policy Administration Node
PAT	Port Address Translation
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
pps	Packet per second
PSK	Pre-Shared Key
PSN	Policy Service Node
PTP	Precision Time Protocol
QoS	Quality of Service
RA	Registration Authority
RA	Resource availability
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RD	Route Descriptor
RDG	Restricted data flow
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
REP	Resilient Ethernet Protocol
RPI	Request Packet Interval
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SGT	Security Group Tag
SHA	Secure Hash Standard
SI	System integrity
SIEM	Security Information and Event Management
SIG	Secure Internet Gateway
SIL	Safety Integrity Level
SL	Security Level
SL-A	Achieved Security Level

Deploying CIP Security within a Converged Plantwide Ethernet Architecture

Table B-1   Acronyms and Initialisms (continued)

Term	Description
SL-C	Capability Security Level
SL-T	Target Security Level
SPW	Software Provisioning Wizard
SR	System Requirement
SSID	Service Set Identifier
STP	Spanning-Tree Protocol
SV	Stackwise Virtual
SYN	Synchronization
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOFU	Trust On First Use
TRE	Timely response to events
UC	Use control
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VSS	Virtual Switching System
WAN	Wide Area Network
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall

Deploying CIP Security within a Converged Plantwide Ethernet Architecture

About the Cisco Validated Design (CVD) Program

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation which follows the Cisco Validated Design (CVD) program.

CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by engineers to help achieve faster, more reliable, and fully predictable deployment.

The CVD process is comprehensive and focuses on solving business problems for customers and documenting these solutions. The process consists of the following steps:

- Requirements are gathered from a broad base of customers to devise a set of use cases that will fulfill these business needs.

- Network architectures are designed or extended to provide the functionality necessary to enable these use cases, and any missing functionality is relayed back to the appropriate product development team(s).

- Detailed test plans are developed based on the architecture designs to validate the proposed solution, with an emphasis on feature and platform interaction across the system. These tests generally consist of functionality, resiliency, scale, and performance characterization.

- All parties contribute to the development of the CVD guide, which covers both design recommendations and implementation of the solution based on the testing outcomes.

Within the CVD program, Cisco also provides Cisco Reference Designs (CRDs) that follow the CVD process but focus on reference designs developed around specific sets of priority use cases. The scope of CRD testing typically focuses on solution functional verification with limited scale.

For more information about the CVD program, please see the Cisco Validated Designs at the following URL:

https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.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:	Asia Pacific:	Europe/Middle East/Africa:	Latin America:
Panduit Corp.	One Temasek Avenue #09-01	Panduit Corp.	Panduit Corp.
World Headquarters	Millenia Tower	West World	Periférico Pte Manuel Gómez
18900 Panduit Drive	039192 Singapore	Westgate London W5 1XP Q	Morin #7225 - A
Tinley Park, IL 60487	Tel. 65 6305 7555	United Kingdom	Guadalajara Jalisco 45010
iai@panduit.com		Tel. +44 (0) 20 8601 7219	MEXICO
Tel. 708.532.1800			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	Asia Pacific Headquarters	Europe Headquarters
Cisco Systems, Inc.	Cisco Systems (USA) Pte. Ltd.	Cisco Systems International BV
San Jose, CA	Singapore	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.

Catalyst, Cisco, and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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:	Asia Pacific:	Europe/Middle East/Africa:
Rockwell Automation	Rockwell Automation	Rockwell Automation
1201 South Second Street	Level 14, Core F, Cyberport 3	NV, Pegasus Park, De Kleetlaan 12a
Milwaukee, WI 53204-2496 USA	100 Cyberport Road, Hong Kong	1831 Diegem, Belgium
Tel: (1) 414.382.2000	Tel: (852) 2887 4788	Tel: (32) 2 663 0600
Fax: (1) 414.382.4444	Fax: (852) 2508 1846	Fax: (32) 2 663 0640

Allen-Bradley, Compact 5000, CompactLogix, ControlLogix, FactoryTalk, FactoryTalk Network Manager, GuardLogix, Kinetix, Logix 5000, Point I/O, Rockwell Automation, RSLinx, Stratix, Studio 5000 Logix Designer and Trusted are trademarks of Rockwell Automation, Inc.

CIP, CIP Motion, CIP Safety, CIP Security, CIP Sync, and EtherNet/IP are trademarks of ODVA, Inc.

Excel and Microsoft are trademarks of Microsoft Corporation.

Trademarks not belonging to Rockwell Automation are property of their respective companies