CIP Security™ Protocol

Defense in Depth Security

Rockwell Automation

expanding **human possibility**™

PUBLIC

Agenda

1 Why do we care?

2 What are we doing?

3 How are we doing it?

4 Phase approach

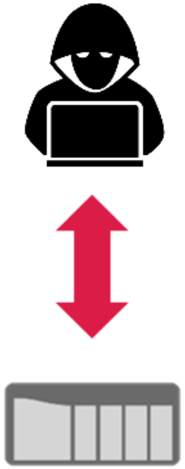
5 Questions

Why do we care?

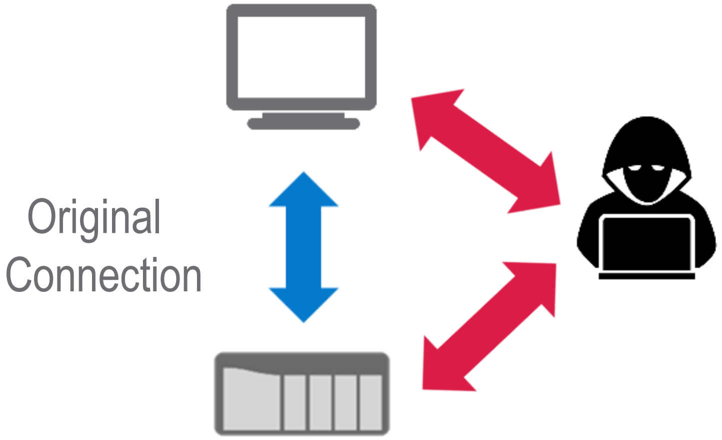
- Historically, Industrial Control Systems (ICS) network protocols lack the security properties necessary to allow a device to “defend itself” against a network/communications attack
  - Lack of authenticity (security), integrity, and confidentially
  - Ethernet/IP™ network protocol, PROFINET, Modbus, etc. all have the same issues
- Secure communications are required for certification to IEC62443, and are identified as a critical capability in most all other publications, standards and frameworks.

Attacker

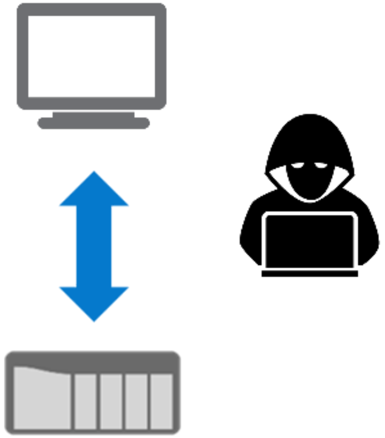
What happens when someone gets into the network?



Direct Connect



Man-in-The Middle (MitM)



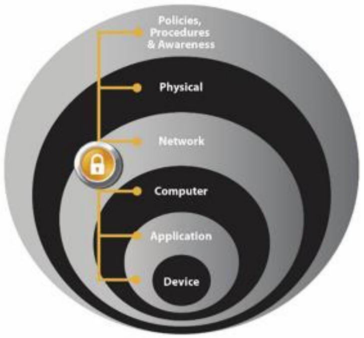
Monitoring Data

Secure communications

CIP Security™ protocol helps provide a secure transport for an EtherNet/IP™ network

- Enables an EtherNet/IP™ connected device to help protect itself from malicious communications
  - Reject messages sent by untrusted people or untrusted devices (authenticity)
  - Reject data that has been altered (integrity)
  - Helps prevent viewing of EtherNet/IP™ data by unauthorized parties (confidentiality)

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

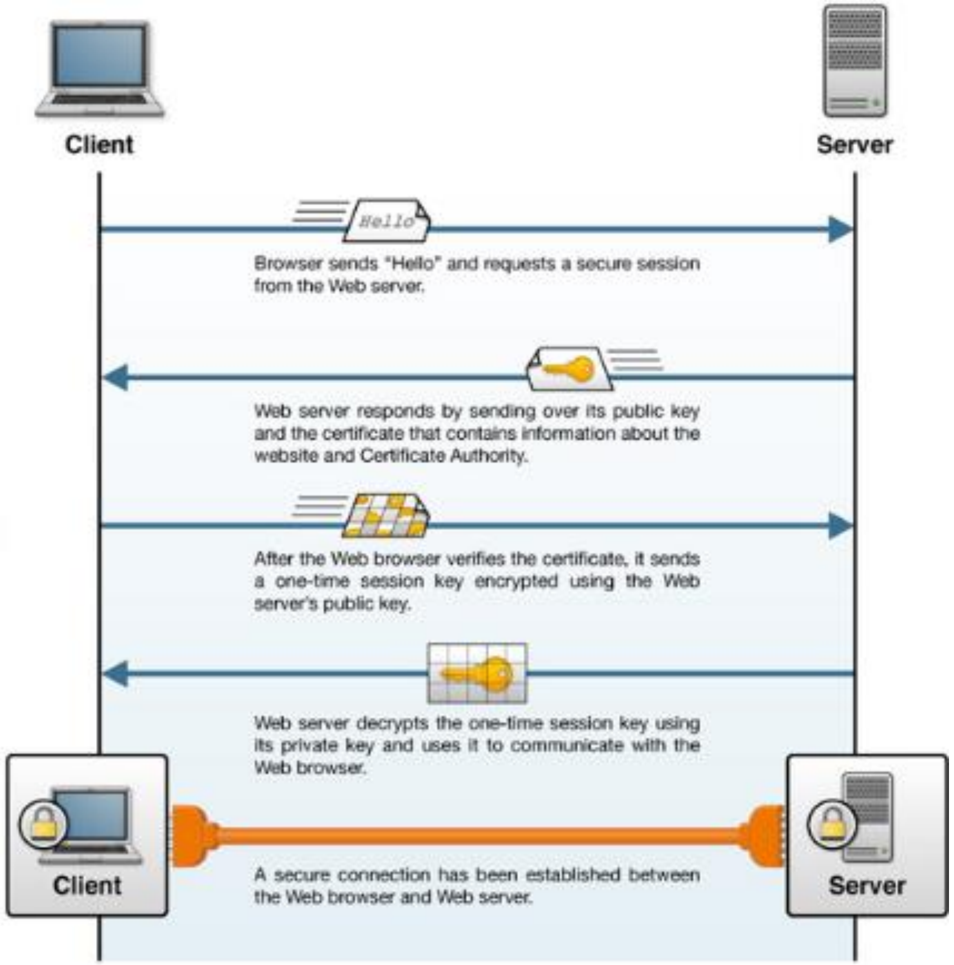


ODVA CIP Security™ protocol

Security property	Volume 8: CIP Security™ Technical Description
Device identity	X.509v3 digital certificates used to provide cryptographically secure identifies to devices
Device authentication	TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security) cryptographic protocols used to help provide secure transport of EtherNet/IP™ traffic
Data integrity	Hashes or HMAC (keyed-Hash Message Authentication Code) as a cryptographic method of providing data integrity and message authenticity to EtherNet/IP™ traffic
Data confidentiality	Data encryption as a means of encoding messages or information to help prevent reading or viewing of EtherNet/IP™ data by unauthorized parties

