

Advancing Automation

Cybersecurity



April 2019
Volume XV

Automation.com

INTRODUCTION

Since 2017, Automation.com has published a series of Advancing Automation eBooks, several of which have focused on Cybersecurity. Each year, we see cyber threats continue to evolve, with more and more businesses finding themselves falling victim to attacks. Automation.com, your unrivalled source for automation news, information and innovation, has compiled the 3rd Cybersecurity edition of the Advancing Automation eBook series. After working with prominent industry experts and leaders, we have compiled the latest preparation strategies and technology tips in order to help ward off cyber threats.

This eBook includes security roadmaps and resources in order to ensure an active and successful cyber defense strategy for any organization.

Honeywell

THE POWER OF **CONNECTED**



Indegy

Activate All Your Senses



3eTI

Life Is On

Schneider
Electric

ODVA



FDT GROUP



TABLE OF CONTENTS



No More Dangling from Rooftops: Integrating Cybersecurity into the Connected Plant Transformation

[Page 5](#)

by: Marty Israels, Marketing Director, Honeywell Industrial Cybersecurity



How to Prepare for a Cyber Attack at Every Stage

[Page 11](#)

by: Andrew Kling, Senior Director of Cybersecurity and System Architecture, Schneider Electric



ICS Built-in Security in Today's Connected Enterprise

[Page 14](#)

by: Glenn Schulz, FDT Group and Katherine Voss, ODVA



Different Security for Digital Times

Now that cyber attacks rank as a top threat facing the world, according to the World Economic Forum, it's now more important than ever to work with a partner you can trust. Honeywell combines innovative cybersecurity technologies with hard-to-find expertise to protect industrial assets, operations and people from digital-age threats. Our portfolio includes innovative cybersecurity software, security consulting services, managed security services and integrated security technology. Be cyber secure with Honeywell.

Honeywell

Visit www.becybersecure.com to know more.

© 2019 Honeywell International. All rights reserved.



No More Dangling from Rooftops: Integrating Cybersecurity into the Connected Plant Transformation

By: Marty Israels, Marketing Director, Honeywell Industrial Cybersecurity


The risk of our times is digital in nature. Risk now comes in different forms, such as knowing a specific technical protocol like ModBus and manipulating it to control an asset. Or obfuscating digital machine readings so operators are blind to equipment that might be surpassing safety thresholds. As the World Economic Forum most recently reported, cyber attacks represent one of the top five risks facing the entire world, behind only weather-related risks like natural disasters and climate change.

Process control industries are still at the early stages of industrial cybersecurity relative to how quickly risks have evolved. As we all know, however, once we have experienced the compelling benefits of new technology eras – like a reduction of up to 20 percent in unit downtime or a reduction of maintenance costs of up to 13 percent thanks to digitally connected plants – there is no going back.

So how do we move forward? One way is to identify what has worked in the past, and how to adopt lessons learned for the future. Safety programs for industry are an interesting parallel, exposing some perils and victories that could be similar for today's industrial cybersecurity leaders.

In 1931, for example, when New York's Empire State building completed construction, worker safety was in its infancy. While water carts and food were supplied at every floor for 3500 workers, historical photos remind us that safety procedures were not so routine. Workers did have protective gloves – but dangled precariously on beam edges and cables without harnesses or hard hats. Eventually, the skyscraper earned the "world's tallest building" accolade at the time, and all 102 stories were built in merely 13 months.

Those pioneering industrialists pushed ahead despite the risks, and without even really understanding how to institute safety measures relative to risk (why water for workers, but not harnesses?). It took nearly 40 years when, in 1970, the US Congress established worker safety and health hazard requirements (e.g. OSHA).



Sure enough, many visionary industrial leaders were already far ahead of that standard, competitively touting worker safety records to win new bids. Others less prepared, however, had to embark on expensive and time-consuming safety catch-up measures, losing business, as well as the ability to attract top talent along the way (who wants to apply for the Dangling Steel Welder position?).

Today, as digital connectivity transforms industry, we are excited by similar technological achievements, measured more so by real business outcomes rather than number of stories or physical height. We know it's now possible to increase gasoline production by 8%, or reach full asset capacity in 6 months instead of in years. It's possible by connecting industrial systems from edge to enterprise, and turning data into actionable insight to improve the bottom line. Leading companies, from Honeywell to oil & gas supermajors, are focusing on security built into the Industrial Internet of Things as a fundamental requirement, not as a bolt-on after-thought (still dangling from the rooftop?).

