CIP Security with Rockwell Automation Products
Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

---

**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

**IMPORTANT** Identifies information that is critical for successful application and understanding of the product.

---

Labels may also be on or inside the equipment to provide specific precautions.

**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

**ARC FLASH HAZARD:** Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).
# Table of Contents

## Preface

Additional Resources

## Chapter 1

**Industrial Security Overview**

- Industrial Automation Control Systems Environment
- Security Threats
- Vulnerability and Exploits
- Security Assessment
- Defense-in-Depth Architecture
- CIP Security is an ODVA Standard
  - Device Identity/Authentication
  - Secure Data Transport

## Chapter 2

**CIP Security-capable Rockwell Automation Products**

- Software and Hardware
  - CIP Security Software Applications
  - CIP Security-capable Hardware Devices
- Benefits of Using Rockwell Automation Products
- CIP Security Properties
- CIP Security Profile and Attributes
- CIP Security Components
- CIP Security Policy Model
  - Zone Security Policy Properties
  - Conduit Security Policy Properties
- Limitations and Considerations
  - Dual-port Devices
  - CIP Bridging
  - Network Address Translation
  - ControlLogix Redundancy Systems
  - Automatic Device Replacement
  - RSLinx Classic Software
## Table of Contents

### Chapter 3
- CIP Security Implementation Process
  - Install, Plan, and Design the System ........................................ 32
  - Identify, Organize, and Create Zones ........................................ 33
    - Create a Zone .............................................................................. 34
    - Configure the Zone ...................................................................... 36
  - Identify, Organize, and Create Conduits .................................... 37
    - Create a Conduit ........................................................................... 38
    - Configure the Conduit ................................................................. 42
  - Identify and Create Security Features/Policies ............................... 44
  - Deploy Security Model .................................................................... 45
  - Back Up CIP Security Model ............................................................ 48
  - Remove CIP Security Configuration ................................................ 49
    - Remove the CIP Security Configuration From a Software Application .................................................... 49
    - Remove the Security Configuration From a Device ...................... 53

### Chapter 4
- CIP Security Implementation Example Architecture
  - Phase One of Implementation .......................................................... 57
    - Create Zones ................................................................................ 58
    - Create Zone-to-Zone Conduits ....................................................... 60
    - Configure Conduit Security Policies ............................................. 61
    - Deploy Security Policies ................................................................. 63
  - Phase Two of Implementation .......................................................... 64
    - Create a Device-to-Device Conduit ................................................. 64
    - Create a Zone-to-Device Conduit .................................................... 65
    - Create Conduit Security Policies .................................................... 67
    - Deploy Security Policies ................................................................. 68

### Index ..................................................................................................... 69
Preface

This manual explains how to implement the Common Industrial Protocol (CIP™) Security standard in your control system. The term CIP Security™ is used throughout the rest of this manual.

Make sure that you are familiar with the following before you use this manual:

- Basic understanding of EtherNet/IP™ networking fundamentals
- Basic understanding of network security terminology and concepts
- Use of Rockwell Automation® software, for example:
  - FactoryTalk® Policy Manager
  - FactoryTalk Linx
  - Studio 5000 Logix Designer®

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001</td>
<td>Describes how to install and use FactoryTalk System Services and FactoryTalk Policy Manager.</td>
</tr>
<tr>
<td>ControlLogix 5580 and GuardLogix 5580 Controllers User Manual, publication 1756-UM543</td>
<td>Describes how to design, implement, and maintain an industrial control system that uses ControlLogix® or GuardLogix®-based controllers.</td>
</tr>
<tr>
<td>ControlLogix EtherNet/IP Network Devices User Manual, publication 1756-UM004</td>
<td>Describes how to use ControlLogix EtherNet/IP communication modules with a Logix 5000™ controller and communicate with devices on the Ethernet/IP network.</td>
</tr>
<tr>
<td>Kinetix 5700 Servo Drives User Manual, publication 2198-UM002</td>
<td>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.</td>
</tr>
<tr>
<td>Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1</td>
<td>Provides general guidelines for installing a Rockwell Automation industrial system.</td>
</tr>
<tr>
<td>Product Certifications website: rok.auto/certifications</td>
<td>Provides declarations of conformity, certificates, and other certification details.</td>
</tr>
</tbody>
</table>

You can view or download publications at http://www.rockwellautomation.com/global/literature-library/overview.page.
Notes:
Chapter 1

Industrial Security Overview

This section provides an overview of CIP Security™.

Historically, industrial automation control systems (IACS) have been air-gapped environments, isolated systems that are running proprietary control protocols. But IACS networks are evolving toward smart manufacturing.

Smart manufacturing represents a gateway to digital transformation that connects plant-level and enterprise networks, and securely connects people, processes, and technologies.

Collectively this opens new windows to connected smart devices for visibility into processes, data, and analytics. The visibility enables better and faster decision making and seamless connectivity for remote locations.

As EtherNet/IP™ becomes a growing standard, evolving these isolated IACS networks towards smart manufacturing, network convergence and industrial security become a necessity.
Security Threats

As IACS networks transition to open standards of Ethernet-media and Internet Protocol (IP) to meet the needs of end-to-end connectivity of entities, the threat landscape broadens.

With an increase of smart devices and end-to-end connectivity come more assets to protect and a greater risk of security threats.

Security risks can take many forms, for example:

- Threat actors that try to gain unauthorized, and undetected, access to an IACS network with the intention to commit malicious acts.

- Well-intentioned personnel with no malicious intention but who make mistakes that can result in unintended consequences.

**IMPORTANT**

This publication focuses on threat actors with malicious intentions, also called attackers. The word attacker is used throughout the rest of the publication.

In this publication, attacker refers to one individual or to an Advanced Persistent Threat (APT), or a group of attackers working collectively.
Vulnerability and Exploits

By default, IACS communication protocols are proprietary and insecure. They lack the security properties such as authentication, integrity, and confidentiality. As a result, data and endpoints are at risk. These security properties are necessary for IACS devices to defend themselves against a network-based attack.

Insecure communication protocols can be exploited to make data accessible for anyone to collect, and vulnerable endpoints can become open targets for denial-of-service (DoS) and other types of attacks.

When attackers access a system, they use many ways to exploit the IACS communication protocol vulnerabilities.

Table 1 - Attack Types

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS (Unauthorized Open Access)</td>
<td>An attacker executes a DoS attack that renders the CIP™ device inoperable.</td>
</tr>
<tr>
<td>Man-in-the-Middle</td>
<td>The attacker eavesdrops on data in transit to alter the communication between CIP devices.</td>
</tr>
<tr>
<td>Monitor Data</td>
<td>The attacker monitors or views sensitive or classified data that is exchanged between CIP devices.</td>
</tr>
</tbody>
</table>
Security Assessment

Getting a security assessment is the starting point for any security implementation. An assessment provides a picture of your current security posture and what mitigation techniques you need to achieve a preferred acceptable risk state.

An assessment is a collaborative process, between Operational Technology (OT) and Information Technology (IT) personnel to maximize the protection of confidentiality, integrity, and availability while still providing functionality and usability.

There are three steps to perform a security assessment.

1. Conduct a threat assessment.

   A threat assessment considers a range of threats from natural, criminal, terrorist, to accidental for a given facility/location. Based on business requirements, a company should evaluate the likelihood for each threat.

2. Perform a vulnerability assessment.

   A vulnerability assessment is designed to identify methods by which the threats can be exploited and to provide recommendations on how to address these vulnerabilities.

   Each vulnerability should be rated for the probability or ease of exploitation and the resulting impact in terms of cost or injury should the exploit be successful. This establishes a risk score for each vulnerability.

3. Perform a risk assessment.

   A risk assessment evaluates the risk scores and assigns responses to each risk. One of the following actions should be taken for each risk:
   - Mitigated - A mitigated risk requires an explanation of what was done to prevent the vulnerability from being exploited.
   - Terminated - A terminated risk requires an explanation of what was removed or disabled to prevent the vulnerability from being exploited.
   - Transferred - A transferred risk requires an explanation of what is being done outside this system to prevent or respond to the vulnerability being exploited.
   - Accepted - An accepted risk requires notation of the authority accepting the risk.

Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to your IACS assets.
Industrial security is best implemented as a complete system across your operations. The Defense-in-Depth (DiD) approach is common to security standards.

The DiD security approach establishes multiple layers of protection that are based on diverse technologies through physical, electronic, and procedural safeguards.

For example, you restrict physical access to managed switches with port locks. Then you position edge industrial firewalls to restrict access and block unapproved traffic flows. Finally, you employ an Industrial Demilitarized Zone (IDMZ) as a perimeter buffer zone between the Industrial and Enterprise zones. The IDMZ lets secure data sharing and services take place without direct connection.

The following are key tenets of the DiD security approach:

- Multiple layers of security are more resilient to attack
- Each layer adds to the one above it
- It does not replace the need for firewalls or other security infrastructure in a system.

The expectation of the DiD approach is that in the event an attacker breaches one layer of defense, there is always an additional layer that will thwart their effort.

Figure 1 - Defense-in-Depth Architecture
CIP Security is an ODVA Standard

As attackers become more sophisticated and network convergence opens more potential gateways to industrial zones, CIP-connected devices must be able to defend themselves.

Recognizing the need for CIP-connected device protection, ODVA developed CIP Security. It is an open-standard secure communication mechanism for EtherNet/IP networks.

The following CIP Security properties are countermeasures that address the security exploitations:

- Device identity and authentication
- Data integrity and authentication
- Data confidentiality (encryption)

Positioned at the device-level in the DiD architecture, CIP Security enables CIP-connected devices to authenticate each other before transmitting and receiving data. Device connectivity is limited to only trusted devices.

Optionally, to increase the overall device security posture, it can be combined with data integrity to guard against packet tampering and message encryption to avert unwanted data reading and disclosure.

Figure 2 - CIP Security As Part of Defense-in-Depth Architecture
Device Identity/Authentication

Before devices start communicating, each device must be able to verify that the identity of the device with which it wants to communicate is authentic. This protects legitimate devices from a rogue device gaining access to the system by pretending to be a system component.

To build this endpoint trust, a certificate or pre-shared (secret) key can be used to provide identity to the device:

- Certificate is used to provide identity based on the X.509v3 standard.

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

  FactoryTalk System Services is the certificate authority. It is the service that signs and issues certificates to give assurance for a communicating party's authenticity.

  An advantage to using certificates is that they provide a greater level security than pre-shared keys.

  - Pre-shared keys are used to prove identity that is based on keys that are shared in advance among the communicating parties.

    Pre-shared keys are agreement between two entities to the parameters that determine identity and authentication. The entities are the devices that communicate with each other.

    An advantage to using pre-shared keys is that they provide less performance impact on when establishing connections

**IMPORTANT** Devices can only use one pre-shared key; as a result, any conduits required between any Zones configured with pre-shared key must be created using Trusted IP.
Secure Data Transport

CIP Security is based on Transport Layer Security (TLS) (RFC 5246) and Datagram Transport Layer Security (DTLS) (RFC 6347) protocols to protect EtherNet/IP data while in transit.

TLS and DTLS are network protocols that facilitate data transfer privately and securely between an originator and a target device.

TLS provides the following security properties:

- Authentication - Allows each device to confirm their identity through certificate exchange or pre-shared keys
- Integrity - Makes sure that the data has not been tampered with, or falsified, while in transit, by means of TLS Hash-based Message Authentication Code (HMAC)
- Confidentiality - Data is encrypted while being transmitted between the originator and target device. Encrypting the data prevents unauthorized parties from reading it.

DTLS is based on TLS but is used for User Datagram Protocol (UDP) connections instead of Transmission Control Protocol (TCP) connections.

For complete descriptions of the security properties, see the ODVA home page available at: https://www.odva.org/.

Table 2 defines the icons that are used in Table 3 beginning on page 15.

<table>
<thead>
<tr>
<th>Name</th>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td><img src="image" alt="Certificate" /></td>
<td>An electronic representation of an identity. A certificate binds the identity’s public key to its identifiable information, such as, name, organization, email, user name, and/or a device serial number. This certificate is used to authenticate a connection to a zone or device. Selected by default when CIP Security is enabled.</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td><img src="image" alt="Pre-shared key" /></td>
<td>A secret that is shared among trusted entities to represent identities. FactoryTalk Policy Manager can create a key that can be shared.</td>
</tr>
<tr>
<td>Integrity</td>
<td><img src="image" alt="Integrity" /></td>
<td>Checks whether data was altered and whether the data was sent by a trusted entity. Altered and/or untrusted data is rejected.</td>
</tr>
<tr>
<td>Check mark</td>
<td><img src="image" alt="Check mark" /></td>
<td>Symbol used to indicate that the endpoints for communication between devices have been authenticated and can be trusted.</td>
</tr>
<tr>
<td>Encryption</td>
<td><img src="image" alt="Encryption" /></td>
<td>Encodes messages or information to help prevent reading or viewing of EtherNet/IP data by unauthorized parties.</td>
</tr>
</tbody>
</table>
Table 3 describes how secure data transport enables a CIP-connected device to help protect itself from malicious communication.

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Device Identity and Authentication** | Method of providing secure identity for a device. The following methods can be used:  
  - **Certificates** (recommended)  
  - **Pre-shared keys**  
  Together, these properties help the device take the following actions:  
  - **Reject messages** that are sent by untrusted devices.  
  - **Prevent unauthorized** devices from establishing connections. |
| **Data Integrity and Authentication** | Method of providing data integrity and message authentication to EtherNet/IP network communication.  
Let the device take the following actions:  
  - **Reject data** that has been altered.  
  - **Prevent tampering** or modification of communication. |
| **Data Confidentiality**             | Means of using encryption to encode messages or information that is exchanged across an EtherNet/IP network.  
Let the device take the following actions:  
  - **Prevent viewing** of EtherNet/IP data by unauthorized parties.  
  - **Prevent snooping** or data disclosure.  
**IMPORTANT**: This security property is optional. Some IACS network communication do not need to be secure; data integrity and authentication is typically the goal. Encryption impacts network performance. |
Notes:
Chapter 2

CIP Security-capable Rockwell Automation Products

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software and Hardware</td>
<td>18</td>
</tr>
<tr>
<td>Benefits of Using Rockwell Automation Products</td>
<td>20</td>
</tr>
<tr>
<td>CIP Security Properties</td>
<td>20</td>
</tr>
<tr>
<td>CIP Security Policy Model</td>
<td>24</td>
</tr>
<tr>
<td>Limitations and Considerations</td>
<td>26</td>
</tr>
</tbody>
</table>

This section describes the components and concepts that are part of the Rockwell Automation method of implementing CIP Security™ in an IACS.

For information on the tasks that are required to use CIP Security-capable products in an IACS, see the following table:

- Chapter 3, CIP Security Implementation Process on page 31
- Chapter 4, CIP Security Implementation Example Architecture on page 57
- Publications listed in Additional Resources on page 5
Software and Hardware

The list of CIP Security-capable Rockwell Automation® products includes software and hardware products, for example, FactoryTalk Policy Manager software and ControlLogix® 5580 controllers, respectively, to configure the CIP Security policy model.

CIP Security Software Applications

**IMPORTANT** FactoryTalk® Policy Manager and FactoryTalk System Services are components of FactoryTalk Services Platform, version 6.11 or later.

When you install FactoryTalk Services Platform, version 6.11 or later, you must select Customize from the installation wizard and check the boxes for installation of FactoryTalk Policy Manager and FactoryTalk System Services components.