Leveraging proven technology

Identity, authentication, integrity and confidentiality



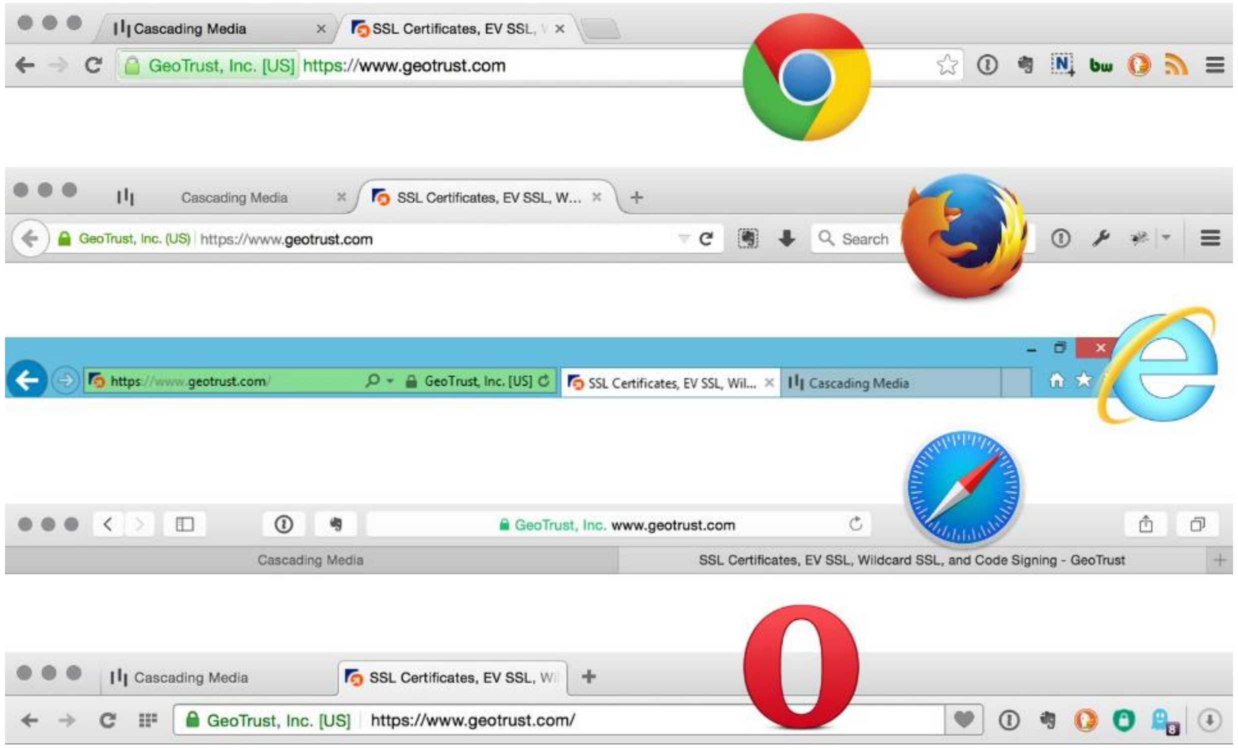
Browser sends "Hello" and requests a secure session from the Web server.

Web server responds by sending over its public key and the certificate that contains information about the website and Certificate Authority.

After the Web browser verifies the certificate, it sends a one-time session key encrypted using the Web server's public key.

Web server decrypts the one-time session key using its private key and uses it to communicate with the Web browser.

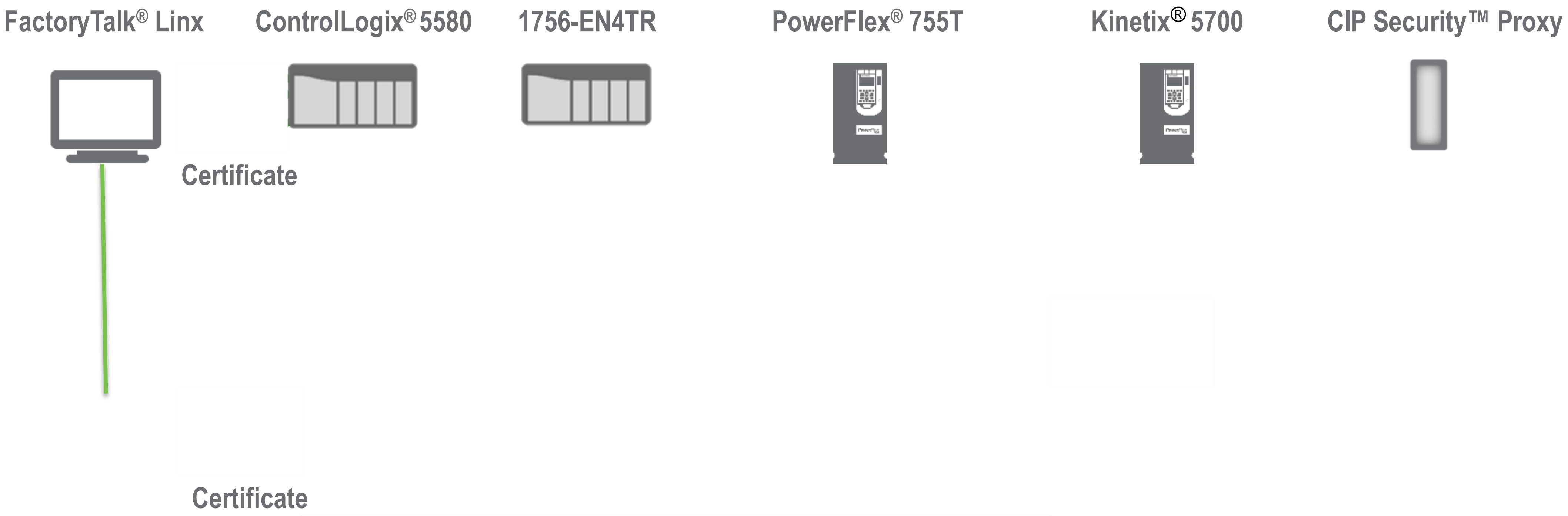
A secure connection has been established between the Web browser and Web server.


Cascading Media
SSL Certificates, EV SSL,
GeoTrust, Inc. [US]
https://www.geotrust.com
Cascading Media
SSL Certificates, EV SSL, W...
GeoTrust, Inc. (US)
https://www.geotrust.com
Search
https://www.geotrust.com/
GeoTrust, Inc. [US]
SSL Certificates, EV SSL, Wil...
Cascading Media
GeoTrust, Inc. www.geotrust.com
Cascading Media
SSL Certificates, EV SSL, Wildcard SSL, and Code Signing - GeoTrust
Cascading Media
SSL Certificates, EV SSL, W
GeoTrust, Inc. [US]
https://www.geotrust.com/

CIP Security™ protocol overview

Secure communications with EtherNet/IP™ network protocol

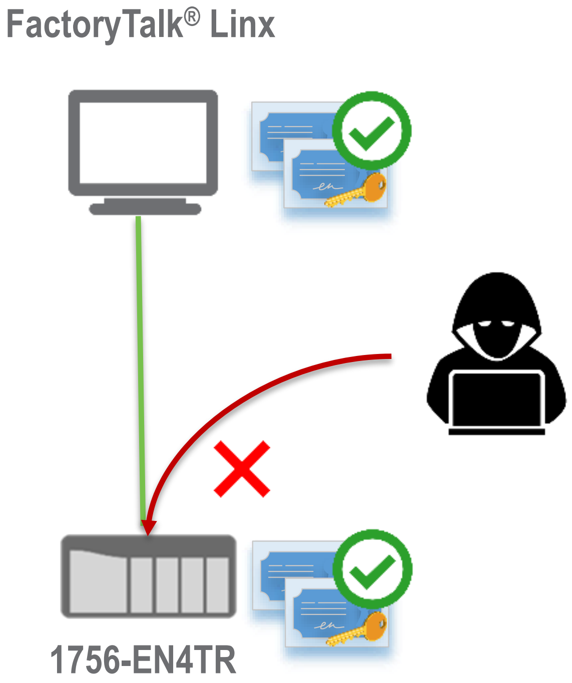
- **Identity, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data
- **Initial products, CIP™ securable products**