Where we differ from history, however, is that we have millions of dollars of assets already in use as we unlock massive new digital benefits. Fortunately, experts have already developed industrial cybersecurity maturity models, and mapped out how to develop and run programs that realize cybersecurity risk reduction goals. Perhaps most exciting is that forward-thinking industrials are drawing from guidance (such as defense-in-depth from ICS-CERT) to layer in security measures as they modernize. Rather than security on its own, security is part of the next industrial transformation. Just as worker safety needs changed when we sent humans 102 stories up, industrial cybersecurity will keep evolving as we send terabytes of data across plants and remotely adjust 1000 degree furnaces. New cybersecurity standards, methods, and technologies are getting built into IIoT fabrics, and equipment will use new design requirements that address digital plant protection.

Of course, there are many subtleties and differences as we draw any parallels to history. But if you're reading this today and you're involved in smart industry, you can't miss this generation's leadership opportunity – where and how can you build industrial cybersecurity measures into your transformation? Or will you choose to leave your company dangling from rooftops?

The New Cybersecurity Imperative Amidst New Conditions

The new imperative for process control industries facing digitization is to re-think cybersecurity in light of vastly changed conditions, some of which include:

New Uses of Data:

The amount and variation of data flowing through industrial networks has never come under more scrutiny than in our digital age. Information and communication messages were often specialized, incomprehensible machine languages never intended for human view. Today, every ounce of data represents a building block into major insights. Industrial companies are collecting security information and event data and analyzing it in ways never before considered.

As a result, there is increasing urgency for getting data out of industrial networks for centralized analysis. From a security perspective, air gapping is no longer a sustainable strategy when frequent, time-sensitive data sharing is the new norm.

Similarly, closed off networks are less and less comfortable for high level executives accountable for enterprise-wide cybersecurity. Standardized risk metrics demand, Board-level pressures, and other drivers are prompting interest in ICS data that can help improve security posture.

As security is discussed, understanding what types of data and how it will be used can change your tactics. For example, in ICS, it is not simply a piece of data getting stolen that is a problem, as it can be in retail or personally identifiable information (PII) situations. Instead, it is whether multiple types of information can be used by malicious actors to discern operational settings and equipment types, for later use to stage an attack, as one example.

Security strategies can also include advanced technical controls that make it safer to share information. Secure tunnels that record session activity and require multiple authorizations can cross-check that the right people are accessing the most sensitive information. These are the same remote access solutions that bring productivity and efficiency gains, as well as security benefits.

Dynamic Threat Vector – Doppelganger USBs & Bitcoin Miners

Threats come in many shapes and forms, and while traditional security measures may still play a role (e.g. patching), process control industries need more creative responses to new threats in the digital era. What typically was a malware proliferation worry among USBs usage, for example, is today more an issue of whether what workers plug in is actually a storage device at all. The most recent USB attacks overtake command and control of an ICS machine by posing as a benign peripheral, whether a malicious phone charging cable or an e-cigarette charger.

The proliferation of ransomware and bitcoin mining have implications as well, prompting a need for better discipline around plant back-ups. How do you know your backups are in place and will perform at the moment of truth? Many plants today have not standardized cybersecurity risk metrics and have no baseline data to know what is “normal” operating behavior.


While many organizations still focus on the threat detection phase of cybersecurity, there are considerable best practices for improving response time when the inevitable happens. In the case of ransomware, the combination of updating patches more frequently using centralized solutions, and turning to back-ups to restore plant uptime rapidly, can vastly impact success rates. As bitcoin miners ride on industrial network power, automated risk monitoring and performance tools can uncover such behaviors and stop the drain.

Considering how multi-dimensional threats have become, and the high level of motivation among attackers to earn “easy money,” it’s clear that

any industrial cybersecurity strategy must include automation. Technical controls can help scale vigilance, continually measure status, and automatically alert to concerning changes in conditions. For example, a large Oil & Gas company uses automated risk management (Honeywell Risk Manager) to standardize how plants in its fleet report risk status. As a result, budget can be properly allocated to those facilities lagging behind on implementing controls.



In addition, in time-sensitive moments of concern, gaining a pulse on security posture is no longer a labor-intensive, multi-week effort for a German energy provider. Their Risk Manager solution automatically collects key data and aligns it to the company’s defined risk threshold, with dashboards available anytime to easily understand the latest status.



The new ability to automate end node checks instead of performing them manually across all assets also saves them a significant amount of money every time!

Starting the Cybersecurity Journey Now

As the next examples illustrate, many foreseeable risks associated with digital progress can be offset by people, process, and technology security measures. While there are timelines to manage and asset ROI to uphold, these parameters are no reason to hold off on cybersecurity. In fact, modernization plans and cybersecurity go hand in hand.

