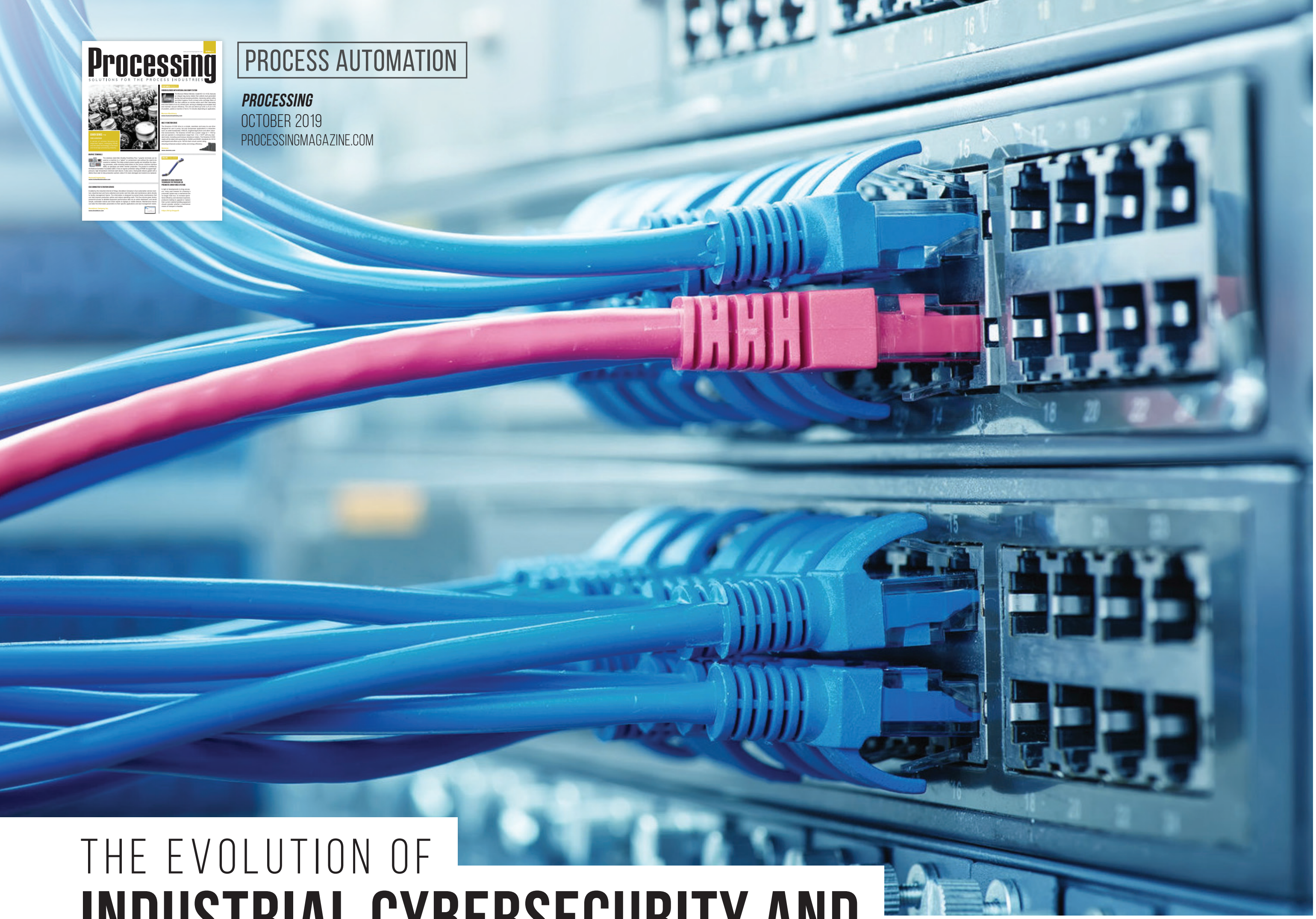

PROCESS AUTOMATION

PROCESSING
OCTOBER 2019
PROCESSINGMAGAZINE.COM

THE EVOLUTION OF INDUSTRIAL CYBERSECURITY AND CONTEMPORARY NETWORK DESIGN

Process automation systems are increasingly connected to IT systems and the outside world, introducing cybersecurity concerns, which can be addressed using techniques such as software-defined networking and monitoring services.