CIP Security™ protocol overview

Secure communications with EtherNet/IP™ network protocol

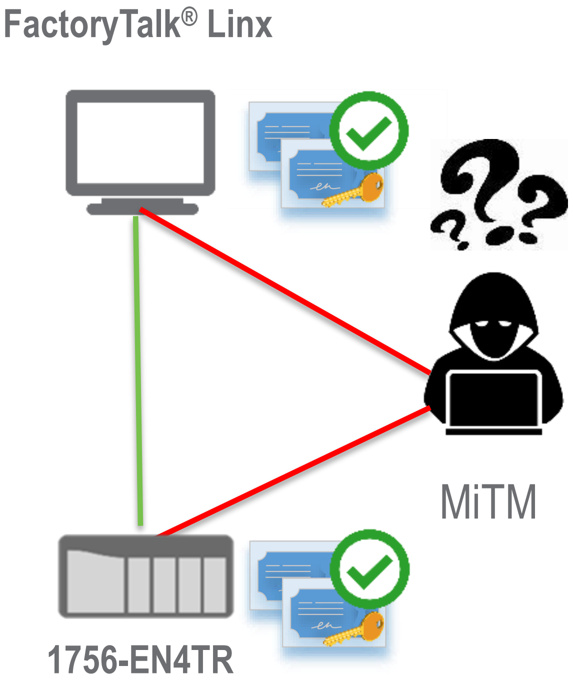
- **Identify, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data



CIP Security™ protocol overview

Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data

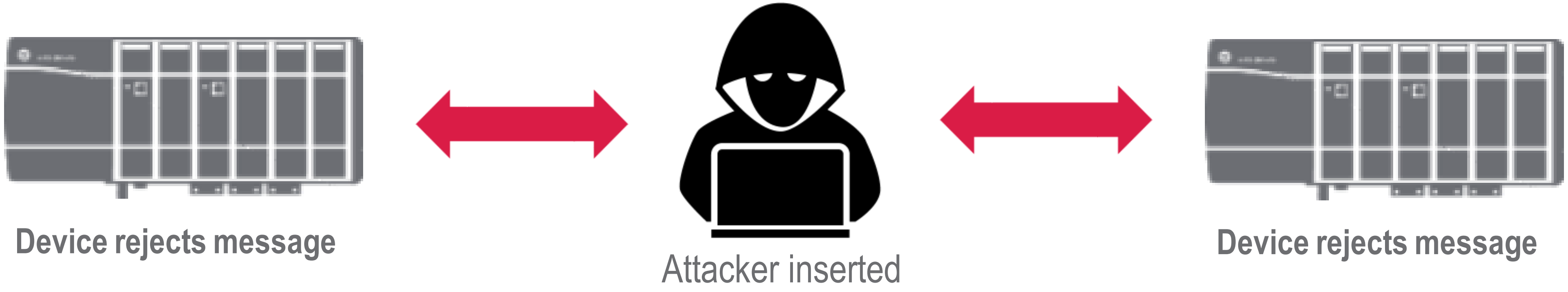


Hacker is able to send commands to the controller

Integrity

HMAC keyed-hash message authentication code

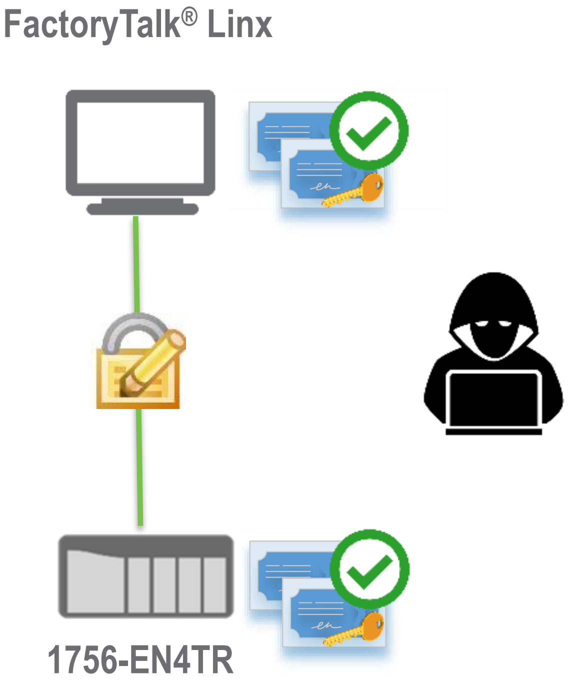
- An HMAC is attached to <u>every message </u>as a means to validate integrity and authenticity
- The message is first “hashed” to provide <u>integrity</u>
  - A mathematical function that maps a message of arbitrary size to a message of fixed size (like a checksum or CRC)
  - It is easy to compute the hash value for any given message
  - It is infeasible to generate a message from its hash (i.e., one way)
  - It is infeasible to modify a message without changing the hash
  - It is infeasible to find two different messages with the same hash
- A secret key is also added to the message before it is “hashed” to provide <u>authenticity</u>
  - You can’t validate the message unless you know the secret
- HMAC is fast and efficient with only a minor performance impact



CIP Security™ protocol overview

Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Help prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data



Now, hacker is not able to modify data, however, can still view it

Data confidentially

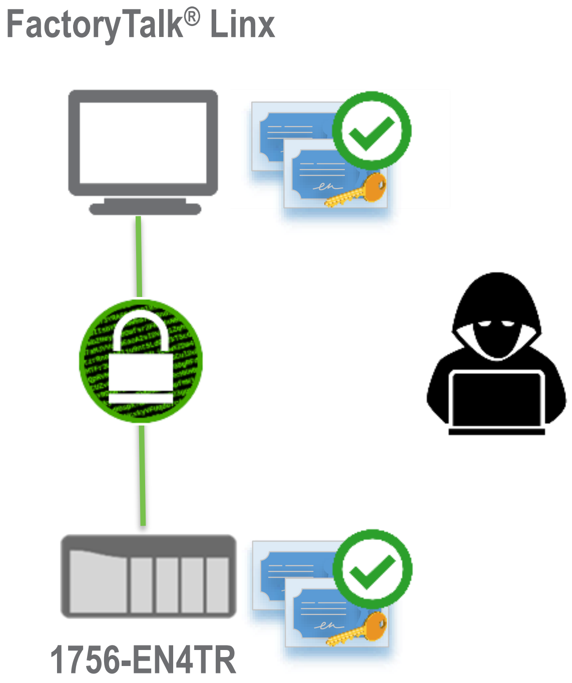
- Encryption can be used as a means of encoding messages or information to help prevent reading or viewing of EtherNet/IP™ data by unauthorized parties (eavesdropping on the wire)
- The encryption method is negotiated as part of the TLS/DTLS "handshake" process

- It is optional
  - Not all ICS traffic contains "secrets" that need to be safeguarded (data integrity and authenticity is typically the goal)
  - The added encryption will impact data throughput performance

