ARC VIEW

FEBRUARY 16, 2016

Future of Manufacturing: How Digitalization is Changing the Face of Cyber Security

By David W. Humphrey

Keywords

Industrial Cyber Security Digitalization; Plant Security; Network Security; System Integrity

Summary

The industrial cyber security (ICS) landscape has matured in years recent. As attacks have grown in number and sophistication, so have the methods and technologies used to defend industrial equipment. The good news is that most industrial companies now understand the risks of cyber attacks and are investing in security measures. Even better news is that automation suppliers have grown to understand the particular needs of industry users and most now offer solutions to address the three pillars of ICS: system integrity, network security and plant security.

A modern, comprehensive industrial cyber security solution takes a holistic approach to security by addressing the three pillars of ICS: system integrity, network security and plant security.

The Changing Landscape of Cyber Security

Industrial users were long immune to cyber attacks, but that changed drastically in the past decade in part due to the digitalization of industry. The automation world has increasingly adopted commercial platforms and networks to keep pace with rapid technology development. Industry users today rely on both automation and IT suppliers for complete security solutions. While enterprise security solutions are keeping pace with the growing variety and sophistication of attacks, industry users are faced with the dilemma of having their own requirements and goals. For example, according to ARC research, non-industrial companies view information confidentially and integrity as top priorities, while industrial companies are more concerned with ensuring process uptime/availability and safety. For this reason, plant engineers should not assume that security concepts borrowed from the IT world will help them both ensure a secure plant environment and reach their production goals.

For industrial companies, the risks will only grow in the future as companies continue to install systems, such as PC-based controllers and operator panels or Ethernet, that increase their exposure to attacks. Security solutions today often focus only on a single area. Commercial IT suppliers typically deliver solutions for the enterprise, but are unaware of the particular needs of manufacturers. Some automation suppliers offer "black box" security components to isolate a machine, but these are difficult to integrate and can be compromised. Finally, third party industry software and patches can expose security holes and are becoming a dangerous new attack vector that can undermine existing defense strategies.

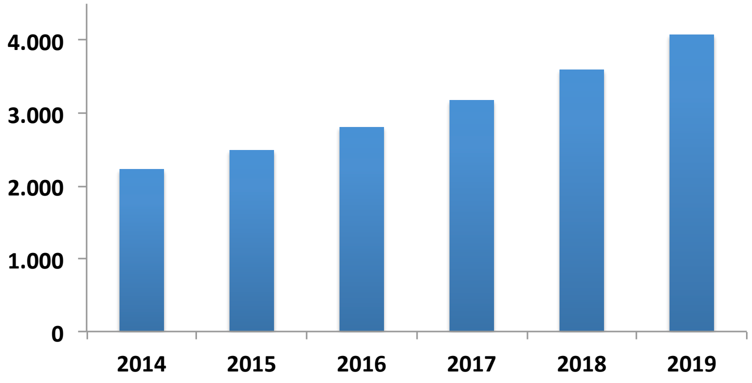
Cyber Security in the Process Industries

Even within the industrial community there are differences in attitudes and approaches to cyber security. The process industries have their own special requirements because of the scale of damage that could result from a security breach. If a machine in a factory is compromised, the line stops and production is halted until the problem is fixed. But in a chemical plant or refinery, a targeted cyber attack could result in the destruction of the entire facility and the surrounding area. For this reason process communities around the world have set up open forums in which incidents can be reported and detailed information shared.

How Will Industrial Cyber Security Evolve?

The number and sophistication of cyber attacks are increasing and raising the likelihood of serious industrial cyber intrusions. The spectrum of perpetrators is broad and growing, ranging from government-sponsored espionage and vulnerability testing to inside jobs by disgruntled employees and "hacktivists". While data on the growth rate of attacks are sketchy, the variety of types of attacks is growing. Currently at the top of the list is "spear-phishing", a method by which emails that appear to come from trusted partners, such as business partners or even inside the same company, are sent to employees with a request to "update" access information to critical systems. One variation sends a document that, if opened, loads spyware onto the user's machine, thus using email as a backdoor into an otherwise protected system.