For more information, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

<table>
<thead>
<tr>
<th>Software Application</th>
<th>Description</th>
<th>Minimum Version Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Policy Manager</td>
<td>FactoryTalk Policy Manager is a secure software application that you use to configure, deploy, and view the system communication security policies. The security policies are divided into different components, that is, devices, zones, and conduits. You use these components to design security models that control the permissions and usage of devices within the system. For more information, on security models and how components are used to design the models, see page 20. The security policies are distributed to the devices at once. You are not required to make changes at the device level and face the risk of human error that results in inconsistent configuration among the devices.</td>
<td>Version 6.11</td>
</tr>
</tbody>
</table>
| FactoryTalk System Services| FactoryTalk System Services is a secure EtherNet/IP™ client that runs in the background to deploy the security policies that are configured in FactoryTalk Policy Manager. You do not take action in the client. FactoryTalk System Services provides the following in the FactoryTalk Directory to enforce security policies that are based on the ODVA CIP Security standard:
  - Identity/Authentication Service - Authenticates users and validates user resource requests. Validate user credentials against the FactoryTalk Directory and FactoryTalk Security policy settings to obtain privileges associated with the user.
  - Deployment Service - Translates the security policy model to CIP™ configurations that are delivered to endpoints.
  - Policy Service - Build and manages CIP network trust models and defines security policy for the CIP endpoints.
  - Diagnostic Service - Makes FactoryTalk audit and diagnostic logs available as a web service. | Version 6.11              |
| FactoryTalk Linx           | FactoryTalk Linx is a secure EtherNet/IP client that initiates connections over a secure EtherNet/IP network with CIP Security-enabled devices. This server and communication service that lets devices communicate with the FactoryTalk software portfolio and Studio5000 Logix Designer® software. **IMPORTANT**: You cannot use RSLogix Classic software to implement CIP Security in an IACS network. | Version 6.11              |
| Studio 5000 Logix Designer®| Logix Designer application is a comprehensive programming software that you use with Logix 5000™ controllers. In a system with CIP Security implemented, the software is only used with ControlLogix 5580 controllers. | Version 32.00.00          |
CIP Security-capable Hardware Devices

The following hardware devices are CIP Security-capable.

**IMPORTANT** The table represents products that are CIP Security-capable in the initial release of CIP Security with Rockwell Automation products. Over time, new products will be released that are CIP Security-capable. New versions of existing products that are not CIP Security-capable will be released in the future to make them CIP Security-capable. To see if a product is CIP Security-capable, see the product documentation.

<table>
<thead>
<tr>
<th>Hardware Product</th>
<th>Description</th>
<th>Minimum Firmware Revision Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlLogix 5580 Controllers</td>
<td>ControlLogix 5580 controllers use a common Logix control engine and common development environment to control large control systems. The controllers communicate with, and can control, local and remote devices. For example, the devices can be I/O modules, network communication modules, drives, and operator interfaces. You use the Logix Designer application to configure ControlLogix 5580 controllers. The Logix Designer application version must be compatible with the firmware revision on the controllers. <strong>IMPORTANT</strong>: You <strong>do not</strong> use the Logix Designer application to configure the CIP Security policy. You use FactoryTalk Policy Manager to configure the CIP Security policy.</td>
<td>Firmware revision 32.011</td>
</tr>
<tr>
<td>1756-EN4TR ControlLogix EtherNet/IP Communication Module</td>
<td>The 1756-EN4TR communication module performs the following functions: • Facilitate high-speed data transfer between ControlLogix 5580 controllers and devices on an EtherNet/IP network. • Connect Logix 5000 control systems to multiple EtherNet/IP network topologies.</td>
<td>—</td>
</tr>
<tr>
<td>Kinetix® 5700 Drives</td>
<td>Kinetix 5700 drives are single and dual-axis inverters that you can use to expand the use of Integrated Motion on EtherNet/IP to large, custom machines with high axis counts and power requirements. The drives have built-in dual Ethernet ports that let you connect the drives directly to EtherNet/IP networks.</td>
<td>Firmware revision 11.001</td>
</tr>
</tbody>
</table>
Benefits of Using Rockwell Automation Products

Implementing CIP Security with Rockwell Automation products has the following benefits:

- Centralized System Management - Use FactoryTalk Policy Manager software to easily create and deploy security policies to many devices at once.

- Micro-segmentation - Segment the automation application into smaller cell/zones, thus, reducing the attack surface.

- HTTP ports - You can enable or disable unsecure (HTTP) ports/protocols of devices in a system with CIP Security configured.

- Legacy system support - The following options are available to use for products that are not CIP Security-capable in a specific unsecured communication network that deploys the CIP Security feature:
  - Whitelisting - Authorize specific communication based on IP address.
  - Retrofit ControlLogix 5570-based systems with the new 1756-EN4TR communication module.

CIP Security Properties

CIP Security is made up of a security profile, attributes, and components. These key mechanisms facilitate the security requirements for the resource you are trying to protect.

CIP Security Profile and Attributes

CIP Security defines the concept of a Security Profile. 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.

Understanding that security is a balance and not every CIP-connected device requires the same level of security, FactoryTalk Policy Manager lets administrators enable only the desired attributes when they create a Security Profile.

The Device Identity/Authentication attribute must be enabled before the options for enabling Data Integrity and Data Confidentiality can occur.
Rockwell Automation CIP Security-capable products support the following security attributes:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Identity and Authentication</td>
<td>Certificate base on the X.509 v3 standard is used to provide identity. Pre-shared keys are shared secrets that are shared among trusted entities that are used to provide identity. The TLS protocol facilitates mutual authentication to create trusted endpoints.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Keyed-Hash Message Authentication Code (HMAC) is used as a cryptographic method of providing data integrity and message authenticity to EtherNet/IP traffic.</td>
</tr>
<tr>
<td>Data Confidentiality</td>
<td>Data encryption is used to encode messages or information to help prevent reading or viewing of EtherNet/IP data by unauthorized parties.</td>
</tr>
</tbody>
</table>

**IMPORTANT** The rest of this section describes each component and, for zones and conduits, steps to create and configure them. However, the descriptions are not exhaustive.

For more detailed information on security models, including the tasks that you must complete to configure them, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.

## CIP Security Components

FactoryTalk Policy Manager divides the system security policies into different components. The following components are used to design security models:

- **Devices**
- **Zones**
- **Conduits**

### Devices

Devices are the modules, drives, controllers, HMI panels, computers, and servers that work together to create an IACS network. You add devices that share security requirements for a particular function to the same zone.

Considerations with devices in the CIP Security model when you use devices in an IACS network:

- The lists of current CIP Security-capable Rockwell Automation products are on page 18 and page 19.

  More CIP Security-capable Rockwell Automation products are in development.

- Just because a device is CIP Security-capable, you are not required to enable CIP Security on that device in an IACS network.

- You can use non CIP Security-capable devices in an IACS that includes CIP Security-enabled devices.
Zones

Zones are groups to which devices are added. Zones establish the rules for data integrity, data privacy, and the authentication method that is used to authenticate trusted devices.

- You can have multiple zones in a system and set security policy on a zone-by-zone basis. By using zones, you simplify management of large sets of devices in a system.

- Zones can include devices that are CIP Security-capable and devices that are not. There can be multiple zones in an IACS network, but a device can only belong to one zone.

- Once a CIP Security-capable device is added to a zone, the device uses the policy default settings of that zone.

Communication between devices in the same zone are implied and mutually trusted. Therefore, you do not have to create conduits between devices in the same zone.

Figure 3 shows a zone that includes devices that are CIP Security-capable, for example, a ControlLogix 5580 controller, and devices that are not, for example, a PanelView™ Plus terminal.

Figure 3 - Security Model - Zones
Conduits

Conduits create trusted communication pathways outside of zones. You must have at least two endpoints, that is, zones or devices, to create a conduit.

Conduits facilitate secure communication in the following ways:

- Zone to zone
- Device to device
- Device to zone

Conduits let you configure trust beyond individual zones using the following methods:

- Trusted IP authentication method - Assigns a trust relationship to an asset based on its IP address. Also known as Whitelisting,
- Certificate authentication method - Establishes the identity of the device by using a certificate from a trusted authority.

**IMPORTANT** Currently, a device cannot use more than one pre-shared key. If you require communication between a zone that is configured with a pre-shared key and other zones, you must configure a conduit that uses the Trusted IP authentication method to the other zones.