CIP Security™ protocol overview

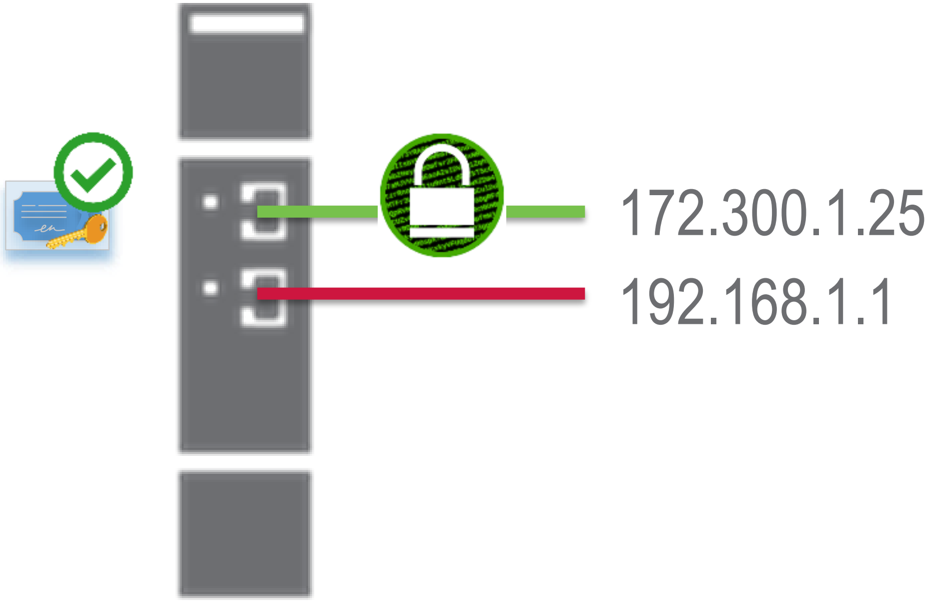
Secure communications with EtherNet/IP™ network protocol

- **Identify, authentication** – Helps prevent unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data



So what exactly am I securing with CIP Security™ protocol?

- The EtherNet/IP™ port itself
- Dual IP ports can contain different security configurations



CIP Security™ protocol overview

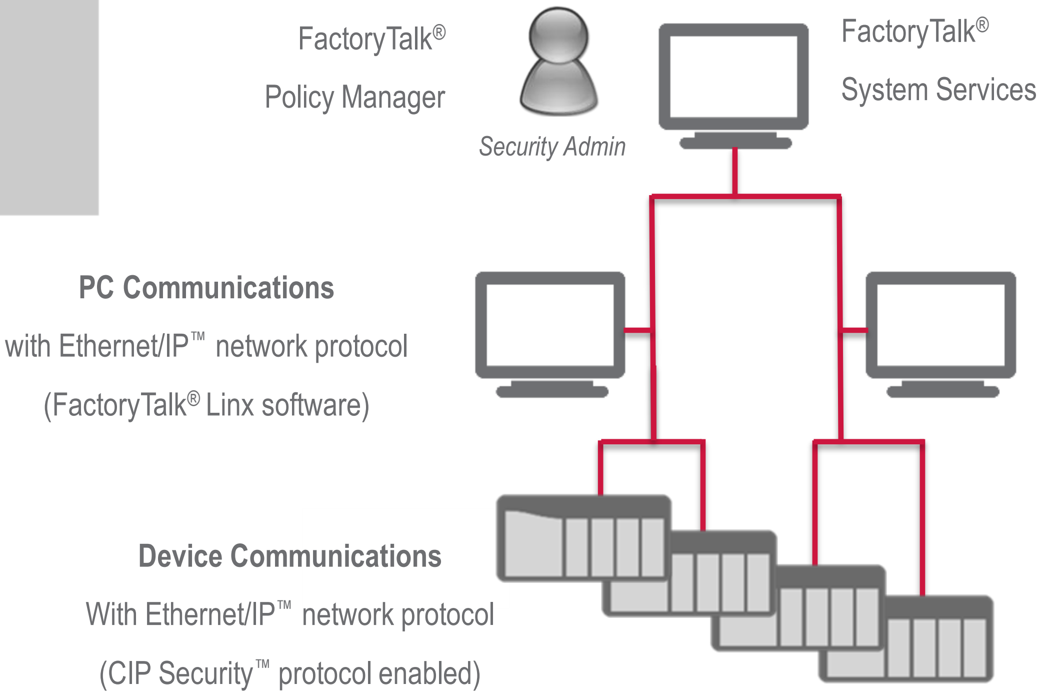
Secure communications with EtherNet/IP™ network protocol

- **Authentication** – Helps prevents unauthorized devices from establishing connections
- **Integrity** – Helps prevent tampering or modification of communications
- **Confidentiality** – Helps prevent snooping or disclosure of data

Notable features:

- **System management**
  - Easily create and deploy security policies to many devices, all at once
- **Micro-segmentation**
  - Segment your automation application into smaller cell/zones.
- **Device-based firewall**
  - Enable/disable available ports/protocols of devices (ie./ HTTP/HTTPS)
- **Initial key products**
  - FactoryTalk® Linx software, ControlLogix® 5580 controllers, 1756-EN4TR ControlLogix® communication module, and Kinetix® 5700 and PowerFlex® 755T drives
- **Legacy Systems Support**
  - Trusted IP – authorize specific communications based on IP address
  - Retrofit 1756 based systems with the new 1756-EN4TR