ICS Security Consolidation with Secure Remote Access

For example, power companies consolidating control rooms to save on costs are -- at the same time -- implementing secure remote access technologies as they centralize. This enables technicians to safely access remote plant locations, performing monitoring or updates through one secure connection. It also cuts down on the myriad of unsecured connections routinely overlooked, or neglected, as dozens of skilled technicians work on different assets. For physically or politically challenging locations where local cybersecurity talent is hard to find, such secure connectivity makes it far easier to deploy security patches. As recent WannaCry and the Equifax data breach underscore, unpatched systems often lead to negative headlines.

Technologies such as Honeywell's ICS Shield are making secure remote access a reality for over 6,000 industrial plants. These solutions have already been tested widely in the field, as they have been in use behind the scenes across major industrial suppliers for years. Each time those suppliers remotely support their customers, they are using ICS Shield for safe access that does not disrupt operations. The use of automation for centralized patching also simplifies regulatory compliance documentation and adherence. This movement toward efficiency and connected operations is, at the same time, progress for cybersecurity.

Fleet Migrations to Improve Cybersecurity

In other industries such as manufacturing, the tightly controlled, heavily secured digital connections can help eliminate the USB threat vector, if plant equipment is modern enough to support connectivity. The reality today, however, is that many plants have mixed vintage assets that are missing basic capabilities. These include important security improvements introduced in the last several years, such as more resilient cryptography or better designed default settings. Most older ICS systems, in place for decades, don't have advanced security features, since they were designed for isolated conditions. Most notorious for security exploitation is Windows XP, yet many companies are reliant on solution types still tied to that older operating system.

To work around these operational realities, companies are using a phased approach to remote connectivity, as well as adding advanced compensating controls. For example, plants may start with providing remote access to the most modern assets, and then, as migrations and upgrades across the fleet occur, add further machines into the remote access purview.

In those situations where no advanced connectivity is possible yet, companies are layering in technical controls such as USB security checks (e.g. Secure Media Exchange from Honeywell). By allowing local technicians to deliver updates by carefully checked USBs, the company can protect plant uptime and security at the same time. Moving forward, as companies invest in plant modernization or build green field facilities, they can more easily implement secure remote connectivity across such connected-ready assets.

Augmenting Cybersecurity Skills

In other industries such as pulp and paper, companies short on industrial cybersecurity staff are drawing up new partnership contracts with equipment vendors to provide the right security skillsets as a service. Together with the advanced capabilities of remote connectivity technologies, the entire business set-up for operations is being reimagined.

In some situations, a company may have enough staff on site for day-to-day industrial cybersecurity management, yet may need experts to help design

policies. Particularly amidst the changed conditions covered above, most industrial cybersecurity policies are either outdated, missing controls for new threat types, or misaligned with the latest security standards. In other cases, companies may have policy creators, but no capability to continually monitor and track key security indicators. They may outsource this aspect of cybersecurity, and may or may not pair it with associated remediation services. Return to uptime requires deep knowledge of the systems, an identified incident response plan, and clear responsibilities for who does what should an incident occur.

Drawing from historical lessons, then reviewing current conditions, and looking to case studies as examples, there is no doubt companies can forge ahead with digital while remaining responsible operational stewards. Particularly by leveraging automation solutions and cybersecurity expertise, they can gain better visibility and control over risks specific to their organization. As the old adage goes, those who dare, win. Those who pair security with digital, win.



About the Author

Marty Israels, Director of Product Marketing, Honeywell Industrial Cybersecurity

Marty Israels is the Director of Product Marketing for Honeywell's Industrial Cybersecurity group. In this role, Marty is responsible for leading marketing efforts to drive the rapid growth of Honeywell's Industrial Cybersecurity business for critical infrastructure protection (CIP) and the Industrial Internet of Things (IIoT). He brings more than 20 years of experience in the process industries in various leadership roles focused on software business growth in both startup and corporate environments.

Marty has an MBA from the University of Windsor and a B.A. Degree in Economics from Western University in London, Canada.



KNOW YOUR OT ATTACK SURFACE

Help Ensure the Right IT Tools
are Used in Your OT Environment.

Watch Video

Hear how PUD#1 IT & SCADA Manager protects Whatcom County from remote and local attacks, including insider threats.

Download Whitepaper

Critical Infrastructure Cybersecurity: How to Actively Secure Your Industrial Environment In the New Era of Distrust

View Webinar

Watch the State of Industrial IOT SANS webinar, featuring Indegy CEO Barak Perelman and other security experts.

Read Analyst Report

451 Research report provides perspectives on Indegy product portfolio, partnerships, SWOT and more.

See Infographic

Learn about the 7 most common unsafe gaps in industrial cyber security and how you can protect against them

Request a Demo

Interact with our subject matter experts as they demonstrate total situational awareness across all sites and OT assets.