Figure 4 shows conduits in a system with multiple zones.

**Figure 4 - Security Model - Conduits**
CIP Security Policy Model

The CIP Security policy model is made up of zone, conduit, and device security policy property configurations.

**TIP** If multiple devices use the same security policies and are in the same zone, we recommend that you configure the security policies at the zone level.

The advantage to configuring security policies at the zone level is that you can configure the policies once and apply them to multiple devices. This method eliminates the possibility of differences in security policies across devices that should use the same policies.

Zone Security Policy Properties

*Table 4* lists the configurable fields that are available when you configure zone security policy.

### Table 4 - Zone Security Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Available Choices</th>
<th>Example FactoryTalk Policy Manager Screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User configurable</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>User configurable</td>
<td></td>
</tr>
<tr>
<td>Enable/Disable CIP Security</td>
<td>• Enable • Disable</td>
<td></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>• Certificate • Pre-Shared Key</td>
<td></td>
</tr>
<tr>
<td>I/O Data Security</td>
<td>• None • Integrity Only • Integrity + Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Messaging Security</td>
<td>• Integrity Only • Integrity + Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Disable Ports - HTTP (80)</td>
<td>• Enable • Disable</td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT** For more information on the Zone Security Policy Properties, see the FactoryTalk Policy Manager Getting Results Guide, publication **FTALK-GR001**.
Conduit Security Policy Properties

Table 5 lists the configurable fields that are available when you configure conduit security policy.

Table 5 - Conduit Security Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Available Choices</th>
<th>Example FactoryTalk Policy Manager Screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User configurable</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>User configurable</td>
<td></td>
</tr>
<tr>
<td>Connection</td>
<td>Can be any of the following based on how you assign each Endpoint:</td>
<td><img src="image" alt="Example Screen" /></td>
</tr>
<tr>
<td></td>
<td>• Device-to-Device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device-to-Zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Zone-to-Zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Endpoint 1 (Device or Zone)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Endpoint 2 (Device or Zone)</td>
<td></td>
</tr>
<tr>
<td>Authentication Method</td>
<td>• Trusted IP</td>
<td><img src="image" alt="Example Screen" /></td>
</tr>
<tr>
<td></td>
<td>• Certificate</td>
<td></td>
</tr>
<tr>
<td>I/O Data Security</td>
<td>• None</td>
<td><img src="image" alt="Example Screen" /></td>
</tr>
<tr>
<td></td>
<td>• Integrity Only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Integrity + Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Messaging Security</td>
<td>• Integrity Only</td>
<td><img src="image" alt="Example Screen" /></td>
</tr>
<tr>
<td></td>
<td>• Integrity + Confidentiality</td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT** For more information on the Conduit Security Policy Properties, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.
Limitations and Considerations

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

- **Dual-port Devices**
- **CIP Bridging**
- **ControlLogix Redundancy Systems**
- **Network Address Translation**
- **Automatic Device Replacement**
- **RSLinx Classic Software**

### Dual-port Devices

Some CIP Security-capable products have dual built-in Ethernet ports. On these devices, the two physical Ethernet ports share one IP address.

You configure CIP Security based on IP address, not physical port. On CIP Security-capable devices with dual built-in Ethernet ports, it does not matter which physical port is connected to a network. When a CIP Security policy is deployed, the security configuration applies to either port, depending on which port is connected to the network.

For example, a 1756-EN4TR communication module has dual built-in Ethernet ports with one IP address. Once you configure CIP Security for the module, port 1 or port 2 can physically be connected to the network and the CIP Security configuration still applies.

On devices with dual built-in Ethernet ports that are CIP Security-capable, you **cannot** configure separate CIP Security policies for the different Ethernet ports on the same device.

### IMPORTANT

Some Rockwell Automation products with dual built-in Ethernet ports let you configure separate IP addresses for each port, for example, CompactLogix 5380 controllers. However, those products are not CIP Security-capable devices.
CIP Bridging

You **cannot** configure CIP Security through a CIP bridge.

For example, in the following graphic, you can configure Kinetix 5700 Drives_1 and Kinetix 5700 Drives_2 for CIP Security because the Stratix® 5400 switch is transparent.

You **cannot** configure Kinetix 5700 Drive_3 for CIP Security because it is accessed through a 1756-EN4TR communication module, across the ControlLogix backplane and out the other 1756-EN4TR communication module. The **backplane is a bridge** between the communication modules.
Network Address Translation

Network Address Translation (NAT) is supported with CIP Security only if the computer/server with FactoryTalk Policy Manager can access the CIP Security endpoint via an IP address. That is, the devices behind the NAT have IP addresses that are accessible from devices on the outside.

In this example, the 1756-EN4TR device in M1 Zone (Machine 1) can use CIP Security because the Stratix 5700 switch performing the NAT contains a NAT translation for the 1756-EN4TR and a Gateway Translation. When NAT with routing is configured correctly in a network, the outside computer/server with FactoryTalk Policy Manager can access the CIP Security endpoint via the Outside translated IP address configured in the Stratix 5700 switch.

It is important that NAT is properly configured before you apply any CUIP Security implementation. For more information, see Deploying Network Address Translation within a CPwE Architecture Design and Implementation Guide, publication ENET-TD007.
### Routing Table

<table>
<thead>
<tr>
<th>VLAN ID - Description</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 - M1 Zone</td>
<td>10.10.10.1</td>
</tr>
<tr>
<td>20 - M2 Zone</td>
<td>10.10.20.1</td>
</tr>
<tr>
<td>30 - Main Zone</td>
<td>10.10.30.1</td>
</tr>
<tr>
<td>40 - PC Zone</td>
<td>10.10.40.1</td>
</tr>
</tbody>
</table>

### VLAN 30

**MAIN Zone**
- **Outside**
- Line Controller 10.10.30.15

### VLAN 10

**M1 Zone**
- **Inside** 192.168.1.x/24

### VLAN 20

**M2 Zone**
- **Inside** 192.168.1.x/24

### VLAN 40

**PC Zone**
- **Outside**
- 10.10.40.100
- FactoryTalk Policy Manager
- FactoryTalk System Services
- FactoryTalk Linx
- 10.10.40.200
- FactoryTalk Linx
- Studio 5000

### Inside to Outside NAT Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Inside</th>
<th>Outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1 1756-EN4TR</td>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

### Gateway Transition

<table>
<thead>
<tr>
<th>Outside</th>
<th>Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

### Inside to Outside NAT Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Inside</th>
<th>Outside</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2 1756-EN4TR</td>
<td>192.168.1.10</td>
<td>10.10.20.10</td>
</tr>
</tbody>
</table>

### Gateway Transition

<table>
<thead>
<tr>
<th>Outside</th>
<th>Inside</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.20.1</td>
<td>192.168.1.1</td>
</tr>
</tbody>
</table>

### Conduit Types

- (Outside) Device to (Inside) Device
- (Inside) Device to (Inside) Device
- (Outside) Device to (Inside) Device and (Outside) Zone to (Outside) Zone
Chapter 2  CIP Security-capable Rockwell Automation Products

ControlLogix Redundancy Systems

Currently, you cannot use Multicast connections with CIP Security. As a result, you cannot use CIP Security in a ControlLogix Enhanced Redundancy system.

Automatic Device Replacement

Currently, you cannot use Automatic Device Replacement (ADR) to replace devices in an IACS that uses CIP Security. If you replace a device, you must redeploy the security policy manually.

RSLinx Classic Software

You cannot use RSLinx Classic software to implement CIP Security in an IACS network. You must use FactoryTalk Linx, version 6.11 or greater.
Chapter 3

CIP Security Implementation Process

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install, Plan, and Design the System</td>
<td>32</td>
</tr>
<tr>
<td>Identify, Organize, and Create Zones</td>
<td>33</td>
</tr>
<tr>
<td>Identify, Organize, and Create Conduits</td>
<td>37</td>
</tr>
<tr>
<td>Identify and Create Security Features/Policies</td>
<td>44</td>
</tr>
<tr>
<td>Deploy Security Model</td>
<td>45</td>
</tr>
<tr>
<td>Back Up CIP Security Model</td>
<td>48</td>
</tr>
<tr>
<td>Remove CIP Security Configuration</td>
<td>49</td>
</tr>
</tbody>
</table>

This section describes the overall process of implementing CIP Security™ with Rockwell Automation® products in a simple IACS.

