ODVA®

TECHNOLOGY OVERVIEW SERIES

OVERVIEW OF CIP SECURITY™

CIP Security™

AT A GLANCE

With IT/OT convergence being driven by IIoT and Industry 4.0, ODVA saw the need to enhance the defensive capability of devices connected to EtherNet/IP and other CIP Networks. This added approach is the final level of defense in a defense-in-depth architecture. The ultimate goal is to allow vendors to build interoperable EtherNet/IP devices that can defend themselves, the communications between them, and communications with third parties.

This approach is being realized through CIP Security™, ODVA's enhancement to *The EtherNet/IP Specification* for cybersecurity.

Introduction

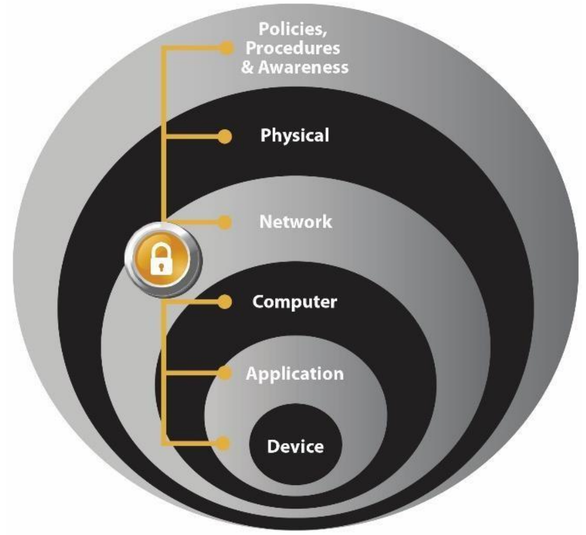
Industrial automation networks were originally developed as a means to simplify the wiring of remote I/O devices and save wiring cost. Over time, this connectivity evolved to allow remote diagnostics and configuration of these devices. The Common Industrial Protocol (CIP™) is a peer-to-peer object-oriented protocol that provides connections between industrial devices (sensors, actuators) and higher-level devices (controllers). CIP has two primary purposes:

- Transport of control-oriented data associated with I/O devices
- Transport of other information that is related to the system being controlled, such as configuration parameters and diagnostics.

These networks were considered secure because they were physically isolated from other networks, they were constrained to geographies that could be secured by physical means (locked doors, etc.) and they could be monitored for unauthorized access. Over time, these once-isolated networks began getting connected with enterprise systems for the purpose of exchanging information to improve productivity, make better use of assets, energy savings and improved decision making. The value of this connectivity is obvious but it comes with certain security risks. These threats include: theft of intellectual property, tampering with plant systems, disruption of plant operations, and possibly damage to equipment.

In order to address these security issues, adoption of a defense-in-depth security architecture has been recommended for many years (see figure below). This architecture is based on the idea that multiple layers of security would be more resilient to attack. The expectation is that any one layer could be compromised at some point in time while the automation devices at the innermost layer would remain secure.

Figure 1: Defense-in-depth



The goal of CIP Security is to improve the defensive capability of the CIP-connected device – the final level of defense – in a defense-in-depth architecture. The ultimate goal of CIP Security is to build CIP devices that are able to defend themselves.

A fully self-defending CIP device would be able to:

- Reject data that has been altered (integrity)
- Reject messages sent by untrusted people or untrusted devices (authenticity)
- Reject messages that request actions that are not allowed (authorization)

CIP Security makes the following basic assumptions:

- The network connected to the device should generally be considered untrusted
- All entities – both people and devices -- that attach to the network are considered untrusted until they can be authenticated
- Network access to a device should not be allowed until authorized by the device
- Physical access to a device will be limited to only trusted individuals (this is not covered by this specification)

Security Threats and Attack Vectors

It is important to understand the security threats and attack vectors to which a CIP device may be subjected, in order to mitigate those threats.

STRIDE is a system developed by Microsoft for thinking about and modeling security threats. It provides a mnemonic for security threats in six categories. The threat categories are:

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

The STRIDE name comes from the initials of the six threat categories listed. It was initially proposed for threat modeling, but is now used more broadly. The Microsoft-developed STRIDE [1] model is a tool that can be used to evaluate security threats.

The following table lists the different STRIDE threat types and security properties that apply to each.