By Takashi Hasegawa, Yokogawa Electric Corporation

The concepts and practices of cybersecurity for process automation systems, such as a distributed control system (DCS), have gone through a series of phases driven by the original vendors and end users. In the larger history, the very notion of cybersecurity came late to the discussion for several reasons.

Early systems, installed prior to 2000, were largely built on proprietary hardware and software and existed in isolation. Security was primarily an internal matter and revolved around who had permission to change setpoints and the like. Anyone wanting to hack into these systems had to be in the building and physically connected.

At the dawn of the 21st century, requests from corporate management for more direct access to production data created the need for mechanisms to build interfaces to corporate IT networks, which spawned the idea of operations technology (OT) for differentiation between corporate and manufacturing networks.

OT/IT integration

OT security remained a relatively minor concern since the interconnectedness was still very limited, along with a belief that few individuals from the outside would be able to make any sense of those proprietary platforms. Security by obscurity became the guiding mindset. The obscurity faded as OT networks moved more toward IT-like hardware and software — particularly PCs, Ethernet and the internet. Hackers also recognized that breaking into a poorly protected OT network might serve as an entry point to corporate targets.

Network managers recognized that it would be necessary to add firewall appliances between the two systems at every interface point to create a hardened perimeter. Of course, if any invader could penetrate the defenses, perhaps through an overlooked interface point, there was nothing to stop free movement once inside the OT networks, possibly disrupting operations or stealing data. Adding defense-in-depth strategies sought to make this more difficult, a concept that grew into the "baked in" security applied with today's process automation systems.

This broad-brush look at the situation suggests a wide spectrum of possibilities, and various process plants and facilities can be anywhere on a continuum from virtually zero defenses to highly sophisticated systems. The responses from equipment vendors have also been on a

← The first step when assessing a cybersecurity system is to carefully examine each component attached to the plant's networks.

All figures courtesy of Yokogawa Electric Corporation

spectrum, with some being highly proactive and embracing international standards, while others have been less responsive.

The situation on the ground has only become more complex in recent years as the convergence of OT and IT has become reality under the banners of digital transformation, digitalization and the industrial internet of things (IIoT). The activities of groups such as the Open Process Automation (OPA) Forum will also increase the demand for security. In many plants, all or some of these initiatives are being implemented, and it is becoming difficult to see where the border is between IT and OT.

As these changes have been going on, the cyber threat picture has also evolved. Attackers have become more creative and sophisticated, and there are many situations in which industrial networks have been targets. The convergence of IT and OT, if not handled carefully (Figure 1), can create many opportunities for cyber criminals to invade through unprotected openings at interfaces between OT and IT systems.

Working through complexity

Designing something as complex as a comprehensive cybersecurity program requires resources that few companies have in house. Some plants try to paper over the protection gap by inserting firewalls, many of which interfere with communication while offering poor protection. Others issue directives and rules, but without supporting network architecture changes.

These attempts are typically unsuccessful, but at least they cause many plants to recognize they have little choice other than bringing in outside help. Recognition of an actual intrusion can add a sense of urgency. Outside help can come from the vendors that provided the plant's automation platforms, along with consultants and system integrators specializing in this area.

Having vendor involvement is important as these companies should understand the specific characteristics, strengths and weaknesses of its systems. Vendors serious about providing secure systems have internal test beds to provide constant evaluation of their products, constantly probing and testing to look for vulnerabilities and evaluate interactions with operating systems and security tools.

Consultants and system integrators may also be necessary to help evaluate how disparate parts from multiple vendors interact because cross-platform interoperation can introduce specific vulnerabilities. All those working on such a project must be conversant with relevant standards, such as IEC 62443, and its interaction with IEC 61511 via safety-instrumented systems. These standards help harmonize practices globally and among vendors.