For information on a more complex IACS, see Chapter 4, CIP Security Implementation Example Architecture on page 57.

You can use the security assessment process to assign security levels to zones and conduits. We recommend that you assign zone and conduit security levels based on the potential consequences should an attack objective be achieved in that zone.

For more information, see Security Assessment on page 10.
You must install software on specific computers and connect hardware devices to EtherNet/IP™ networks.

**IMPORTANT**  FactoryTalk® Policy Manager and FactoryTalk System Services are components of FactoryTalk Services Platform, version 6.11 or later.

- When you install FactoryTalk Services Platform, version 6.11 or later, you must install FactoryTalk Policy Manager and FactoryTalk System Services. You use the Customize option during installation to install FactoryTalk Policy Manager and FactoryTalk System Services.
- You must install FactoryTalk Services Platform and FactoryTalk Linx software on the same computer/server that hosts the FactoryTalk Directory.

Other programming software, for example, Studio 5000 Logix Designer® and FactoryTalk View software are installed on another computer.

At a minimum, the IACS design should include the following information:

- Verification of the system components required to implement CIP Security into the IACS network.

- Inventory of existing devices and software, including firmware revisions.

- Detailed observation and documentation of intended system functions and operation.

- Detailed observation and documentation of required data flows between devices.

Remember, the system can include products that are CIP Security-capable and products that are not. The list of CIP Security-capable products that are currently available from Rockwell Automation are listed at the following:

- CIP Security Software Applications on page 18
- CIP Security-capable Hardware Devices on page 19
Identify, Organize, and Create Zones

Zones are groups to which devices are added. Devices that share security requirements for a particular function, and you want to trust each other, can be added to the same zone.

When devices are added to the zone, communication between the devices is implied while still letting mutual trust be established through an exchange of certificates or pre-shared keys. It is worth noting that any device in a zone that is deemed to be ‘trusted’ is only trusted by other devices in the same zone, not all devices in the IACS.

For example, if a ControlLogix® 5580 controller and Kinetix® 5700 drives are added to Zone 1 and certificates are used with integrity, the devices are authenticated by exchanging certificates with each other.

Devices that are not CIP Security-capable in the same zone as CIP Security-enabled devices can communicate through standard 44818 TCP connections and 2222 UDP connections. As a result, you are not required to create a whitelist between the devices that are not CIP Security-capable.

You can create zones and add other computers/servers that do not use FactoryTalk Linx software but still require communications to IACS devices. The devices that do not use FactoryTalk Linx are added as generic devices. This lets you easily create Trusted IP conduits between the computers/servers to the IACS devices.

**Figure 5 - System Implementation - Zones**
After you identify and organize the zones, create a detailed security matrix that lists what devices occupy each zone.

Table 6 is a security matrix with zones and devices.

### Table 6 - Security Matrix - Zones and Devices

<table>
<thead>
<tr>
<th>PC Zone</th>
<th>Zone 1</th>
<th>Zone 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ControlLogix 5580 controller</td>
<td>ControlLogix 5580 controller</td>
</tr>
<tr>
<td>FactoryTalk Linx(1)</td>
<td>FactoryTalk Policy Manager</td>
<td>FactoryTalk System Services</td>
</tr>
<tr>
<td>Studio 5000 Logix Designer(2)</td>
<td>FactoryTalk View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1756-EN4TR EtherNet/IP communication module</td>
<td>1756-EN4TR EtherNet/IP communication module</td>
</tr>
<tr>
<td></td>
<td>Kinetix 5700 Servo drives</td>
<td>Kinetix 5700 Servo drives</td>
</tr>
<tr>
<td></td>
<td>PanelView Plus terminal(3)</td>
<td>PanelView Plus terminal(3)</td>
</tr>
<tr>
<td></td>
<td>PowerFlex® 755T drive(3)</td>
<td>PowerFlex 755T drive(3)</td>
</tr>
</tbody>
</table>

(1) This group of software is installed on the same server/computer.

(2) This software is installed on a separate computer than FactoryTalk Linx, FactoryTalk Policy Manager, and FactoryTalk System Services.

(3) This device is not CIP Security-capable.

### Create a Zone

1. In the FactoryTalk Policy Manager navigation bar, choose **Zones**.
2. On the toolbar next to **ZONES**, click [+].
A zone is added to the list with the following default values:

- **Name** - Zone 
- **Description** - None

3. Add devices to the zone. You can add devices in three ways:

- Discover devices via FactoryTalk Linx.
- Manually add devices.
- Add all devices in an IP address range.
Configure the Zone

1. In the FactoryTalk Policy Manager navigation bar, choose Zones.
   The ZONES column displays a list of the configured zones.
2. In the ZONES column, choose a zone.
3. Change the properties of the zone as appropriate.

If a zone includes devices that are not CIP Security-capable, a warning notification appears in the zone properties. A whitelist is not needed, however. This device is automatically whitelisted by all of the CIP Security-capable devices in the zone.

For more information on zones, see the following:
- FactoryTalk Policy Manager software online help
- FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001
Identify, Organize, and Create Conduits

Conduits create explicit trusted communication pathways between zones, zones and devices, and between devices in separate zones. After you create, identify, and organize the conduits, update the security matrix to detail the conduits.

Figure 6 - System Implementation - Conduits

Table 7 is an example of an updated security matrix after conduits are identified and organized.

In the table, the Source row and Destination column cell intersections represent the endpoints of the Conduit between the zones. For example, cell at column 2/row 3 indicates that Conduit 2 uses a Zone-to-Zone pathway between PC Zone and Zone 2.

Table 7 - Security Matrix - Conduits

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>PC Zone</th>
<th>Zone 1</th>
<th>Zone 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Zone</td>
<td>Permit(^{(1)})</td>
<td>Conduit 1: Zone-to-Zone</td>
<td>Conduit 2: Zone-to-Zone</td>
<td></td>
</tr>
<tr>
<td>Zone 1</td>
<td>Conduit 1: Zone-to-Zone</td>
<td>Permit</td>
<td>Denied</td>
<td></td>
</tr>
<tr>
<td>Zone 2</td>
<td>Conduit 2: Zone-to-Zone</td>
<td>Denied</td>
<td>Permit</td>
<td></td>
</tr>
</tbody>
</table>

\(^{(1)}\) Default permits pathway.
Create a Conduit

1. In the FactoryTalk Policy Manager navigation bar, choose Conduits.
2. On the toolbar, click [+].

The CONDUIT PROPERTIES pane opens.

3. In Endpoint 1, next to Select an endpoint, choose Browse for Endpoint [...].
4. Select the **endpoint**.

You can choose a zone or device to assign as the first endpoint of the conduit.

**TIP** In Filter, you can type part of the name to list only endpoints that match that criteria.

5. Click OK.
6. In Endpoint 2, next to Select an endpoint, choose Browse for Endpoint [...].

7. To assign as the second endpoint of the conduit, choose a zone or device.

You can choose a zone or device to assign as the second endpoint of the conduit.

**TIP** In Filter, you can type part of the name to list only endpoints that match that criteria.
8. Click OK.

9. Click Next.
The first conduit appears in the Conduits list.

If you need to create another conduit, repeat the process, starting at step 2 on page 38.

**Configure the Conduit**

1. In the FactoryTalk Policy Manager navigation bar, choose Conduits, and choose the conduit that you want to configure.

   **TIP**  
   **CONDUIT PROPERTIES** is automatically opened to the most recently configured conduit.  
   To edit another conduit, select a conduit from the list to display its properties.
2. Change the conduit properties as needed.

If both endpoints are CIP Security capable, configure **CIP Security Communication**.