Table 1: STRIDE

Threat Type	Threat Description	Security Property
Spoofing identity	An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.	Authentication
Tampering with data	Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.	Integrity
Repudiation	Repudiation threats are associated with users or devices who deny performing an action without other parties having any way to prove otherwise. Nonrepudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.	Non-repudiation
Information disclosure	Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.	Confidentiality
Denial of service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.	Availability
Elevation of privilege	In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.	Authorization

Given the general description of STRIDE threat types in Table 1, the following table presents the threats that may apply to CIP based devices:

Table 2: Threat Description in CIP Data Flow Mapped to STRIDE

Threat Type	Threat Description in CIP Data Flow	Security Property
Spoofing identity	**Unauthorized session:** An attacker is able to establish a CIP connection to a target device and send arbitrary CIP packets. **Session hijacking:** An attacker is able to hijack an existing CIP connection and send arbitrary CIP packets. **Message replay:** An attacker is able to capture valid CIP packets and replay them at a later time. **Rogue server:** An attacker is able to spoof the identity of a valid server and accept messages from an unknowing client. **Notes** The source of the malicious messages could be the attacker's device connected to the network at a point of attachment (e.g., switch port), or could be a compromised device already on the network.	Authentication
Tampering with data	**Message alteration:** An attacker is able to intercept and alter or drop CIP packets in a man-in-the-middle (MITM) attack.	Integrity
Repudiation	**Log alteration:** An attacker is able to tamper with a local audit log, crash dump file or diagnostic file on a device. The user would have no ability to assure that the file was originally created by a specific device. This is a major concern in regulated industries where validated audit records are common place.	Non-repudiation
Information disclosure	**Message eavesdropping:** An attacker is able to capture CIP messages between two end points and see their contents.	Confidentiality
Denial of service	A number of threats listed above could result in denial-of-service, by virtue of the sending malicious messages to the CIP end point: 1. Unauthorized session 2. Session hijacking 3. Message alteration 4. Message replay	Availability
Elevation of privilege	**Unauthorized change:** An attacker with permissions of "get only" access to a CIP object somehow elevates the permissions to include both "get and set" access. Since CIP does not support user authentication, every user and attacker has the highest access privilege that the object is designed to support. This is the problem that adding user authentication and device authorization will solve.	Authorization

When using STRIDE, the items in the threat-mitigation table below represent possible techniques that can be employed to mitigate the threats shown in Table 2:

Table 3: Possible Techniques to Mitigate Threats

Threat Type	Threat Description in CIP Data Flow
Spoofing identity	Appropriate authentication Protect secret data Don't store secrets
Tampering with data	Appropriate authorization Hashes MACs Digital signatures Tamper resistant protocols
Repudiation	MACs Digital signatures Timestamps Audit trails
Information disclosure	Authorization Privacy-enhanced protocols Encryption Protect secrets Don't store secrets
Denial of service	Appropriate authentication Appropriate authorization Filtering Throttling Quality of service
Elevation of privilege	Run with least privilege

CIP Security Approach

CIP Security specifies security-related requirements and capabilities for CIP devices. CIP Security comprises Volume 8 of *The EtherNet/IP Specification* and includes material that is network-independent as well as material that is CIP network-specific (e.g., EtherNet/IP).

The specification at present is focused on EtherNet/IP, as EtherNet/IP-connected devices represent the largest risk due to enterprise network connectivity. The specification at present defines the mechanisms, common behaviors, and requirements to provide a secure transport for EtherNet/IP communications. Additional CIP Security material will be added to the specification over time to address additional security properties.

It is not required that all CIP Security enabled devices provide support for all CIP Security properties, however, it is very important for customers of CIP Security enabled products to easily determine the security properties that are supported by the products they are purchasing. In order to simplify the ability for a customer to identify which products support a specific set of security features, a set of Security Profiles have been proposed and are shown in the table below.

The EtherNet/IP Confidentiality Profile from the table below
is the only profile supported in the current specification. The CIP Authorization Profile in the table below is shown as an example of a future profile that might be supported.

Table 4: Supported Security Profiles

Security Profile	General Description
EtherNet/IP Confidentiality Profile	Provides secure communications between EtherNet/IP endpoints to assure data confidentiality. Includes the EtherNet/IP Integrity profile as a subset
CIP Authorization Profile	Provides secure communications between CIP endpoints to assure device and user authenticity (future)

Each of the Security Profiles shown in Table 4 is targeted at providing security properties to mitigate the threats described previously as follows:

Table 5: Supported Security Properties

Security Properties	EtherNet/IP Confidentiality Profile	CIP Authorization Profile
Device Authentication	X	X
Trust Domain	Broad – group of devices	Narrow – individual device
Device Identity	X	X (TBD)
Data Integrity	X	
Data Confidentiality	X	
User Authentication		X
Change Detection (Audit)		X
Policy Enforcement (Authorization)		X