[indegy.com](https://www.indegy.com)

How to Prepare for a Cyber Attack at Every Stage

By Andrew Kling, Senior Director of Cybersecurity and System Architecture, Schneider Electric



Connectivity in industry, for better and for worse, is here to stay. Manufacturers and critical infrastructure companies across the world are joining the digital revolution. The IIoT is ushering in a new era of innovation. Emerging technologies, such as cloud computing, big data analytics, artificial intelligence and more, are enabling industrial companies to grow and transform in ways never imagined even just a few years ago.

Along the way, these open platforms and widely interconnected systems have opened new doors for cybercriminals, as many of the legacy systems used to control manufacturing operations weren't built to account for today's security threats. This has led to a rise in the frequency and severity of cybersecurity attacks on some of the world's most critical and volatile manufacturing processes. Almost every cyber-incursion can disrupt industrial operations. The result can be loss of money, privacy, equipment, intellectual property and reputation. Increasingly, with the rise of malicious nation-state actors with geopolitical vendettas, some attacks have the potential for catastrophic consequences, impacting a country's economy, triggering environmental calamities and even costing human lives.

Hackers follow a process to launch an attack, and there's a concurrent process for manufacturers to defend themselves from these attacks. By describing both of them, organizations can ensure they've addressed every element of their cyber risk strategy.

How an Attack is Executed

No two attacks are the same, but there is a general process for how they're committed, whether they last for a few minutes or several months. Let's examine.

1. Scouting the target. An attacker can usually recon the attack target using such non-invasive techniques as Dorking, which means looking for information released in documents and presentations. Social media is also an avenue for attackers to monitor and engage in targeted social engineering before they make their move.

2. Mapping and probing. After the initial recon, the first invasive step can include mapping and intruding the environment. An attacker might probe the network to better understand the landscape of operators and cyber assets onsite—and which ones might be particularly vulnerable.

3. Insertion of malware and lateral movement. After the initial two phases, the intruder is ready to attack. With multiple successful exploits to gain a foothold, raise privileges and land—with necessary permissions—on the target, they can execute their mission.

4. Exfiltration, malicious action. This next stage depends on the goal of the attack. The attacker might either move targeted data out of the attack site (exfiltrate), or actually execute the attack if the purpose is something else, e.g., distributed denial of service (DDoS), data change, Remote Access Trojan (RAT), etc.

5. Cleanup, backdoor. Once the attack is complete, the actor works quickly to remove all evidence of the attack, such as logs, login attempts, etc. They will often leave backdoor malware to make reentry easy. In a perfect world, a manufacturer will never have to worry about a malicious actor taking these steps to inflict some type of damage on their site. But failing to be prepared could leave them flat-footed, which is an unacceptable situation in today's hyperconnected world.

Preparation for an Attack

Attack prevention should already have begun and is a long-term, ongoing process. There are many facets to it, starting with modeling the cyber-threat landscape. This can help analyze security threats and gaps specific to an organization's industry and particular plant. Plant owners should first perform a risk-and-threat assessment and gap analysis, and establish zones and conduits as a way to segment and isolate similar devices or systems according to security levels. It's important to be aware of every system network connection, and then ensure they have all been secured. This also helps in the event of an attack: If zones are established, investigators only need to take down portions of the operations, saving organizations valuable costs and impact on revenue.

A strong security culture has its foundation in industry and government standards, protocols and best practices. From a governmental perspective, a notable example is the National Institute of Standards and Technology (NIST) framework in the United States. This is considered the authoritative source for cybersecurity best practices, and it was recently expanded to address evolving identity management and supply chain topics. Standards such as this are not limited to the United States; in some countries, such as France, these standards are even carrying the weight of law. Within industry specifically, the most essential standard is IEC 62443, the rigorous standard for industrial automation technology that works to safeguard operations across multiple layers. Cyber threats change by the day, which means these standards are always being refined.

To ensure the integrity and security of plant technology and processes, people are the first and best line of defense. Because the gap between IT and OT continues to close, everyone across the organization—whether in the plant, the field, the office, the boardroom or anywhere else in the enterprise—plays an essential role in mitigating cyber threats.