System Components

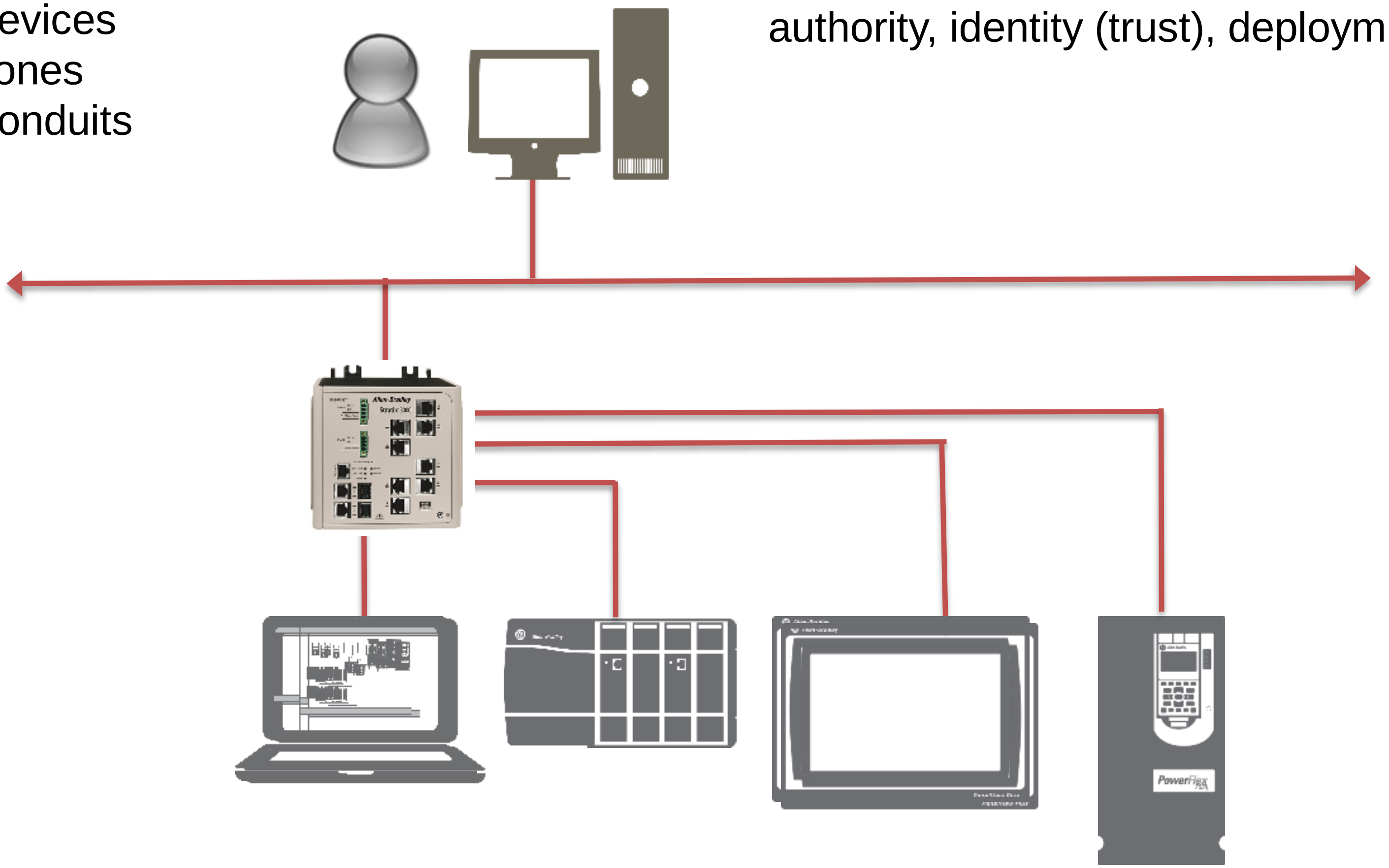

FactoryTalk®
Policy Manager
Security Admin
FactoryTalk®
System Services
PC Communications
with Ethernet/IP™ network protocol
(FactoryTalk® Linx software)
Device Communications
With Ethernet/IP™ network protocol
(CIP Security™ protocol enabled)

Configuration

FactoryTalk® Policy Manager software
Modeling tool concepts

- Devices
- Zones
- Conduits

FactoryTalk® System Services platform
Policy authority (integrity, encryption), certificate authority, identity (trust), deployment, etc.

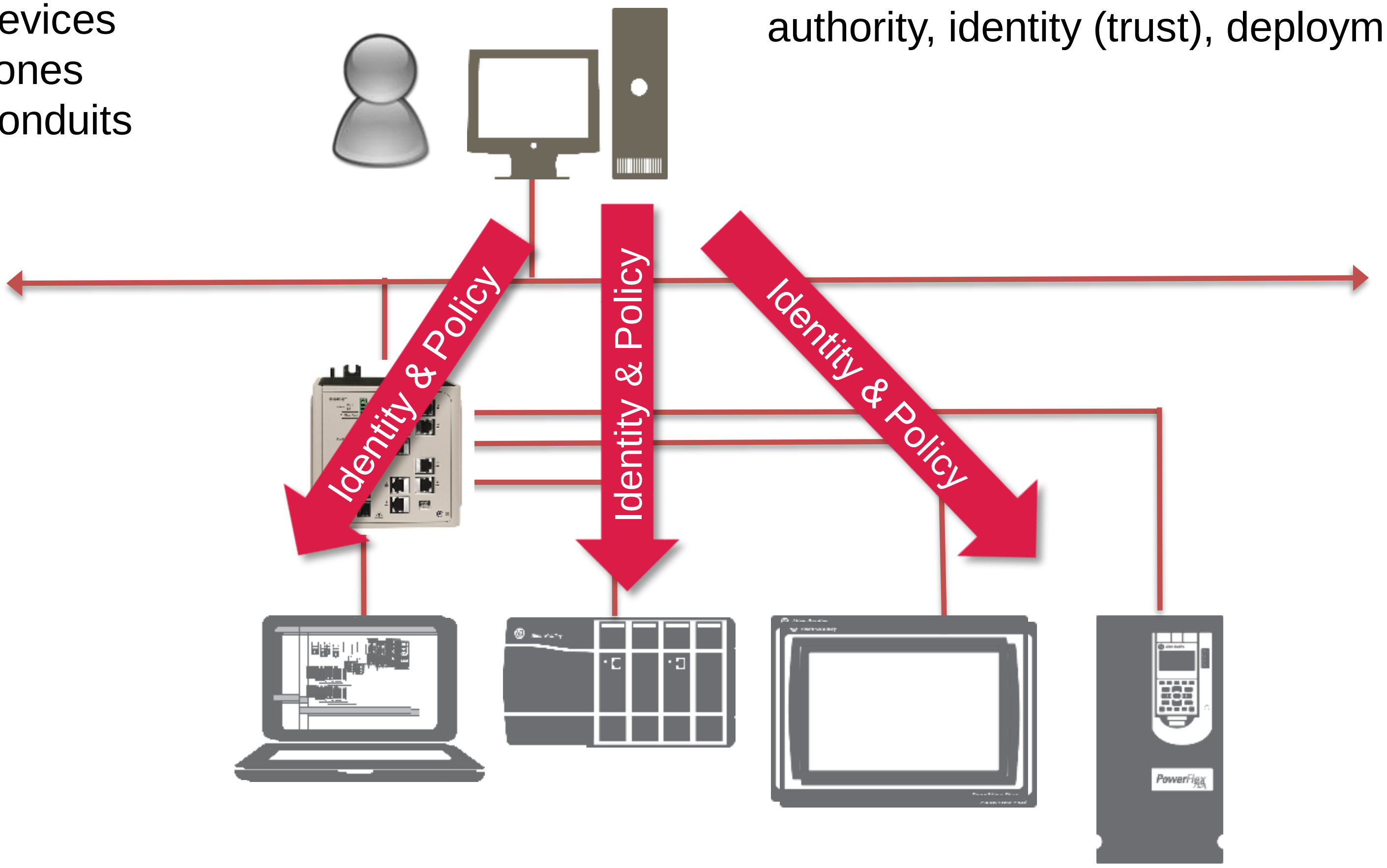


Configuration

FactoryTalk® Policy Manager software
Modeling tool concepts

- Devices
- Zones
- Conduits

FactoryTalk® System Services platform
Policy authority (integrity, encryption), certificate authority, identity (trust), deployment, etc.