The development of the various CIP Security Profiles follows a number of key guidelines:

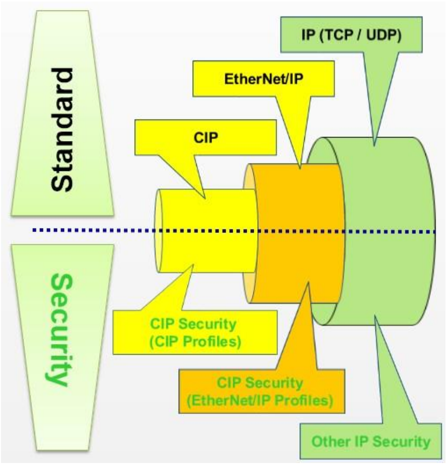
- The EtherNet/IP Security Profiles provide a secure transport mechanism for EtherNet/IP, with relatively little change to the CIP application layer.
- The CIP Security Profile (future) will enhance CIP to provide additional security properties such as user authentication, and potentially extending CIP Security to support other non-EtherNet/IP networks.

CIP Security mechanisms in general should have the following attributes:

- Utilize proven-in-use, open security standards wherever possible
- Provide security options and/or scalable properties compatible with different risk profiles and device capabilities (e.g., apply encryption for confidentiality if required)
- Maximize compatibility with existing network infrastructure (switches, routers, firewalls, etc.)
- Require no custom cryptography to maximize security and minimize any possible import and export restrictions
- Implementations should be available as both commercial and open-source supporting many different OS platforms (embedded, PC, Linux, etc.) where possible
- Devices that support CIP Security must still be able to interoperate with devices that do not support CIP Security, on the same network. It should be a matter of end user configuration to allow or disallow such a mix of devices on the network. When mixing devices with secure and non-secure communications, it is the end user's responsibility to manage the device and network configuration appropriately. The user may need to provide additional controls such as firewalls or physical security means.
- Implementations should be compatible with other IP based security protocols such as IPSec or SSL-based VPN CIP Security should be capable of running over VPN connections to address remote access applications.

Figure 2 shows the relationship between the existing network protocols with no security (CIP, EtherNet/IP and IP) and those that support security enhancement delivered as part of CIP Security:

Figure 2: Security and Standard Network Relationship


Standard
Security
IP (TCP / UDP)
EtherNet/IP
CIP
CIP Security (CIP Profiles)
CIP Security (EtherNet/IP Profiles)
Other IP Security

As Figure 2 illustrates, it is expected that the mechanisms defined for the CIP Profiles would build upon the EtherNet/IP Profiles, and would make use of the secure transport for EtherNet/IP traffic.

Security Technologies

CIP Security makes extensive use of proven-in-use open security technologies such as:

- X.509v3 Digital Certificates used to provide cryptographically secure identities to users and devices
- TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security) cryptographic protocols used to provide secure transport of EtherNet/IP traffic
- Hashes or HMAC (keyed-Hash Message Authentication Code) as a cryptographic method of providing data integrity and message authentication to EtherNet/IP traffic
- Encryption as a means of encoding messages or information in such a way as to prevent reading or viewing of EtherNet/IP data by unauthorized parties

Guide to the Specifications

CIP Security specifies security-related requirements and capabilities for CIP devices and includes material that is CIP network-specific (e.g., EtherNet/IP) in addition to material that is network-independent.

In its present form, the specifications for CIP Security include the following material:

- Chapter 1: Introduction to CIP Security
  The introduction duplicates information found in this technical overview.
- Chapter 2: CIP Security
  CIP security requirements and behaviors that are independent of the particular CIP network. Currently empty, this chapter is expected to include information on CIP-level authentication and authorization.
- Chapter 3: EtherNet/IP Security
  Requirements and behavior specific to EtherNet/IP. Primary material is the mechanism for secure transport over EtherNet/IP using TLS and DTLS.
- Chapter 4: Commissioning and Configuration
  Requirements and behavior related to device security commissioning and configuration.
- Chapter 5: Object Library
  CIP Objects related to security.
- Chapter 6: Certificate Management
  Requirements and behavior related to X.509 certificate usage in devices.
- Chapter 7: EDS Files
  EDS file content specific to security capabilities.
- Chapter 8: Security Profiles
  Explicit definition of requirements and recommendations that define each of the security profiles.

References

[1] https://www.owasp.org/index.php/Application_Threat_Modeling