- **In I/O Data Security and Messaging Security** choose one of the following:
  - Integrity only - Use to check if the data or message was altered and reject altered information.
  - Integrity & Confidentiality - Use to check integrity plus encrypt the data or message so the corresponding decryption key is required to read the information. Rejects altered and/or untrusted information while also protecting the confidentiality of the information.

- **In I/O Data Security**, click None to stop using additional security checks on I/O data.

For more information on conduits, see the following:
- FactoryTalk Policy Manager software online help
- FactoryTalk Policy Manager Getting Results Guide, publication **FTALK-GR001**
Identify and Create Security Features/Policies

Security policies are created based on device capabilities and operational functions of automation applications.

**Figure 7 - System Implementation - Security Policies**

After you identify and create security features/policies, update the security matrix that details applicable security policies between conduits. For example, enable certificates or pre-shared keys, enable/disable confidentiality and whitelisting.

Table 8 is an updated security matrix with security features and policies defined.

<table>
<thead>
<tr>
<th>Conduit 1</th>
<th>Zone to Zone</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure FactoryTalk Linx Communication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone to Zone (Secure communication with FactoryTalk Linx.)</td>
<td>PC Zone</td>
<td>Zone 1 • Certificates • Integrity • Confidentiality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Conduit 2</th>
<th>Zone to Zone</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secure FactoryTalk Linx Communication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone to Zone (Secure communication with FactoryTalk Linx.)</td>
<td>PC Zone</td>
<td>Zone 2 • Certificates • Integrity • Confidentiality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusted IP (whitelisting)</th>
<th>Zone/Device to Zone/Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Non-CIP Security-capable devices)</td>
<td></td>
</tr>
<tr>
<td>PC Zone Device - FactoryTalk Network Manager (IP address: xxx.xxx.xxx.xxx)</td>
<td></td>
</tr>
<tr>
<td><strong>Zone 1 - Devices</strong></td>
<td></td>
</tr>
<tr>
<td>• Kinetix 5700 drive (IP address: xxx.xxx.xxx.xxx)</td>
<td></td>
</tr>
<tr>
<td>• ControlLogix 5580 controller (IP address: xxx.xxx.xxx.xxx)</td>
<td></td>
</tr>
<tr>
<td>• 1756-EN4TR module (IP address: xxx.xxx.xxx.xxx)</td>
<td></td>
</tr>
<tr>
<td>• PanelView Plus terminal: (IP address: xxx.xxx.xxx.xxx)</td>
<td></td>
</tr>
<tr>
<td>• PowerFlex 755T drive (IP address: xxx.xxx.xxx.xxx)</td>
<td></td>
</tr>
</tbody>
</table>

| **Zone 2 - Devices** | | |
| • Kinetix 5700 drive (IP address: xxx.xxx.xxx.xxx) |
| • ControlLogix 5580 controller (IP address: xxx.xxx.xxx.xxx) |
| • 1756-EN4TR module (IP address: xxx.xxx.xxx.xxx) |
| • PanelView Plus terminal: (IP address: xxx.xxx.xxx.xxx) |
| • PowerFlex 755T drive (IP address: xxx.xxx.xxx.xxx) |
Deploy Security Model

After the zones, conduits, and devices security policies have been configured, the resulting security model can be deployed.

You click the Deploy button in FactoryTalk Policy Manager software to trigger FactoryTalk System Services to deploy the security model. FactoryTalk System Services runs in the background. You do not take action in the client.

Before a deployed security policy becomes active, communication must be reset to all configured devices, resulting in a short loss of connectivity.

Once the security model is deployed and active, that is, communication is reset on a device, the device only accepts communication from other devices in the same zone or using conduits that are configured to enable communication with other security zones or devices.

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

After the security model is deployed and active on all affected devices, FactoryTalk Policy Manager and FactoryTalk System Services are no longer required for real-time operations. They are required again if changes to the security model must be deployed.

To deploy the model, complete the following steps.

1. On the FactoryTalk Policy Manager toolbar, select Deploy.
2. Review the **Deploy** dialog box.

The list of devices identifies the devices to be configured when this model is deployed.

**IMPORTANT** If the list contains unexpected devices, click CANCEL and then change the model as needed.

3. Choose one of the following options for when to reset the communication channels for the items included in the security policy model.

The following types of deployment are available:
- **During deployment** - The CIP connection is closed and reopened on the device during the deployment process.

Similar to when the network card on a computer is reset, the device stays functional but is disconnected from the network for a few moments. This option applies the new policy to the device at the same time that the policy is deployed.
- **After deployment** - Security policy settings are deployed to the device but are not in effect until the communication ports are reset.

This option is useful if there is a scheduled maintenance reset process in your environment that can be relied upon to perform this function.
4. Click DEPLOY.

The Results pane updates with the results of the deployment as it occurs. After deployment is complete a summary report is provided listing the successes, failures, and errors encountered during the process.

For information on how to deploy a security model, see the FactoryTalk Policy Manager Getting Results Guide, publication FTALK-GR001.
Back Up CIP Security Model

You are not required to back up the CIP Security model. However, we strongly recommend that you back up the model.

Back up FactoryTalk System Services to save a copy of the security model and its associated certificates. After the model has been created, the FactoryTalk System Services backup file is included with the FactoryTalk Services Platform backup when it is performed.

**IMPORTANT** You must have Administrator privileges to back up FactoryTalk System Services.

To back up the security model, complete the following steps.

1. Open a command prompt as an Administrator.
2. In the command prompt window type:
   ```
   cd C:\Program Files (x86)\Rockwell Software\FactoryTalk System Services
   ```
3. Run the backup utility by typing one of the following commands:
   - `FTSSBackupRestore -B`
     Creates a plaintext backup of the data.
   - `FTSSBackupRestore -B -PW "password"`
     Creates an encrypted backup of the data using the password that is supplied in quotation marks. This password must be supplied to restore the data.
4. The file backup.zip file is created. The file is included in the FactoryTalk Services Platform Backup.

Verify that the file is present in the following location:
`C:\ProgramData\Rockwell\RNAServer\Global\RnaStore\FTSS_Backup`

**TIP** The ProgramData folder is hidden by default in Windows File Explorer.
Remove CIP Security Configuration

If necessary, you can remove the CIP Security configuration from software applications and hardware devices.

Remove the CIP Security Configuration From a Software Application

You can use the following ways to remove the CIP Security configuration from FactoryTalk Linx:

- Via FactoryTalk Policy Manager

  When you use the FactoryTalk Policy Manager method, you not only remove the CIP Security policy configuration from FactoryTalk Linx. But also, the computer with FactoryTalk Linx on it no longer appears in FactoryTalk Policy Manager.

  The FactoryTalk Policy Manager method only works if the computer with FactoryTalk Policy Manager is accessible to the computer with FactoryTalk Linx on it.

- Via FactoryTalk Administration Console

  If the computer with FactoryTalk Policy Manager is not accessible to the computer with FactoryTalk Linx on it, you must use the FactoryTalk Administration Console method.

  When you use the FactoryTalk Administration Console method, you remove the CIP Security policy configuration from FactoryTalk Linx.

  You must then go back to FactoryTalk Policy Manager to delete the computer with FactoryTalk Linx, and then you redeploy the model so that other devices can update their trust models.
Remove Security Configuration From FactoryTalk Linx Via FactoryTalk Policy Manager

1. In the FactoryTalk Policy Manager navigation bar, select Devices, and then select the device.

2. Above the list of devices, click Delete.

3. Deploy the security model as described starting on page 45, and choose to reset the communication channels During deployment.
Remove Security Configuration From FactoryTalk Linx Via FactoryTalk Administration

1. Start FactoryTalk Administration Console for an IACS that is online and has a CIP Security policy in place.
2. At the bottom of the Explorer pane, click the Communications tab.
3. Right-click the FactoryTalk Linx and choose Properties.

The Device Properties dialog box appears.
4. Complete the following steps.
   a. Click the CIP Security tab.
   b. Click the Reset CIP Security.
   c. Click OK.