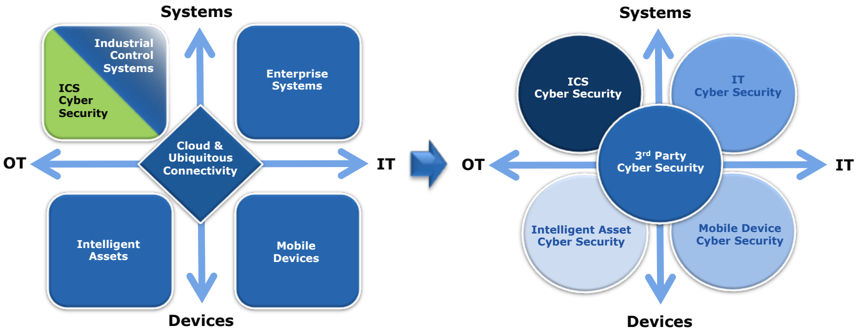
Another dangerous source of attacks is the insider job. Attackers may have any of a wide range of motivations, but what is to stop an employee from comprising a company’s own security? Additional internal security measures are the answer (“protect us from ourselves”). These include intrusion detection, network scanning (detecting unauthorized devices such as private laptop PCs), and deep packet inspection (verifying content and veracity of commands to field devices such as valves to determine if certain commands are authorized). However, such measures can hinder plant personnel in their daily work and can still be defeated by some insiders.



The ICS Market Will Grow More than Twice As Fast As Automation Markets To 2019. Source: ARC Advisory Group.

Industrial cyber security solutions are growing in scope and sophistication and will continue to evolve in the next decade. Until now, solutions have tended to focus on protecting components and systems. The ongoing merging of automation and information technologies will drive the evolution of comprehensive solutions for the whole enterprise, taking into account the different needs of all areas of the enterprise, from business systems to manufacturing. Finally, future solutions will include the people who operate the systems. Systems will be configured to the individual employee with personal identification and specifiable privileges that don’t hinder employee productivity.

Services will play a growing role in end-to-end security solutions. Many industrial users either don’t have personnel in-house with the right expertise or they simply don’t want to maintain specialized staff on a full-time basis. Automation suppliers with security expertise can fill this gap in both the implementation stage as well as with ongoing maintenance of security solutions. For example, Siemens offers a wide range of security consulting services including assessments, development and implementation of action plans and security measures, and support for ISO certification. In addition, Siemens offers 24/7 security monitoring of the whole plant.



Industrial Cyber Security will evolve from its current focus on control systems to a comprehensive, enterprise-wide solution, from devices to systems and from OT to IT.

To achieve the next level of cyber security solutions, suppliers need to address these challenges:

Mobility and Ubiquitous Connectivity

Industrial users are deploying more and more wireless devices in automation systems and using mobile devices in the plant and factory with the goal of allowing access to information from any source, anywhere and at anytime. Wireless strategies used in the factory may conflict those on the enterprise side, and enterprise wireless systems could inadvertently allow access to critical automation systems. The reason for this is that wireless access points are sometimes added locally on both the enterprise and plant side without consideration for enterprise-level security implications.

In a perfectly connected plant, future industrial devices will have security designed into them from the beginning rather than added as an afterthought. Security concepts will be device-centric, meaning that a security breach in any given device won't comprise the security of the whole system.

Everything in the Cloud?

Use of the Cloud for storing and sharing information is commonplace in the commercial world, but still relatively new among industrial companies.

The Cloud can greatly improve project collaboration by allowing engineers around the globe to work simultaneously on complex projects using a single repository for information. Commercial users would not trust their data and applications to the Cloud without the guarantee of a solid security solution behind it. This also applies to industry users, but again the with emphasis that security needs and goals differ somewhat between the two domains, so users should verify that security solutions put in place by Cloud hosts clearly address their specific needs.