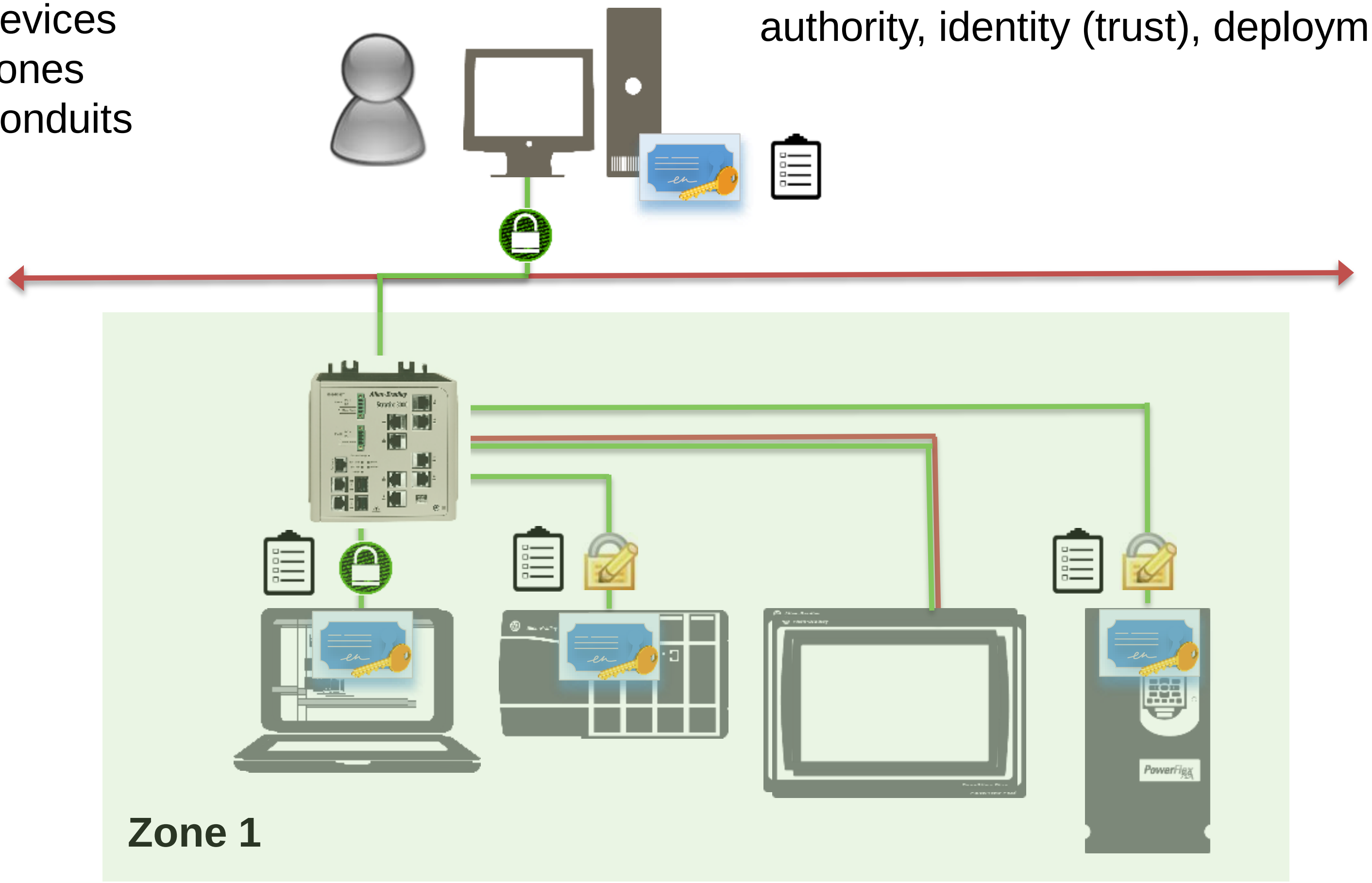


Deployed model

FactoryTalk® Policy Manager software
Modeling tool concepts

- Devices
- Zones
- Conduits

FactoryTalk® System Services platform
Policy authority (integrity, encryption), certificate authority, identity (trust), deployment, etc.