For more information on how to use FactoryTalk Administration Console, see the software online help.
Remove the Security Configuration From a Device

You can use the following ways to remove the CIP Security configuration from a device:

- Via FactoryTalk Policy Manager - Two methods with this option.
  - Option 1 - Change the device security policies.
  - Option 2 - Delete the device from the model.

The FactoryTalk Policy Manager methods only work if the computer with FactoryTalk Policy Manager is accessible to the device.

- Reset device to factory default settings

If the computer with FactoryTalk Policy Manager is not accessible to the device, you can use this method.

Remove Security Configuration From a Device via FactoryTalk Policy Manager - Option 1

1. In the FactoryTalk Policy Manager navigation bar, select Devices, and then select the device.

   PORT PROPERTIES are displayed.
2. In the **Policies** area, change the security policies for the device. In **Zone**, choose either **Unassigned** or a zone that is not CIP Security enabled.

3. Deploy the security model as described starting on page 45, and choose to reset the communication channels during deployment.

   The device security configuration is reset to none.
Remove Security Configuration From a Device via FactoryTalk Policy Manager - Option 2

1. In the FactoryTalk Policy Manager navigation bar, select Devices, and then select the device.

2. Above the list of devices, click Delete.

3. Deploy the security model as described starting on page 45, and choose to reset the communication channels During deployment.

**IMPORTANT** If the device cannot be reached when the Deploy attempts to clear the security configuration from the device, the attempt fails and the security configuration remains in the device.
Remove Security Configuration From a Device By Resetting Device to Factory Default State

You can remove the CIP Security configuration from a device by resetting the device to its factory default state.

**IMPORTANT**  The methods by which you reset devices to their factory default, and the conditions of each device when it is in its factory default state, vary.

Before you reset a device to its factory default state to remove the security configuration, be aware of the impact the reset can have on your IACS in general.

Resetting a device to its factory default state can affect the overall system in ways unrelated to CIP Security.

For information on how to reset a device to its factory default state, see the technical documentation for the device.
CIP Security Implementation
Example Architecture

This section describes an example IACS with CIP Security™ implemented.

Phase One of Implementation

In the first phase of the CIP Security implementation, you secure communication between the Computer (PC) zone and each IACS zone. The degree to which you secure communication depends on your system needs.

For more information on the CIP Security properties that you can use to secure communication, see Secure Data Transport on page 14.

We recommend that you secure communication between the Computer zone to each IACS zone because it presents the most vulnerabilities from Windows-based operating systems.

In this phase, you complete the following tasks:

- **Create Zones**
- **Create Zone-to-Zone Conduits**
- **Deploy Security Policies**
Create Zones

Create zones and all applicable devices including CIP Security-capable and non CIP Security-capable devices.

- PC Zone (FactoryTalk Site servers and engineering workstations [EWS])
- Cell Zone A (Controller zone)
- Cell Zone B (I/O zone)
- Cell Zone C (Controller zone)

**Figure 8 - CIP Security Architecture - Zones**
Table 9 is a security matrix with zones and devices.

<table>
<thead>
<tr>
<th>PC Zone Software</th>
<th>Cell Zone A</th>
<th>Cell Zone B</th>
<th>Cell Zone C</th>
</tr>
</thead>
<tbody>
<tr>
<td>FactoryTalk Linx(1)</td>
<td>L85_Line1</td>
<td>Kinetix 5700 servo drives_1</td>
<td>L85_Motion</td>
</tr>
<tr>
<td>FactoryTalk Policy Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FactoryTalk System Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Studio 5000 Logix Designer</strong></td>
<td><strong>1756-EN4TR module</strong></td>
<td>Kinetix 5700 servo drives_2</td>
<td>1756-EN4TR module</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PanelView Plus terminal_1(2)</td>
<td></td>
<td>PanelView Plus terminal(2)</td>
</tr>
<tr>
<td></td>
<td>PanelView Plus terminal_2(2)</td>
<td></td>
<td>PowerFlex 755T drive_1(2)</td>
</tr>
<tr>
<td></td>
<td>PowerFlex 755T drive_1(2)</td>
<td></td>
<td>PowerFlex 755T drive_2(2)</td>
</tr>
<tr>
<td></td>
<td>PowerFlex 755T drive_2(2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(1) This group of software is installed on the same server/computer.

(2) This device is not CIP Security-capable.
Create Zone-to-Zone Conduits

1. Create zone-to-zone conduits for secure CIP-connection from the FactoryTalk Linx data server and engineering workstation in the PC zone to each of the respective Controller zones named Cell Zone A, B, and C.
   - PC Zone to Cell Zone A
   - PC Zone to Cell Zone B
   - PC Zone to Cell Zone C

Figure 9 - CIP Security Architecture - Conduits
Table 11 is an example of an updated security matrix after conduits are identified and organized.

<table>
<thead>
<tr>
<th>Source</th>
<th>PC Zone</th>
<th>Cell Zone A</th>
<th>Cell Zone B</th>
<th>Cell Zone C</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Zone</td>
<td>Permit (1)</td>
<td>Conduit 1: Zone-to-Zone</td>
<td>Conduit 2: Zone-to-Zone</td>
<td>Conduit 3: Zone-to-Zone</td>
</tr>
<tr>
<td>Cell Zone A</td>
<td>Conduit 1: Zone-to-Zone</td>
<td>Permit</td>
<td>Denied</td>
<td>Denied</td>
</tr>
<tr>
<td>Cell Zone B</td>
<td>Conduit 2: Zone-to-Zone</td>
<td>Denied</td>
<td>Permit</td>
<td>Denied</td>
</tr>
<tr>
<td>Cell Zone C</td>
<td>Conduit 3: Zone-to-Zone</td>
<td>Denied</td>
<td>Denied</td>
<td>Permit</td>
</tr>
</tbody>
</table>

(1) Default pathway.

Configure Conduit Security Policies

Configure the conduit security policies that use certificates and message integrity in the following ways:

- Between the FactoryTalk Linx software to the ControlLogix® 5580 controller in Cell Zone A (Controller zone).

- Between the FactoryTalk Linx software and the Kinetix 5700 drives in Cell Zone B (I/O zone).

- From the FactoryTalk Linx software to the ControlLogix 5580 controller in Cell Zone C (Controller zone) through a 1756-EN4TR communication module.

Optionally, you can apply Whitelisting from the PC zone to each IP address of the non CIP Security-capable devices.
Figure 10 - CIP Security Architecture - Conduit Security Policies
Table 11 is an example of an updated security matrix after the conduit security policies are configured.

**Table 11 - Security Matrix - Conduit Security Policies Matrix**

<table>
<thead>
<tr>
<th>Secure Linx Communication: Conduits 1, 2, and 3</th>
<th>Zone to Zone</th>
<th>Security Policy</th>
</tr>
</thead>
</table>
| **Zone to Zone** (Secure communication with FactoryTalk Linx.) | PC Zone | Cell Zone A | • Certificates  
• Integrity  
• Confidentiality |
| | PC Zone | Cell Zone B | |
| | PC Zone | Cell Zone C | |

| Trusted IP (whitelisting) | Zone Device-to-Zone Device | |
|---------------------------|----------------------------|
| (Non CIP Security-capable devices) | PC Zone Device: FactoryTalk Network Manager  
IP address: 192.168.1.100 | Cell Zone A - Devices | • L85_Line1 (192.168.1.8)  
• 1756-EN4TR module (192.168.1.9)  
• PanelView Plus terminal_1 (192.168.1.10)  
• PanelView Plus terminal_2 (192.168.1.11)  
• PowerFlex 755T drive_1 (192.168.1.12)  
• PowerFlex 755T drive_2 (192.168.1.13) |
| | | Cell Zone C - Devices | • L85_Motion (192.168.3.8)  
• 1756-EN4TR module (192.168.3.9)  
• PanelView Plus terminal (192.168.3.10)  
• PowerFlex 755T drive_1 (192.168.3.11)  
• PowerFlex 755T drive_2 (192.168.3.12) |

**Deploy Security Policies**

Deploy the security policies to the devices as described on page 45.
Phase Two of Implementation

In the second phase of the CIP Security implementation, you secure communication between device to device for micro-segmentation. You use the existing zones that are created in the first phase.