IIoT and Industrie 4.0

These concepts provide the inspiration and a digital framework to secure the competitiveness of industrial companies well into the future. By "perfecting" connectivity in the plant with intelligent devices such as smart sensors, industrial companies can free up raw data hidden deep within manufacturing processes and use this information to continuously improve processes. But as with the Cloud, increased security challenges go hand in hand with growth in the number of connected devices. The sheer variety of new devices connected in industry applications opens up new ways to defeat or circumvent existing security solutions. For this reason, the onus is on industry players, both suppliers and users, to recognize the risks unique to their industries and to address them on an ongoing basis.

Three Pillars of Industrial Cyber Security

Finally, any ICS must address the three pillars of cyber security: system integrity, network security and plant security. Siemens, a leading automation supplier, offers an extensive ICS portfolio that includes products and services for the implementation of a holistic concept to address each of these pillars.

System Integrity

This refers to protection of intellectual property at the controller or system level and is realized through features like protection of algorithms from access and modification, copy protection that links program parts to the serial number of a memory card, multi-level controller access protection, and manipulation protection that validates the source of incoming data.

Network Security

To ensure security of industrial networks from the field level up to remote connections, Siemens offers secure switches with built-in firewall to protect against unauthorized access, as well as VPN technology to protect against manipulation and espionage. Devices equipped with PROFINET offer robustness against large volumes of network packets or faulty network packets to ensure that high network loads or denial-of-service attacks can't impair automation operation.

Plant Security

Plant security protects the entire factory or plant from unauthorized physical access. This includes general building access control as well as access control for sensitive areas via key card. Here, Siemens offers a portfolio of solutions and consulting services to help users develop a comprehensive plant security solution.

Strategies for ICS

Many industrial companies have taken an ad hoc approach to cyber security, solving immediate security problems with bolt-on solutions or adapting enterprise solutions to the plant. Most don't have the luxury of implementing a complete solution from the ground up. But that doesn't prevent the implementation of a new, all-encompassing strategy that takes a holistic approach to address the three pillars of ICS mentioned above.

	ICS Status Today	ICS Future Requirements
Mission	Protect plants & infrastructure AIC*	Protect plants, infrastructure, ext. resources AIC and CIA*
Scope	Systems Private networks	Systems, IIoT & mobile devices, Cloud Private & public networks
People	Internal ICS groups ICS supplier service groups	Internal ICS & IT groups ICS & IIoT supplier service groups Public networking services partners Cloud app & data services partners
Processes	Manage security at perimeter Secure networks Secure zones Authorize people Manage software vulnerabilities	Manage security at device Secure networks and messages Secure zones, devices, messages, data Authorize people & devices Manage software & device vulnerabilities
Technology	Endpoint security wrappers Network firewalls	Secure-by-design endpoint devices Network and device firewalls

* Priority of "availability, integrity, confidentiality"

Cyber Security in Manufacturing

Whether a single-plant company or a multi-site enterprise, industrial users can revisit their approach to ICS with a strategy that both acknowledges today's solutions and addresses tomorrow's needs. Start by building a single, integrated strategy along the line between IT and OT, and from devices to systems. If in-house expertise is lacking, partner with suppliers to fill expertise gaps. Stay awareness of developments by attending industry events and keep abreast of what peers are doing. Periodically review your strategy and fill gaps before they become problems. Finally, establish ongoing awareness training across your company to minimize behavior that creates internal threats.

Economic Benefits or the Cost of Not Investing in ICS

Similar to industrial safety technology, which verifiably reduces equipment downtime, ICS offers economic benefits in terms of increased system availability by mitigating security risks. Rather than simply looking at security as an additional cost, users today take a holistic view and weigh the consequences of security breaches that result in unscheduled downtime, equipment unavailability, disruption of continuous processes, or even the destruction of plant equipment and environmental or even catastrophic damage. Besides the obvious threat to life or physical condition, companies can also risk their public reputation – something that is difficult to shake off as some chemical manufacturers have already experienced.

Last Word

Industrial cyber security has matured, but remains a challenging and dynamic domain. Today's risks and challenges will continue to increase with more sophisticated attacks and attackers while technology developments create new solutions. Industrial users should take a holistic approach to ICS and establish a strategy for both today and tomorrow.

For further information or to provide feedback on this article, please contact your account manager or the author at dhumphrey@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.