ODVA™

OPTIMIZATION OF INDUSTRIAL CYBERSECURITY

ODVA'S VISION FOR SECURING THE FLOW OF DATA IN INDUSTRIAL NETWORKS

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY
- INTEROPERABILITY

Executive Summary

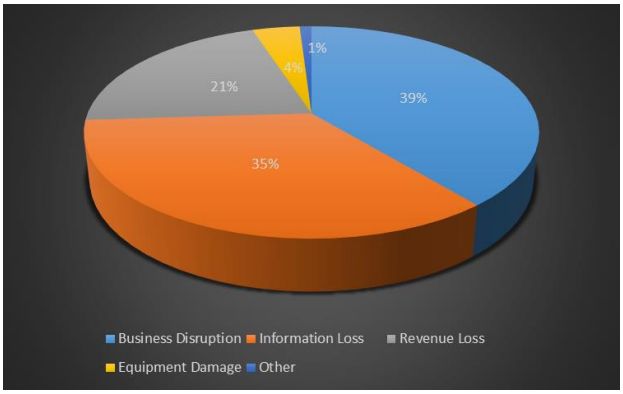

Figure 1
Relative Cost of Cyber Attacks to Industry[2]

In today's connected enterprise, cyber-attacks represent a growing threat to industry. Mitigation of these threats has become an imperative for business, governments and society as a whole. According to the US Department of Homeland Security's ICS-CERT division, cyber-attacks targeting critical infrastructure in the United States rose 20.4 percent in 2015 compared to 2014.[1] Successful cyber-attacks are costly to industry on many levels with business disruption representing the largest component, as shown in Figure 1. For some time ODVA and many others have recommended a defense-in-depth approach to help protect against cyber-attacks on industrial control systems (ICS)[3]. This approach to cybersecurity makes the overall installation more resilient to attack through multiple layers of defense. The objective of this approach is, that while one or more layers of defense could be attacked and possibly compromised, not all layers will be breached. As result, overall risk from cyber-attacks can mitigated and damage to data, systems and components partially or completely avoided.

A missing element of a comprehensive defense-in-depth approach has been the mechanisms to defend the automation networks themselves – for example, the ability for devices to know that the sender or receiver of a message is a trusted entity, or to have cryptographic proof that a message has not been maliciously tampered with while in transit. Recognizing the importance of this missing element, ODVA has been at the forefront of the community of standards development organizations in taking the action to integrate cybersecurity mechanisms into its technology portfolio for automation networks. In November 2015, ODVA published the first of a series of enhancements to its specifications for the implementation of cybersecurity in devices destined for ICS installations that rely on EtherNet/IP™ for communication in automation systems. For industry, the future benefit of these enhancements cannot be underestimated as the number of installations of EtherNet/IP, by some estimates, is approaching that of general purpose Ethernet as shown in Figure 2.

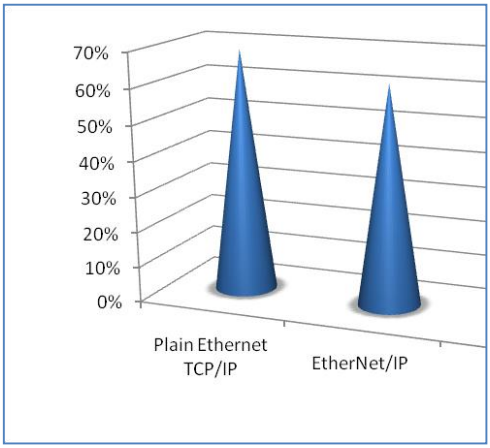

Figure 2
North American Installation of EtherNet/IP and plain Ethernet as of 2014[4]

This white paper describes ODVA's strategy and technical approach to ICS cybersecurity for EtherNet/IP and the Common Industrial Protocol (CIP™) including ODVA's:

- view of cybersecurity in the industrial ecosystem,
- technical approach to ICS cybersecurity; and
- commitment to ICS cybersecurity.

The audience for this paper includes business and technical leadership, IT professionals and plant network architects at industrial companies, as well as product managers at device vendors who are seeking to map out their product roadmaps to support cybersecurity.