Create a Device-to-Device Conduit

Create a device-to-device conduit for secure CIP-connection from the ControlLogix 5580 controller in Cell Zone A (Controller zone) to the ControlLogix 5580 controller in Cell Zone C (Controller zone).

Figure 11 - CIP Security Architecture - Device-to-Device Conduit Added
Create a Zone-to-Device Conduit

Create a zone-to-device conduit from the Kinetix 5700 drives in Cell Zone B (I/O zone) to the ControlLogix 5580 controller in Cell Zone C (Controller zone).

Figure 12 - CIP Security Architecture - Zone-to-Device Conduit Added
Table 12 is an example of an updated security matrix after conduits are identified and organized.

Table 12 - Security Matrix - Device-to-Device and Zone-to-Zone Conduits Added

<table>
<thead>
<tr>
<th>Source</th>
<th>PC Zone</th>
<th>Cell Zone A</th>
<th>Cell Zone B</th>
<th>Cell Zone C</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Zone</td>
<td>Permit(1)</td>
<td>Conduit 1: Zone-to-Zone</td>
<td>Conduit 2: Zone-to-Zone</td>
<td>Conduit 3: Zone-to-Zone</td>
</tr>
<tr>
<td>Cell Zone A</td>
<td>Conduit 1: Zone-to-Zone</td>
<td>Permit</td>
<td>Denied</td>
<td>Conduit 4: Device-to-Device</td>
</tr>
<tr>
<td>Cell Zone B</td>
<td>Conduit 2: Zone-to-Zone</td>
<td>Denied</td>
<td>Permit</td>
<td>Conduit 5: Zone-to-Device</td>
</tr>
<tr>
<td>Cell Zone C</td>
<td>Conduit 3: Zone-to-Zone</td>
<td>Denied</td>
<td>Denied</td>
<td>Permit</td>
</tr>
</tbody>
</table>

(1) Default pathway.
Create Conduit Security Policies

Create the conduit security policies that use certificates, message integrity, and data encryption between endpoints in Conduit 4 and Conduit 5.

Figure 13 - CIP Security Architecture - Conduit Security Policies
Table 13 is an example of an updated security matrix after the conduit security policies are configured.

### Table 13 - Security Matrix - Conduit Security Policies Matrix

<table>
<thead>
<tr>
<th>Secure Linx Communication: Conduits 1, 2, and 3</th>
<th>Zone-to-Zone</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zone to Zone</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Secure communication with FactoryTalk Linx.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC Zone</td>
<td>Cell Zone A</td>
<td>• Certificates</td>
</tr>
<tr>
<td>PC Zone</td>
<td>Cell Zone B</td>
<td>• Integrity</td>
</tr>
<tr>
<td>PC Zone</td>
<td>Cell Zone C</td>
<td>• Confidentiality</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure Controller Communication: Conduit 4</th>
<th>Device-to-Device</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Secure communication with originator and target)</td>
<td>L85_Line1</td>
<td>L85_Motion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secure I/O Communication: Conduit 5</th>
<th>Zone-to-Device</th>
<th>Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Secure communication with originator and target)</td>
<td>L85_Motion</td>
<td>Cell Zone B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusted IP (whitelisting)</th>
<th>Zone Device to Zone Device</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Non CIP Security-capable devices)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC Zone</td>
<td>Cell Zone A - Devices</td>
<td>• L85_Line1 (192.168.1.8)</td>
</tr>
<tr>
<td>Device: FactoryTalk</td>
<td></td>
<td>• 1756-EN4TR module (192.168.1.9)</td>
</tr>
<tr>
<td>Network Manager IP address: 192.168.1.100</td>
<td></td>
<td>• PanelView Plus terminal_1 (192.168.1.10)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PanelView Plus terminal_2 (192.168.1.11)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PowerFlex 755T drive_1 (192.168.1.12)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PowerFlex 755T drive_2 (192.168.1.13)</td>
</tr>
<tr>
<td></td>
<td>Cell Zone C - Devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• L85_Motion (192.168.3.8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1756-EN4TR module (192.168.3.9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PanelView Plus terminal (192.168.3.10)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PowerFlex 755T drive_1 (192.168.3.11)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PowerFlex 755T drive_2 (192.168.3.12)</td>
</tr>
</tbody>
</table>

**Deploy Security Policies**

Deploy the updated security policies to the devices as described on page 45.
Index

A
attack types
- denial of service 9
- man-in-the-middle 9
- monitor data 9
automatic device replacement 30

B
back up
- security model 48

C
certificates 13
CIP bridging 27
CIP Security components 21 - 23
- conduits 23
- devices 21
- zones 22
CIP Security properties
- data confidentiality 15
- data integrity and authentication 15
- device identity and authentication 15
CIP Security-capable
- hardware 19
  - ControlLogix 5580 controllers 19
  - ControlLogix EtherNet/IP communication module (1756-EN4TR) 19
  - Kinetix 5700 drives 19
- software 18
  - FactoryTalk Linx 18
  - FactoryTalk Policy Manager 18
  - FactoryTalk System Services 18
  - Studio 5000 Logix Designer 18
conduits 23, 37 - 43
- configure 42
- create 38 - 42
- security matrix 61
- security policy properties 25
ControlLogix 5580 controllers
- description 19
ControlLogix EtherNet/IP communication module (1756-EN4TR)
- description 19
ControlLogix redundancy 30
countermeasures
- data confidentiality 12
- data integrity and authentication 12
- device identity and authentication 12

d
data confidentiality
- description 15
data integrity and authentication
- description 15
defense-in-depth architecture 11
denial of service attack 9
deploy
- security model 45 - 47
device identity and authentication 13
- certificates 13
- description 15
- pre-shared keys 13
dual-port devices
- limitations with CIP Security 26

F
FactoryTalk Administration
- remove security configuration from FactoryTalk Linx 49, 51 - 52
FactoryTalk Linx
- description 18
FactoryTalk Policy Manager
- description 18
- remove security configuration from a device 53 - 55
- remove security configuration from FactoryTalk Linx 49, 50
FactoryTalk System Services
- description 18

K
Kinetix 5700 drives
- description 19

L
limitations
- automatic device replacement 30
- CIP bridging 27
- ControlLogix redundancy 30
- RSLinx Classic 30
- using dual-port devices 26
- using network address translation 28
Index

M
man-in-the-middle attack 9
monitor data attack 9

N
network address translations
  limitations with CIP Security 28

P
pre-shared keys 13

R
risk assessment 10
  RSLinx Classic 30

S
security assessment
  conduct threat assessment 10
  perform risk assessment 10
  perform vulnerability assessment 10
security configuration
  remove from a device 53 - 56
  remove from FactoryTalk Linx 49 - 52
security matrix
  conduits 61
  zones and devices 34, 59
security model
  back up 48
  deploy 45 - 47
security policy properties
  conduits 25
  zones 24
software
  RSLinx Classic 30
  Studio 5000 Logix Designer
    description 18

T
threat assessment 10

V
vulnerability assessment 10

Z
zones 22, 33 - 36
  configure 36
  create 34
  security matrix 34
  security policy properties 24
Rockwell Automation Support

Use the following resources to access support information.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Dial Codes</td>
<td>Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer.</td>
<td><a href="http://www.rockwellautomation.com/global/support/direct-dial.page">http://www.rockwellautomation.com/global/support/direct-dial.page</a></td>
</tr>
</tbody>
</table>

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.


Allen-Bradley, ControlLogix, FactoryTalk, GuardLogix, Kinetic, Logix 5000, PanelView, POINT I/O, Rockwell Automation, Rockwell Software, Stratix, Studio 5000 Logix Designer, and Trusted, are trademarks of Rockwell Automation, Inc. CIP, CIP Security, EtherNet/IP is a trademark of ODVA, Inc. Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

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

Publication SECURE-AT001A-EN-P - September 2019

Copyright © 2019 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.