Swift and Effective Reaction to an Attack

No manufacturer is inherently safe from attack, so they must be prepared to react if and when an attack happens. They should be prepared to take the following steps:

- 1. Isolate the attack/malware.** The end user needs to be well-informed enough to take this action, which goes back to ensuring you hire the right people, then continually train them. Isolation could include disconnecting network and internet connections and switches.
- 2. Alert and incorporate the experts.** If the organization has a solid risk management plan, an incident response team will have been identified. This team needs to be contacted immediately after an incident. They can help capture logs, lock credentials and close remote access. In some cases, reporting an incident to government officials is mandatory.
- 3. Assess the mode and scope of the attack.** The incident response team and end user should collaborate to determine how the attack occurred and its full impact. It's worth examining if and how human error contributed.
- 4. Ensure business continuity.** This plan should include a system restore from a secure backup. Only then should the plant go back online.
- 5. Communicate as appropriate.** Whether it's to plant executives, software suppliers, regulatory bodies, etc., it's essential to determine who must be contacted and do so quickly.
- 6. Identify room for improvement, enact remediation.** Any attack should serve as a wake-up call to the affected user. To reduce the likelihood of another attack, the user should conduct a full-fledged analysis and remediation plan.
- 7. Share information.** As part of the attack postmortem, the organization should look for ways to share information about the attack so industry as a whole can benefit from lessons learned. Think about sharing vertically with government agencies. Seek out opportunities to share horizontally across industry. Collaboration among the various stakeholders connected to industry and cybersecurity can only strengthen preparedness for increasingly complex attacks.

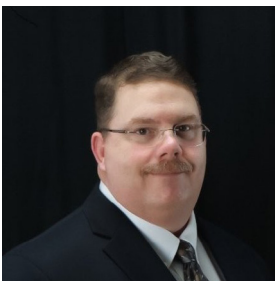


There is no way to eliminate cyber threats, but industrial organizations can do plenty to beef up their cybersecurity hygiene and protect their critical infrastructure.

No business would leave their front doors wide open and unattended 24/7, yet industrial networks, assets and even entire operations often are. There needs to be a shift from reactive to proactive cybersecurity management, and a commitment to standing together in the face of cyber threats. The entire industry is counting on it.

About the Author

Andrew Kling, Senior Director of Cybersecurity and System Architecture, Schneider Electric



Andy has over thirty years of software development experience. He has worked in the Industrial Control Systems (ICS) development organization at Schneider Electric since 2001. Andy has ushered the Schneider Electric Process Automation Development team to the first in the world ISA Secure - Secure Development Lifecycle Assurance certification for three development sites on three different continents. In this responsibility Andy is chartered with improving our Secure Development Lifecycle adoption, ensuring that cybersecurity requirements are part of every project that is executed.

Cybersecurity is core to everything we do.



Industrial Control System Cybersecurity

- Application layer firewalls/DPI
- Encryption
- Secure energy systems



Cyber-secured Wireless Platforms

- Certified mesh networks
- Sensor & metering networks
- Intrusion Detection



Cyber-hardened Perimeter Management

- Perimeter surveillance
- Situational awareness
- Central management

Don't be intimidated by endpoint vulnerabilities

From the core to edge, cybersecurity is our focus. A DoD partner for more than 20 years, we deliver non-intrusive solutions that safeguard endpoint operations and protect your critical infrastructure.

Learn how to cyber-harden and improve operations. Schedule a briefing today. ultra-3eti.com/core



ICS Built-in Security in Today's Connected Enterprise

By Glenn Schulz, FDT Group and Katherine Voss,
ODVA

Over the last decade, the rise in cyber attacks on manufacturing facilities and critical infrastructure has resulted in cyber security becoming a central concern amongst industrial automation and control system users and vendors.

With the convergence of information technology (IT) and operational technology (OT) in industrial manufacturing, there is a need to safeguard data access from the enterprise all the way down to the device level.

The following article describes efforts by the automation industry to develop next generation standards and technology, which enhance security throughout the lifecycle of industrial control devices in today's connected world.

Introduction

As factory and plant operations become more connected in the era of the Industrial Internet of Things (IIoT) and Industrie 4.0, industrial organisations are making significant security investments to help protect their intellectual property, operations, and corporate image.

In the past, industrial control networks were primarily isolated systems, running proprietary protocols, using specialised hardware and software. But the industrial architecture has transformed over time, with collaborative mechanisms that involve internal and external integration.

Industrial facilities have traditionally relied on logical or physical security to protect their perimeter. These defences range from firewalls to gates, guards and fences. However, any breach in perimeter security can put the facility's industrial control system (ICS) at serious risk of denial-of-service (DoS) attacks or other disruptions.

Many plant sites employ a defence-in-depth security architecture to secure their ICS. This strategy is based on the idea that multiple layers of security are 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.

However, as attackers become more sophisticated, it becomes more important for the connected end device — the final layer of defence — to defend itself.

Evolving Security Challenges

Industrial security presents a difficult challenge in the age of open systems, increased connectivity and expanded data sharing. The fourth industrial revolution brings new cyber risks for plant and factory automation platforms. It is imperative for cyber security strategies to be secure, vigilant and resilient, as well as fully integrated into flexible business models.