ODVA's View of Cybersecurity in the Industrial Ecosystem

Industrial processes and business systems are increasingly interconnected and interdependent. With seemingly little effort, contemporary open networks exchange information, bridging automation systems with corporate infrastructures and the broader Internet. As cyberspace shrinks because of the benefits derived from greater data exchange, new risks to industrial control systems arise and new threats emerge. Left unchecked, products and networks can be exploited by threat actors and pose potentially negative impacts on the safe, reliable and/or secure operation of critical processes and industrial control systems. EtherNet/IP and CIP were engineered with the express intent to improve interconnectivity and the integration of industrial control products from multiple vendors. Thus, ODVA envisions an approach to cybersecurity that encompasses the relevant data flows in the industrial enterprise between the ICS and other systems as depicted in Figure 3.

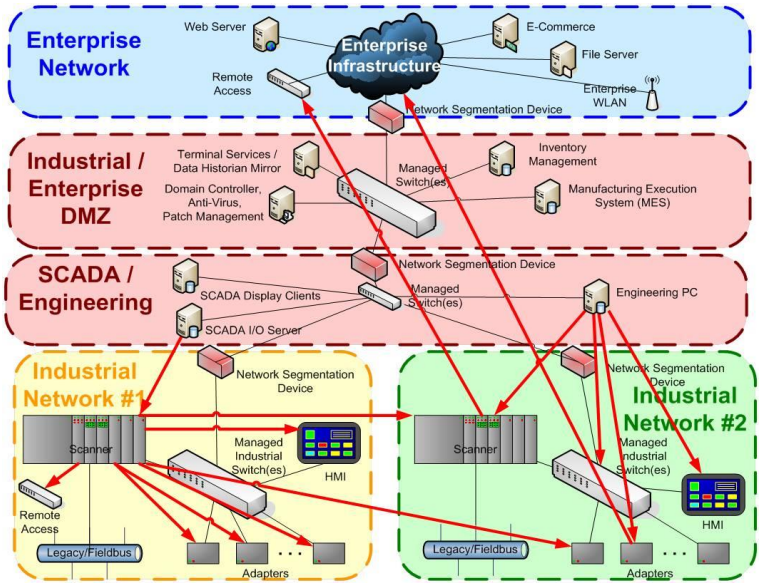

Figure 3
Typical Data Flows in the Industrial Enterprise

Based on its view of typical data flows in the industrial ecosystems, ODVA's approach to cybersecurity for EtherNet/IP and CIP is built on a defense-in-depth approach and based on a four-part working hypothesis:

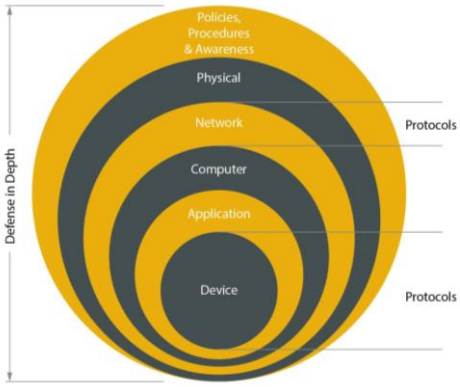

Figure 4
Defense-in-depth

1. Cybersecurity weaknesses will always exist in products, networks and systems, increasing the potential for cybersecurity threats.
2. Stand-alone industrial control assets and systems are quickly disappearing with the convergence of production systems with one another and of production domain with the enterprise and power grid domains.
3. Traditional defense-in-depth practices, including secure protocols, are necessary, but not sufficient, to help mitigate risk from cybersecurity threats and protect data flows between ICS assets.
4. Remote access to the industrial control systems is essential.

ODVA's Technical Approach to ICS Cybersecurity

The goal of cybersecurity enhancements to the ODVA specifications for EtherNet/IP is to extend a defense-in-depth architecture to network communications with and between ICS systems - and with and between ICS systems and edge devices. ODVA's realization of this goal is the enhancement of the potential defensive capability of ICS systems and devices using EtherNet/IP by providing cybersecurity mechanisms that are native to EtherNet/IP and CIP.

ODVA has based these specification enhancements on the following assumptions:

- The network connected to the device should generally be considered to have very limited trust.
- All entities – both people and devices -- that attach to the network should be considered untrusted until they can be authenticated.
- Access to a device over the network should not be allowed until authorized by the device.
- Physical access to a device will be limited to only trusted individuals.

Based on these assumptions, a self-defending EtherNet/IP ICS or device should be able to: (1) reject data that has been altered in any way, functionally referred to as "data integrity"; (2) reject messages that request actions that are not allowed, functionally referred to as "authorization"; and (3) choose to accept or reject messages sent by unknown or untrusted people or untrusted devices based on configuration, functionally referred to as "authenticity".