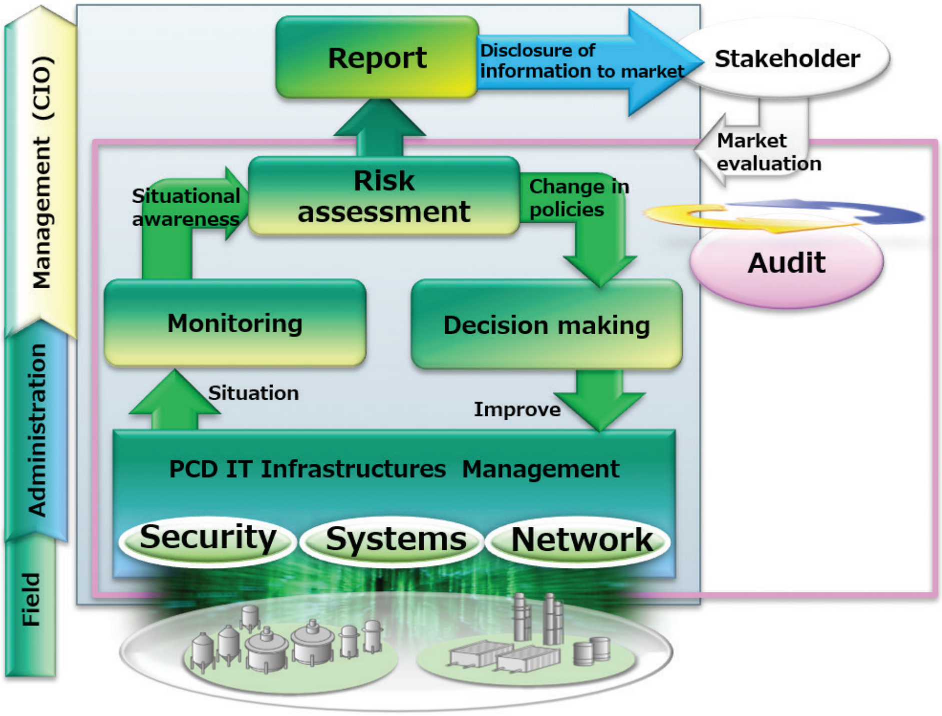

Figure 1. A cybersecurity program is an ongoing effort, requiring constant evaluation and improvement. The lifecycle approach depicted in this diagram keeps a program current as threats change.

Cybersecurity programs generally begin with a risk assessment, the first step of which is an in-depth asset inventory and analysis. Every item on the network must be identified down to its specific model number and software version. This can be checked against the ICS-CERT advisories and reports to identify items with known vulnerabilities.

Once this assessment has been completed, it is important to establish goals for what the system should look like and how network needs may change in the foreseeable future. Since the effort will invariably involve securing an existing network, which may involve many old assets, techniques must be adaptable to these situations.

Yokogawa frequently uses software-defined networking (SDN) as a flexible solution that minimizes impact on running systems while providing mechanisms to increase security levels. SDN can be dynamically controlled even in an operating environment.

In most plants, OT systems tend to reside on the same massive segment. This makes for free communications, but it makes these systems hard to defend. Using SDN, it is possible to construct an independent virtual network for each system (Figure 2), with the need for partitioning. Even systems running on old operating systems outside of vendor support can be grouped and separated on a single virtual network so that they cannot communicate directly with the outside world, temporarily mitigating vulnerability risk until the system is upgraded to the latest version.

An actual implementation

In 2018, a Japanese company introduced a virtual network infrastructure using SDN technology to strengthen cybersecurity measures in the plant networks, and to create a safer and more efficient network infrastructure. This also future-proofed the networks, preparing for the anticipated introduction of IIoT strategies and new enterprise resource planning system capabilities.

Unfortunately, previous efforts to expand and protect networks had not been optimally executed, resulting in complex network topologies and wired infrastructure. It was therefore necessary for the plant to establish a comprehensive cybersecurity approach to understand, evaluate and improve the security status of networks in the plant.

The few internal network administration resources available were busy with other tasks, so implementing this project would depend on help from outside resources. The company called on Yokogawa to provide next generation industrial network security solutions, and to bring its experience and knowledge to bear for both plant operation and OT-IT security.

> “The convergence of IT and OT, if not handled carefully, can create many opportunities for cyber criminals to invade through unprotected openings at interfaces between OT and IT systems.”