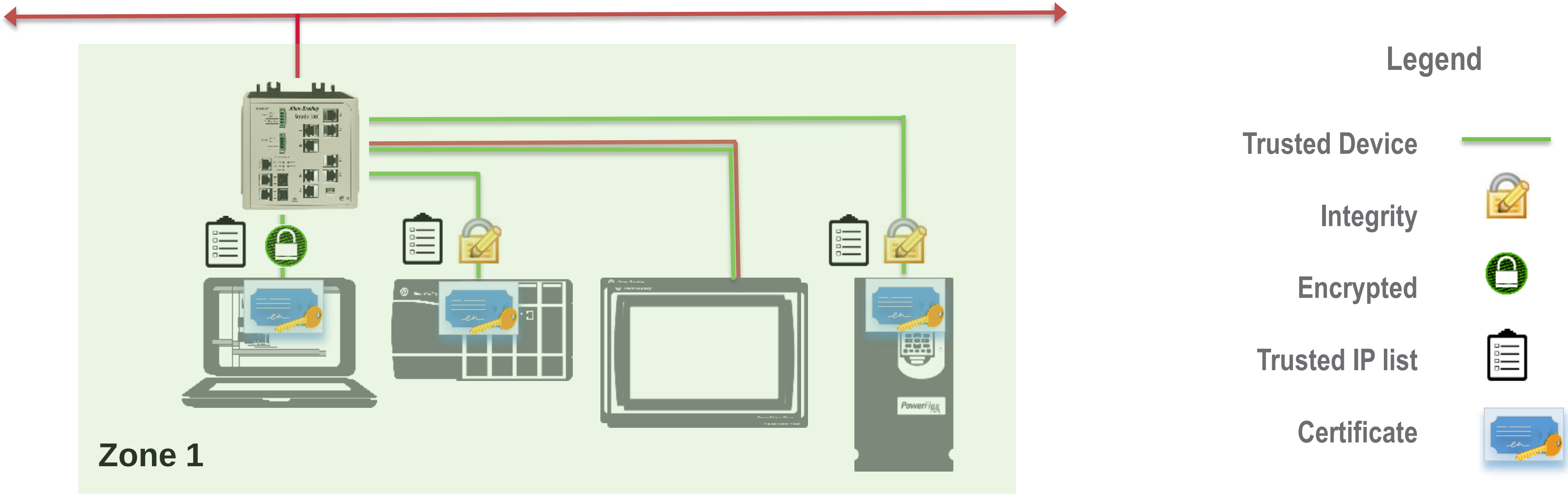


Legend

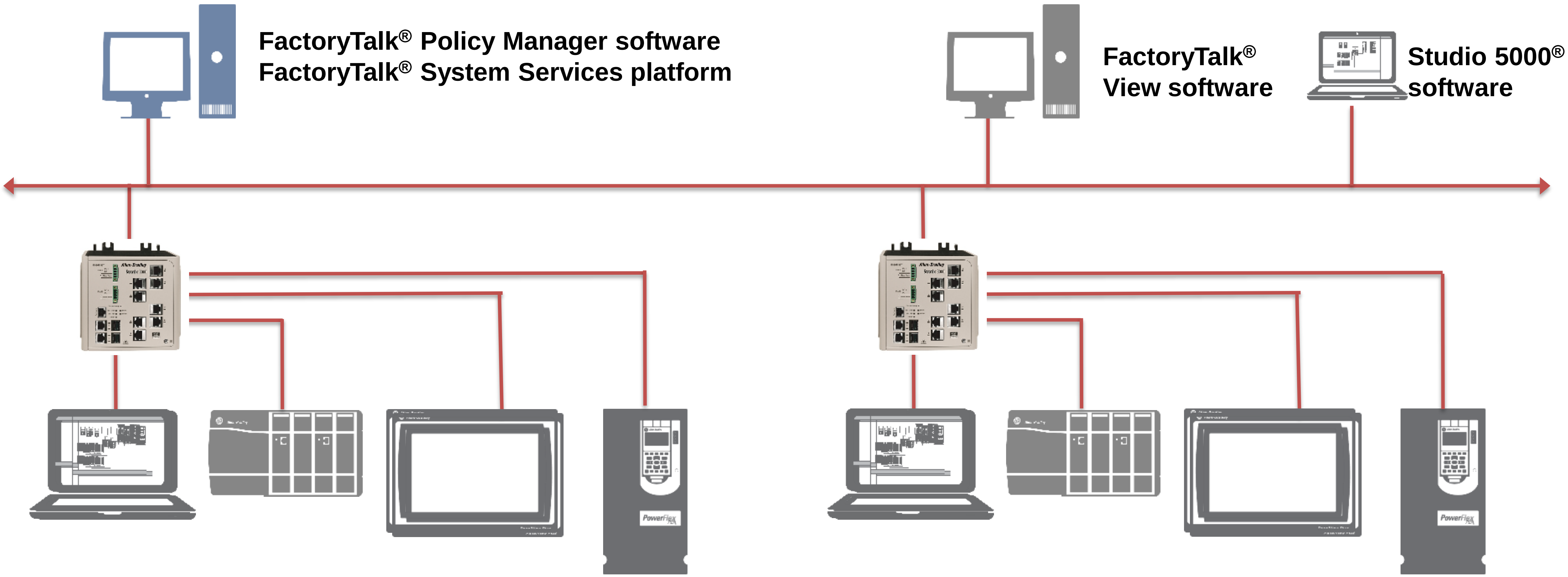
Trusted Device	🟩
Integrity	🔏
Encrypted	🔒
Trusted IP list	📋
Certificate	📜

Deployed model

Once the model has been deployed, **FactoryTalk® Policy Manager** software and the **FactoryTalk® System Services** platform are no longer required. They are only required if additional changes need to be deployed.