As cyberspace shrinks due to the benefits derived from greater data exchange, new vulnerabilities in the ICS arise and new threats emerge. Left unchecked, the ICS, its devices and the networks to which they are connected, can be exploited by threat actors and pose potentially negative impacts on the safe, reliable and/or secure operation of production processes.

Governments and the private sector alike have expressed concern about cyber security vulnerabilities within automation systems. Regulatory bodies have identified threats to critical infrastructure where industrial Ethernet networks, such as EtherNet/IP, are commonly used. From a business standpoint, industrial firms are facing growing challenges from ransomware and other cyber threats.

With increasing reliance on connected systems, and ever-increasing amounts of data, it becomes more important for the systems, their devices, the data and points of connectivity to be inherently secure.

Manufacturing plants have to give serious consideration to policies dictating how sensors and other edge devices can be accessed from the outside world.

One of the biggest concerns for end users is the industrial equipment lifecycle, particularly as it relates to the protection of data and access to crucial instruments. They must find ways to effectively address cyber security demands and protect plant assets such as field instruments, sensors and input/output (I/O) devices. A key issue is managing access to devices and their digitised artifacts over the entire lifecycle in a secure and reliable way.

Advancing Industry Standards

International standards bodies concerned about disruptive and dangerous cyber security attacks on plants and critical infrastructure operations have already established guidelines, standards and policies to help mitigate risks of cyber security threats to industry. In addition, governmental agencies such as ICS-CERT with the US Department of Homeland Security are working with industrial enterprises to identify threats.

ODVA, a global standards development and trade organisation, develops and maintains the Common Industrial Protocol (CIP), an open communication protocol designed for automation and data use cases in industrial control systems and used by EtherNet/IP, the world's largest industrial Ethernet network, and found in devices across diverse segments of the automation market.

CIP Security, first released by ODVA in 2015, allows users to take additional steps to protect their ICS with techniques for securing transport of messages between EtherNet/IP devices and systems, and thus reduce their exposure to cyber security threats. The goal of CIP Security is to enable the EtherNet/IP device to protect itself from malicious communications. ODVA's roadmap for CIP Security call for capabilities to be released in phases as shown in Figure 1. The first phase of CIP Security provides mechanisms to encrypt the transport of messages between EtherNet/IP ports and for certificates. In addition, recognising that every EtherNet/IP device and system

does not need to provide the same level of support for all defined security features, CIP Security defines a Security Profile to allow for a scalable solution. 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. In the next phase of CIP Security, capabilities will be added around role-based authentication and authorization and enhanced encryption methods.

On the integration side of the automation industry, FDT Group is an international, non-profit corporation providing an open standard for enterprise-wide network and asset integration. The organisation was founded for integration and lifecycle management of devices. Ongoing advancement of FDT technology is leveraging major developments like the IIoT and Industrie 4.0 to enable end users to realise the true potential of decentralisation, interoperability, integration, as well as a unified view of all data and functions across process, factory and hybrid control applications.

FDT was built to support a comprehensive, open architecture for the connected world of industrial automation networks and assets. It supports the current installed base, and will adapt to future technologies and protocols. FDT/FRAMEs and Device Type Managers (DTMs) based on the current FDT specifications (FDT 2.0) are digitally signed, providing tamper-proof software delivery and non-repudiation. Granular DTM security with enhanced user rights is added to the security settings.



Figure 1: CIP Security is designed to protect Industrial Control Systems (ICS) in the new era of automation.

Ongoing Industry Collaboration

ODVA and FDT Group are both working to address cyber security vulnerabilities with on-going enhancements to their technologies and standards. The two organisations have collaborated on the ability to integrate devices implementing ODVA technologies and standards into the FDT ecosystem for more than 10 years. The latest work resulted in a CIP annex supporting FDT 2.0, which allows for seamless tunnelling through industrial networks.

ODVA is one of the first standards development organisations to publish a true security overlay on an industrial network protocol. CIP Security utilises standard encryption mechanisms and cryptographic keys to provide scalable security on the wire. This approach is in response to recognition that every device in a production system is potentially a point of attack. With the growing use of EtherNet/IP within the ICS, there is a corresponding proliferation of malware into control networks and distributed assets.

As part of CIP Security, security on the wire will allow for end devices to defend themselves from unauthorised and/or malicious access — a critical capability with the move towards more connected systems. End users will have a choice of features they need to secure their particular environment. Because of the nature of typical workflows, devices will, in most cases, have CIP Security off by default and users will need to enable it. They will then have the option of more simple methods such as use of pre-shared keys for device authentication, or more sophisticated mechanisms like x.509 certificates. This will allow for the creation of a single zone of trust for devices, or multiple zones, depending on the application requirements.

