Cybersecurity for Industrial Control Systems

ODVA’s Vision for Securing the Flow of Data in Industrial Networks

... confidentiality
... integrity
... accessibility
... interoperability

About ODVA
Founded in 1995, ODVA is a global trade association whose members comprise the world’s leading automation companies that make and sell products compliant with ODVA technologies. ODVA’s mission is to advance open, interoperable information and communication technologies in industrial automation and thus create value for our members, adopters, alliance partners and employees. Recognizing that secure communication over networks is essential for reliable and safe operation of industrial automation, ODVA is committed to help users to address cybersecurity risks and enhance protection of EtherNet/IP assets and CIP data found within industrial control systems. For more information about ODVA and enhancing Cybersecurity in EtherNet/IP systems, visit www.odva.org.
Executive Summary

For the industrial sector, the widespread adoption of Ethernet and internet technologies in industrial control systems ("ICS") has expanded cybersecurity from being dominantly a concern for IT departments charged with securing business information to encompass plant personnel responsible for industrial security systems. This is because, today, Ethernet and internet-enabled ICS are widely adopted across the industrial ecosystem in critical applications from manufacturing to infrastructure. Although lessons learned from securing data found in business systems can be adapted and applied to ICS cybersecurity, the relative importance of primary cybersecurity objectives can differ in the ICS setting. For example, in the ICS setting, the need for accessible data may outweigh the need for confidential data, the opposite of what is often required in many business systems.

Thus, it is critical for ODVA to help address cybersecurity risks and enhance protection of data transported on EtherNet/IP and CIP in industrial control systems. Moreover, businesses benefit from implementing a comprehensive approach to ICS cybersecurity with enhanced productivity through increased uptime while concurrently protecting their people, assets and information.

ODVA’s approach to ICS cybersecurity originates from a four-part working hypothesis:
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 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.

In this white paper, ODVA describes an overview of ODVA’s comprehensive approach to ICS cybersecurity for EtherNet/IP and CIP including:
- Data flows in the industrial ecosystem;
- ODVA’s view of cybersecurity for industrial control systems;
- ODVA’s technical approach to ICS cybersecurity; and
- ICS cybersecurity in practice.

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.

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. Nevertheless, 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 between industrial control systems and which would be typical within the industrial ecosystem as depicted in Figure 1.
ODVA’s View of ICS Cybersecurity

Optimization of ICS cybersecurity requires a response from 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. Each stakeholder group has roles and responsibilities in managing and mitigating cybersecurity risks as shown in Figure 2. ODVA, with its large community of device suppliers who make and sell products for use in this domain, can collectively provide industry with an approach to ICS cybersecurity that protects and defends against cybersecurity threats by focusing on the following 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.
The ODVA Technical Approach to ICS Cybersecurity

ODVA’s approach to ICS cybersecurity combines the “defense-in-depth” strategy with three complementary areas:

- **Harden endpoints** – Increased connectivity on the plant floor demands that equal care be given to the resiliency of end-devices in the face of demanding network traffic conditions, such as broadcast storms and denial of service attacks. To achieve this goal, ODVA will define base-level product hardening requirements for EtherNet/IP devices and rationalize defaults for CIP services and conditions for their use.

- **Protect CIP** – A well-segmented network design is essential to reducing cybersecurity risk. However, application needs - including, but not limited to, remote access - dictate that CIP messages be allowed to cross zone boundaries. To achieve this goal, ODVA will define methodologies for allowing transport of CIP messages via secure tunnels.

- **Secure CIP** – Ultimately, managing and mitigating cybersecurity risk in industrial control systems will require features, such as authentication and encryption. To achieve this goal, ODVA will define future enhancements to CIP for end-to-end cybersecurity in industrial control systems.

ICS Cybersecurity in Practice

ICS cybersecurity requires all stakeholders share the responsibility for risk management and mitigation. For the optimization of ICS cybersecurity, participants in each stakeholder group need to adopt cybersecurity processes for risk management and mitigation internally, yet feed the standards and recommendations to other stakeholder groups externally. Ultimately, this environment will enable all stakeholders to reduce the risk of threats or react more quickly and effectively to threats when they occur. In practice, the management and mitigation of ICS cybersecurity risk needs to be integral to technology lifecycle management for all technology contributors – ODVA, product vendors, OEMs and SIs and end users – as shown in Figure 3. As a continuous process, this will lead to a compounded understanding and response to cybersecurity risks and objectives over time.

ODVA’s Commitment

The definition 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 role that ODVA can and should play in helping to meet these requirements. Two ODVA technical working groups are contributing 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 2013, the SIGs will be proceeding with enhancements to fulfill ODVA’s technical approach to cybersecurity.

*CIP and EtherNet/IP are trademarks of ODVA.*