Sample deployment

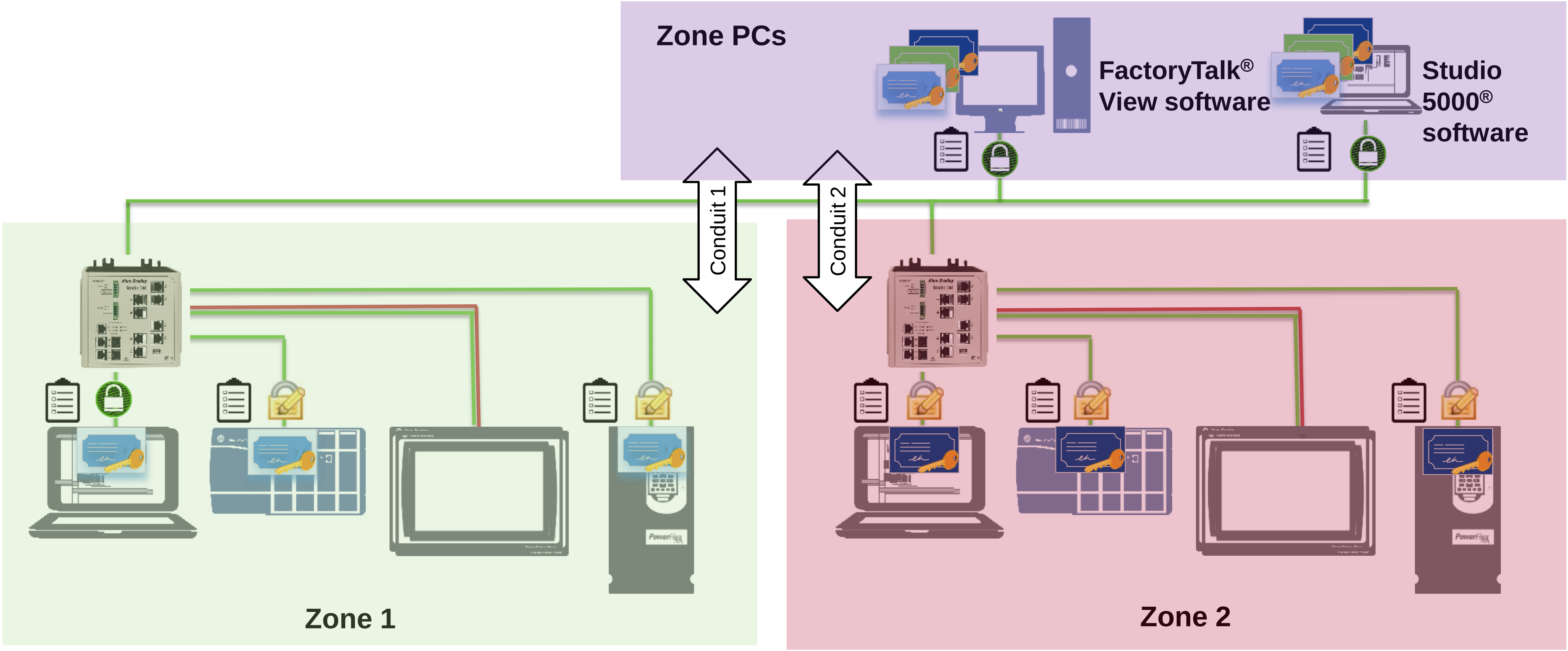


FactoryTalk® Policy Manager software
FactoryTalk® System Services platform

FactoryTalk®
View software

Studio 5000®
software

Sample deployment



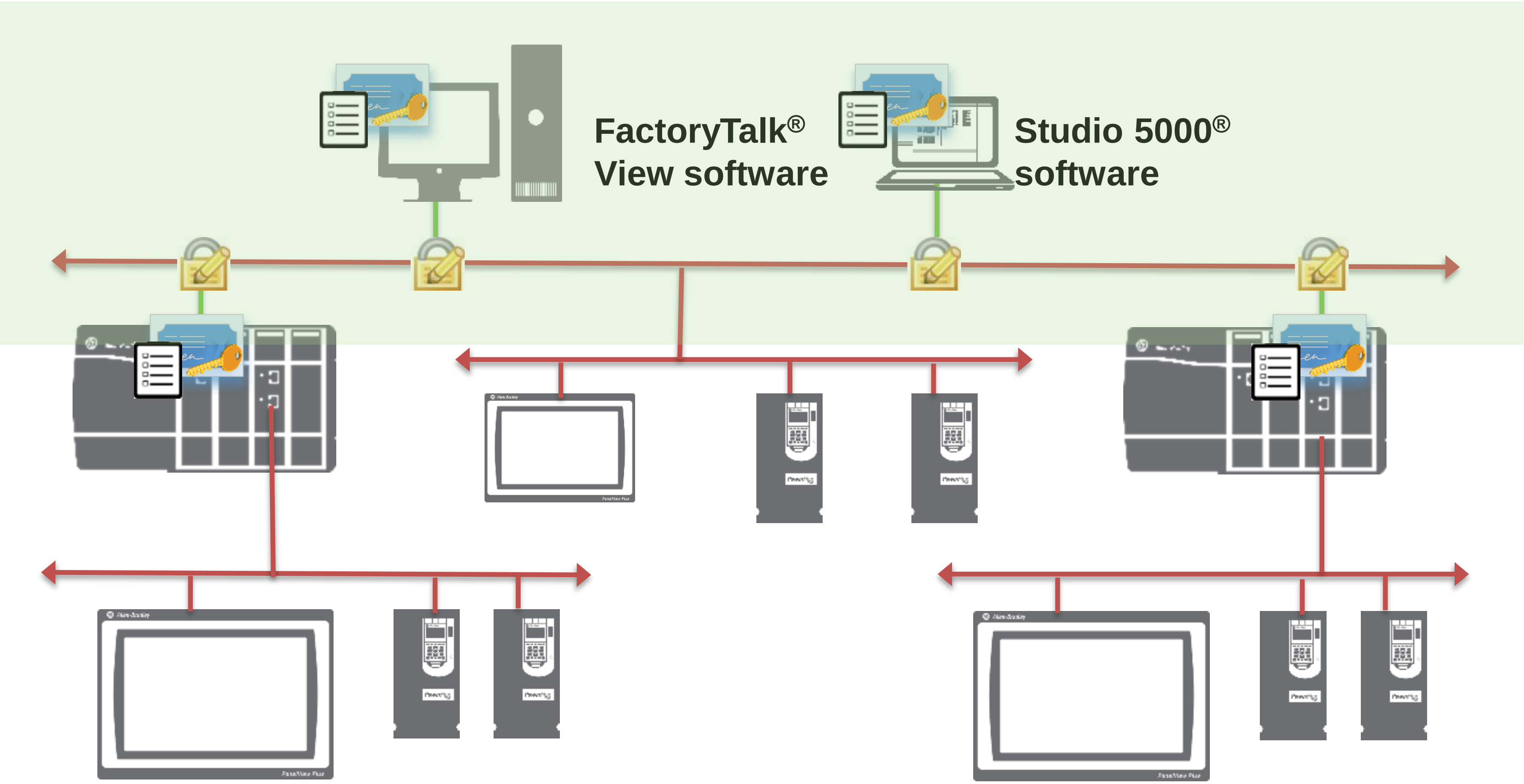
Things to be aware of

Initial Constraints in 2019 (FT Services 6.11.00) Release

- Does not support CIP™ protocol bridging
  - Can’t configure CIP Security™ protocol through a CIP™ bridge
- Does not support high availability
- Does not support Network Address Translation (NAT)
  - Unless the NAT is mapped to a public IP address
- Does not support Automatic Device Replacement (ADR)
- Supports only one NIC if multiple NICs are available in FactoryTalk® Linx software

Use case scenario (Phase I)

- Secure configuration to the controller: computers to controller
- Secure the inbound connection via 1756-EN4TR module or the ControlLogix® 5580 controller itself

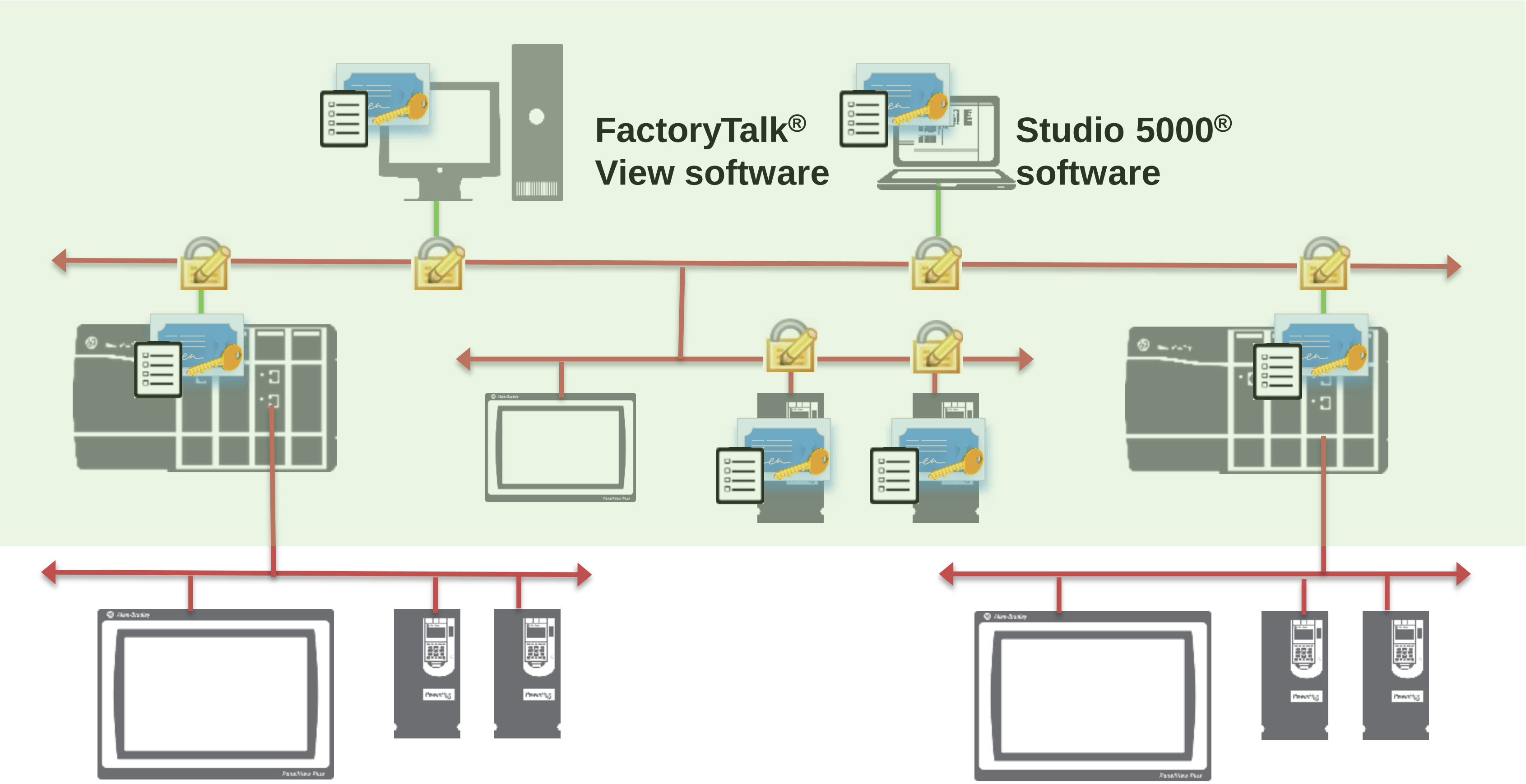


FactoryTalk® View software

Studio 5000® software

Use case scenario (Phase II)

- Extend the model: Add devices to Trusted IP list as appropriate
- Remove devices from Trusted IP list as they become CIP™ securable



Release schedule

Available

- FactoryTalk® Policy Manager software (FactoryTalk® Services Platform version 6.11.00 or later)
- ControlLogix® 5580 controller (version 32 or later)
- 1756-EN4TR ControlLogix® communication module
- Kinetix® 5700 drive

Upcoming

- CIP Security™ proxy, target Q3 2020
- PowerFlex® 755T drive, target Q3 2020

References

- CIP Security with Rockwell Automation Products – Application Technique

https://literature.rockwellautomation.com/idc/groups/literature/documents/at/secure-at001_-en-p.pdf

- System Security Design Guidelines – Reference Manual

https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/secure-rm001_-en-p.pdf

- CIP Security within a Converged Plantwide Ethernet Architecture – White Paper

https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp043_-en-p.pdf

- FactoryTalk Policy Manager – Getting Results Guide

https://literature.rockwellautomation.com/idc/groups/literature/documents/gr/ftalk-gr001_-en-e.pdf

Thank you

www.rockwellautomation.com

Rockwell Automation

expanding **human possibility**™