FDT Group, at the same time, is focused on incorporating methodologies and workflows into its standard to support emerging security requirements. The organisation is compiling a series of best practices to help manufacturers implement FDT solutions in a way that avoids possible threat vectors. In addition to an Audit Team to provide an independent perspective on security enhancements, it has established an Incident Response Committee to help ensure timely communication for active issues and provide a vision for long-term security activities, as well as a technical group within the Architecture and Specification

Team responsible for a security framework for the development of new specifications and tools.

From FDT Group's perspective, any device that wants to communicate on a control network must be part of an established security model. Devices such as I/O cards, transmitters, etc. need to have awareness of the network's security provisions and be able to participate in them. The same holds true for various software applications and tools.

To extend its support for the IIoT and Industrie 4.0, and simplify the automation ecosystem exchange, FDT Group is developing the FDT IIoT Server (FITS) solution. FITS enables mobility, cloud, and fog enterprise applications, as well as sensor-to-cloud and enterprise-wide connectivity employing FRAME and DTM business logic at the heart of its client-server architecture. The FITS solution features robust layered security, leverages vetted industry standards, and utilises transport layer security (TLS) to establish a hardened shell and encrypt all communications throughout the architecture. Optionally, this solution can authorise devices that connect to the FITS server. User-based security is employed to determine the user's role and rights within the application.

The addition of security on the wire to the FDT standard will enable a complete solution for comprehensive, end-to-end, enterprise-wide security.

Forward-thinking Approach

As established international standards development organisations representing many of the world's leading suppliers of devices used in industrial control systems, ODVA and FDT Group have key roles in advancing end-to-end security for the connected enterprise, and in supporting the development of technologies and standards for security on the wire.

ODVA and FDT Group are committed to optimising the industrial device lifecycle with robust built-in security features. Other potential collaboration between the two groups involves the security and authentication of tools and digitised artifacts within the FDT domain. This encompasses ODVA member suppliers utilising DTMs in their field devices.

The next update to the CIP annex will embed CIP Security for seamless security integration and scalability of security control. In FITS, the FDT Server will natively support CIP Security to allow for security on the wire in a scalable format. It will link the IT and OT security architecture with control from the FDT/FRAME-enabled system. Security on the wire will enable the ICS to defend itself from unauthorised and/or malicious access.

When the ICS and its connected assets have inherent protection from cyber security threats, there is the possibility of access from other trusted systems that might otherwise be considered part of an untrusted IT system. Conversely, devices may be able to produce data that can flow more directly and securely to IT systems.

One issue for industrial organisations is that production systems, and the assets (devices) within those systems, have very long lifecycles. Some devices may allow for field updates with new security capabilities. In other cases, the user would be looking at systems with varying degrees of device-level security. Tools such as firewalls or security proxies may be employed to help secure less-capable devices.