CIP Security™, ODVA's name for the mechanisms defined in the ODVA specifications for protecting and securing EtherNet/IP and CIP, is based on the security threats and attack vectors to which an EtherNet/IP device may be subjected. Each of these threats can then be paired with security properties that can be employed to help to mitigate the threats. Table 1 summarizes the cybersecurity mechanisms released in the specification enhancements published in November 2015 and those currently planned for future releases. The initial set of enhancements focuses on improving the security of EtherNet/IP-connected devices by adding support for device authentication, data integrity and data confidentiality. The ultimate roadmap, over the next several specification enhancement cycles, is to enable EtherNet/IP devices, and potential other types of devices using CIP, to become autonomous, taking responsibility for their own security and effectively securing themselves from attack as shown in Figure 5.

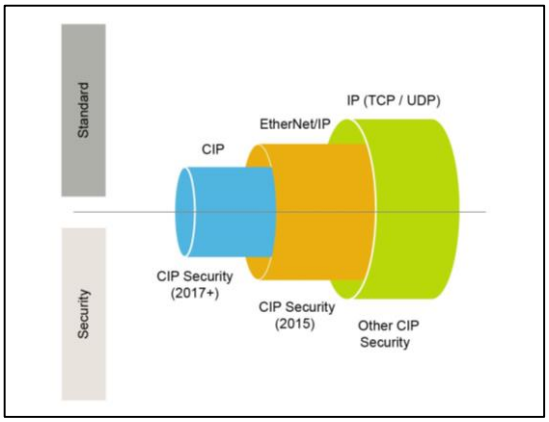

Figure 5
Roadmap for CIP Security

CIP Security™ makes extensive use of proven-in-use open security technologies to deliver these key security properties including:

- 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 authenticity to EtherNet/IP traffic whilst keeping the delays and load on existing devices minimized; and
- Data 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 when required.

Table 1: ODVA Specification Enhancements for CIP Security™

Threat Type (STRIDE[5])	Threat Description	Security Property	Current Specification[5] for CIP Security™	Future Specification Enhancements[5] Planned for CIP Security
Spoofing identity	Illegally accessing and then using another user's or devices authentication information, such as username and password.	Device authorization	✓	
		User authorization		✓
Tampering with data	Malicious modification of data including 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.	Message integrity	✓ **(EtherNet/IP)**	✓ **(CIP)**
		Data integrity (at rest)		✓
Repudiation	Threats 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.	Non-repudiation through audit of events		✓
Information disclosure	Exposure of information to individuals who are not supposed to have access to it.	Message confidentiality	✓	
		Message integrity	✓	
Denial of service	Denying service to valid users.	Availability		✓
Elevation of privilege	Unprivileged user gaining privileged, and thereby 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		✓

ODVA's Commitment to ICS Cybersecurity

ODVA is committed to providing industry with the most appropriate cybersecurity solution to meet the communication needs for industrial control systems while maintaining the interoperability and information access necessary for efficient, future-oriented industrial communication. The vision and roadmap for ODVA's plan for ICS cybersecurity is the result of a lengthy investigation by ODVA and its leadership into the cybersecurity requirements of industry and the value that ODVA can add in helping to meet these requirements.

Two ODVA technical working groups are tasked with the majority of work related to ICS cybersecurity - its Special Interest Group for EtherNet/IP System Architecture and its Special Interest Group for EtherNet/IP Infrastructure – in a multi-year plan for cybersecurity-related specification enhancements delivered in phases as shown in Figure 6.