Utilizing SDN technology for IoT-enabled smarter plant infrastructure

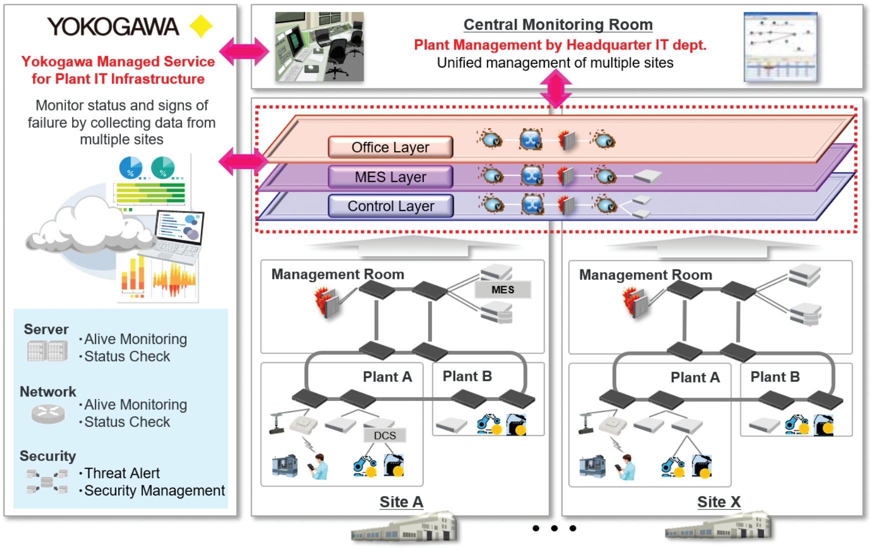

Figure 2. Software-defined networking allows creation of an independent virtual network for process automation systems to protect plants from cyber intrusion.

Initial assessment results

Yokogawa's network specialist team worked with the plant administration team to understand the current state of the plant-wide network and various IT assets associated with the Yokogawa CENTUM DCS platform. The analysis covered all network equipment from the office area to field equipment, the control room and electrical room. The physical network cables were traced while checking the asset inventory list and the system architecture diagrams. The models and settings of each network asset such as firewalls and switches were detected and recorded. The team addressed the human needs as well through interviews with plant personnel.

IT infrastructure management would need to include secure wireless access points and guest Wi-Fi, plus preparation for future requirements including management of increasing numbers of IT assets, along with prospects for growing network utilization.

Yokogawa’s proposal was a virtual network using SDN technology to integrate existing network cables and equipment without making any physical changes. This created a new, secure and intelligent network.

Designing a virtual network

The team assessed the plant network and sorted out the communication requirements for each segment. The logical configuration of the entire plant network was then designed and implemented using SDN to retain and make the most of the existing assets. The switchover from the conventional network to the virtual network was completed in about 30 minutes without any problems. Minimizing the impact on the running plant operations is one of the main benefits of virtual networking, as demonstrated on this project. In addition to anti-spam and conventional anti-virus measures, intrusion detection, log collection and traffic analysis tools were also introduced to enable real-time network monitoring.

With the introduction of IT asset management tools, it is now possible to monitor and manage the devices connected to the network, including the access and security status of each device. Secure wireless access points with appropriate access rights and guest Wi-Fi are now available in all areas where required.

Yokogawa provides continuing security monitoring services to support both IT and OT systems. When a network failure or security threat occurs, the monitoring team can take immediate action. Using these types of outside services allows a company to use its internal resources for ongoing operations. Although IT support services can be provided by many companies, only industrial automation suppliers are able to also provide support for OT systems, with this support encompassing both security and other types of problems.

The security monitoring team uses secure remote access that gives it the same capabilities as if it were the customer’s IT department. If an abnormality or threat is detected, predetermined procedures dictate appropriate response actions and who gets notified.

In this way, the plant can maintain and manage a safe network infrastructure, allowing plant personnel to focus on safe plant operation and new initiatives to improve productivity. PR

Takashi Hasegawa is the manager of global service business incubation for Yokogawa Electric Corporation. He has over 15 years of experience leading both OT and IT service business planning, including cybersecurity programs for mission critical systems. He is a subject matter expert in industrial automation and control systems cybersecurity service delivery, including managed services.

Yokogawa Electric Corporation
www.yokogawa.com

MORE ONLINE
Visit **processingmagazine.com** for more on cybersecurity.