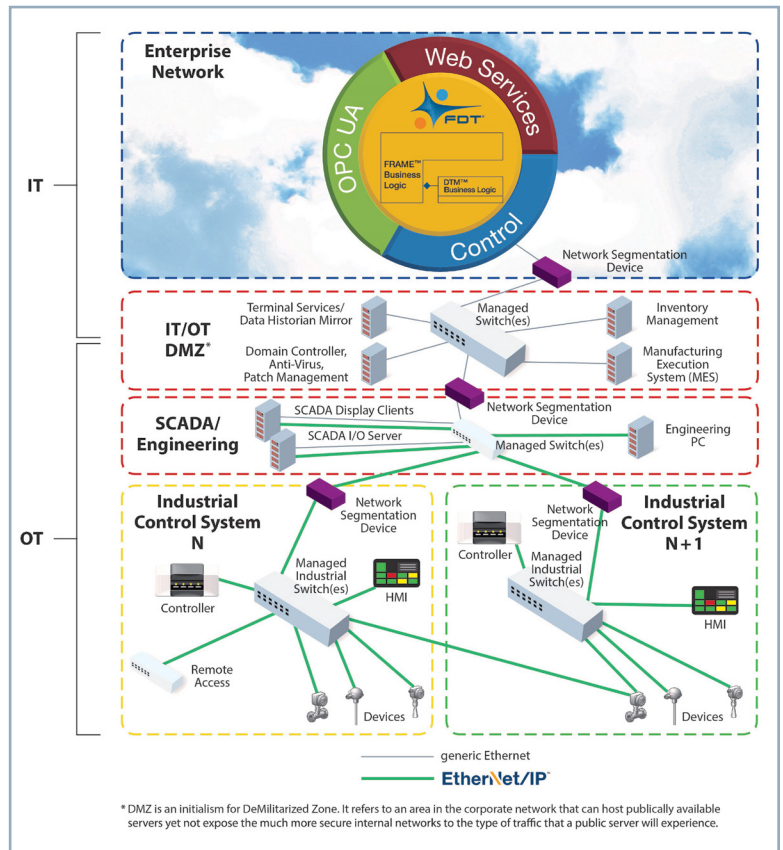


Figure 2: Converged IT/OT cyber security solution for the industrial enterprise

Ultimately, security on the wire will be implemented across the entire enterprise, from business systems down to the lowest device level. Any “open wire” will be regarded as a vulnerability and handled accordingly. As shown in Figure 2, technologies and standards, such as FITS and CIP Security, will provide users with a converged IT/OT cyber security solution for the industrial enterprise.

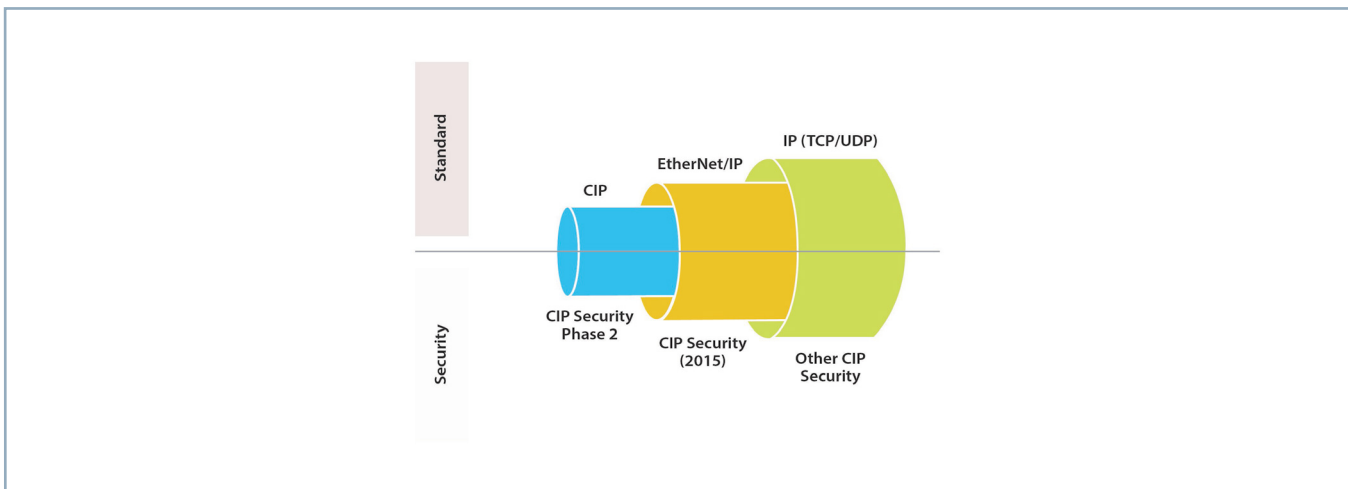


Figure 3: ODVA's Roadmap for CIP Security

Conclusion

Industrial security is a complicated, multifaceted challenge that cannot be solved by simply purchasing the latest technology. Instead, managing the security of an industrial control network requires changing processes and managing risk.

ODVA and FDT Group share a similar vision for enhancements to ICS security technology. They recognise that it is crucial to secure the control network itself in a changing cyber security environment. Indeed, every automation industry stakeholder must be aware of the crucial aspects of security throughout the lifecycle of industrial control devices in a connected enterprise ecosystem. Advancements such as control on the wire offer the opportunity for self-protected devices, which add another dimension of security to the industrial network hierarchy.



About the Authors

Glenn Schulz, Managing Director, FDT GROUP

Glenn Schulz is a seasoned executive with a passion to accelerate and differentiate technology driven companies. Extensive global experience including ex-pat status in Europe. Broad general management with service and support, engineering, sales, marketing, IT, legal, and business development expertise.



Katherine Voss, CEO, ODVA, Inc.

As the chief executive officer for ODVA, I led this international standards development and trade organization which is at the forefront of the application of ICT to industrial automation and IIOT. ODVA represents over 300 corporate members who share a common interest in making and selling products using ODVA's technologies and standards including EtherNet/IP, the world's leading industrial Ethernet network. As CEO, I managed the day-to-day business operation of the company, supported the Board of Directors in fulfilling their governance and strategic planning responsibilities, fostered a spirit of collaboration and innovation across ODVA's stakeholder community, and promoted the mission, vision, value proposition and brands of the organization to industry.