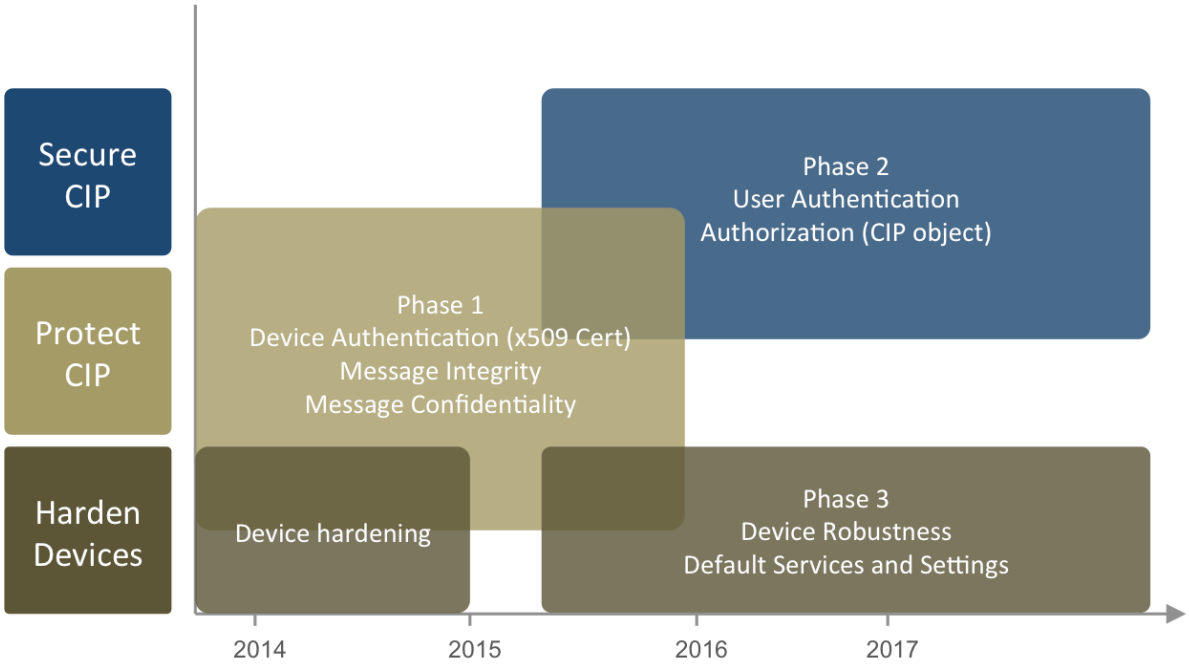

Figure 6
Multi-Year Plan for ODVA's Cybersecurity-related Specification Enhancements

Ultimately, optimization of ICS cybersecurity requires a response, and shared responsibility, by the industry from all stakeholders in the industrial ecosystem – vendors, OEMs, system integrators, end users, and standards development organizations – who must work together as a community to help manage and mitigate risks associated with securing the data found in ICS.

For its part ODVA, with its large community of device suppliers who make and sell products for use in this domain, can contribute an approach to ICS cybersecurity that protects and defends industry against cybersecurity threats in the ICS domain through it its shared vision and focus on common objectives:

- **Confidentiality** of information by securing data in motion;
- **Integrity** of information by protecting data in motion;
- **Availability** of information by hardening device end-points;
- **Interoperability** of multi-vendor systems that have been designed to protect and defend against cybersecurity threats.

About ODVA

Founded in 1995, ODVA is a global association whose members comprise the world's leading automation companies. ODVA's mission is to advance open, interoperable information and communication technologies in industrial automation. ODVA recognizes its media independent network protocol, the Common Industrial Protocol or "CIP" – and the network adaptations of CIP – EtherNet/IP, DeviceNet, CompoNet and ControlNet – as its core technology and the primary common interest of its membership. ODVA's vision is to contribute to the sustainability and prosperity of the global community by transforming the model for information and communication technology in the industrial ecosystem. For future interoperability of production systems and the integration of the production systems with other systems, ODVA embraces the adoption of commercial-off-the-shelf (COTS) and standard, unmodified Internet and Ethernet technologies as a guiding principle wherever possible. This principle is exemplified by EtherNet/IP – the world's number one industrial Ethernet network. For more information about ODVA, visit odva.org.

Footnotes

[1] Grey, Jeff. "Cybersecurity Workshop II: DHS Update." Presenting the 20th Annual ARC Industry Forum Industry in Transition: Navigating the New Age of Innovation. Orlando. 8 Feb. 2016. Speech.
[2] *2015 Cost of Cyber Crime Study: Global*: Ponemon Institute, October 2015.
[3] ODVA, Inc. *Securing EtherNet/IP Networks* (Publication Number 269).: ODVA, 2011.
[4] AW Survey 2014: Ethernet and Wireless in the Plant. Survey. Automation World, 14 January 2015.
[5] STRIDE is an acronym developed by the Microsoft Corporation for collectively describing cybersecurity threats and which is has been generally adopted by the cybersecurity community