Featured Articles I

Process Industry Examples

Control Security Support in Hitachi Instrumentation Systems

Shigenori Kaneko
Kazunobu Morita
Tomoyuki Sunaga
Hitoshi Murakami
Makiko Murakami
Katsumi Hanashima

OVERVIEW: Many industries typically have long upgrade cycles for plant production lines and production control systems, and are often still using old machines. In the past, systems were protected by having no connections to external networks, however, since external connections have become unavoidable due to the growing use of big data and the IoT, systems are becoming increasingly vulnerable to security threats. To address this issue, Hitachi has proposed a method of improving security that uses templates to reduce the workload on production sites. The concept behind this method divides security measures into three whitelists that prioritize affinity with production lines and production control systems.

INTRODUCTION

TO increase productivity in plants and factories, many industries are increasingly using the Internet of Things (IoT) as a way to improve construction of new equipment, extend the life or improve the utilization of existing equipment. The IoT is being used for big-data analysis of operation data, and for gathering equipment and system statuses in the form of data.

Inevitably, control systems will need to be connected to external systems for things such as sending equipment data to the cloud server for big-data analysis of operation data, and using wireless or carrier lines for IoT compatibility.

Japan's government has responded by enacting the Basic Act on Cybersecurity, which specifies 13 key infrastructure areas. Cybersecurity measures are considered key requirements for the production equipment of various industries. However, sites prioritize response measures that are taken to keep equipment operating and to ensure productivity. Standard response measures that start with upstream consulting, and then involve system threat analysis, security system installation, and parameter setting increase the site workload, making them difficult to implement.

When instrumentation systems contain production lines or production control systems and are used as production equipment, Hitachi feels it is important to define templates of security measures for them. These templates are used to propose and implement systems, aiming to provide security solutions that do not increase site workload. Hitachi's work in this area is gaining momentum. This article looks at these solutions.

FEATURES AND ISSUES FOR PRODUCTION LINES AND PRODUCTION CONTROL SYSTEMS

The instrumentation system for a production line or production control system has a system configuration mainly composed of a client/server-based manufacturing execution system (MES), a distributed control system (DCS) with a human-machine interface (HMI), an engineering station (ENGS), a controller, and the network that links these components.

The conventional idea that this system is safe because it is offline has been largely abandoned today. And even if the system is connected through a firewall, there are high risks of cyber-attacks via remote monitoring systems and office automation (OA) systems, and of direct attacks and malware infiltration. These risks are the result of big data usage and IoT compatibility. They can be caused not only by connecting control systems to external systems, but also by network-based remote monitoring, connection to OA systems, and the use of removable memory media such as universal serial bus (USB) memory (see Fig. 1).

To devise templates for security measures to combat these risks, Hitachi compiled a list of system features and issues. It found the following three points are key for templates:

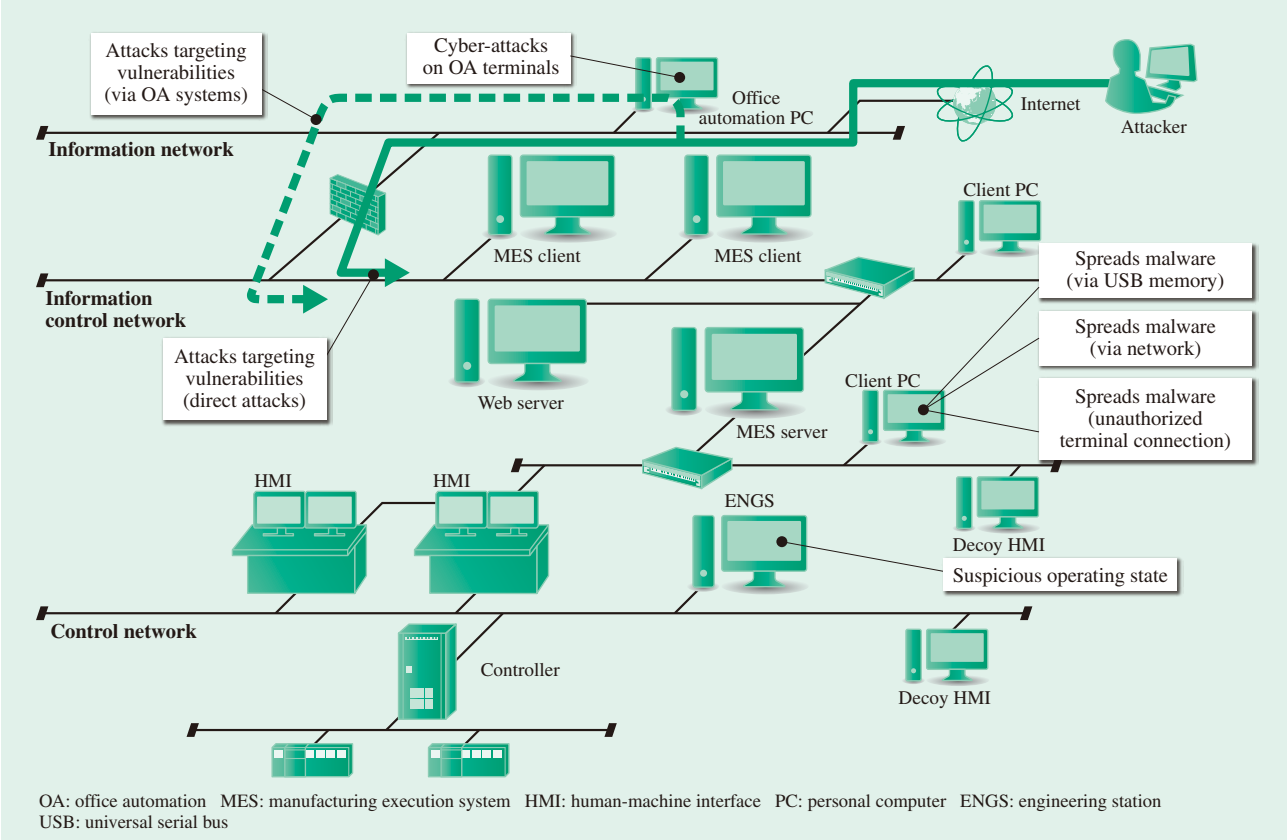

Fig. 1—Production Line/Production Control System Overview and Security Threats.
A standard production line/production control system is defined and made into a template to analyze threats and create templates for security measures. The security level can be selected and the system gradually improved in accordance with the budget and system.

(1) Long system life

While the hardware and software comprising IT systems have maintenance/service periods of five to seven years, production lines and production control systems are used for longer terms of 10 to 20 years.

This longer life results in the problem of software and operating systems (OS) exceeding their support period and continuing to be used without providing security patches for them.

(2) Inability to shut systems down

Three elements are considered important for information security response measures—confidentiality, integrity, and availability. Among these elements, the availability of not being able to shut a system down is often prioritized, resulting in the problem of not being able to make frequent upgrades (requiring restarts) using security patches or security tools.

(3) Frequently critical delayed responses

Some systems are time-critical types that do not permit delayed responses, so a delayed response in applying a security patch or installing a tool could ultimately be fatal for them. Another problem is the difficulty of adding programs after a system has been put into operation, because upgrades must be carefully examined to determine their effect on system response.

SECURITY REQUIREMENTS AND SECURITY CONCEPTS FOR PRODUCTION LINES AND PRODUCTION CONTROL SYSTEMS

Below is a discussion of requirements derived from the features and issues listed in the previous chapter.

Security Requirements

(1) Systems that are offline

The first requirement is an extension of previous security concepts—it must be possible to provide responses to offline systems operating in an offline network environment not connected to any external system. Although external connection is becoming mandatory, there are still many systems in offline environments. These systems cannot update signature and pattern files in real time, so they must maintain a secure state in the environment in which they were adopted.

(2) Systems that have long lives

The second requirement is that tools installed in OSs must work on legacy OSs. To enable use for long periods, they must also work on OSs that have exceeded their support periods.

(3) Systems that are given priority because they cannot be shut down

The third requirement is that systems are not permitted to be shut down and restarted. Since system shutdowns are directly linked to the continuity of the business itself, system shutdowns and restarts for purposes such as software updates must be kept to a minimum.

(4) Systems that are time-critical

The fourth requirement is that delayed responses must not occur. A delayed response in applying a security measure has a very high risk of developing into a critical problem.

Security Measure Concepts

To satisfy the requirements above for the purpose of continuing business without shutting down production lines or production control systems, a multi-stage defense approach is an effective way to implement containment measures. This approach presupposes the risk of malware infiltration, while reducing the infiltration risk and rapidly detecting infiltration to prevent its spread to peripheral equipment. Hitachi has proposed the following three whitelisting concepts:

(1) Whitelisting applications

(2) Whitelisting devices connected to networks

(3) Whitelisting control network communication

SECURITY MEASURE PROPOSALS FOR PRODUCTION LINES AND CONTROL SYSTEMS

(1) Whitelisting applications

Hitachi has enabled responses with affinities to systems conforming to templates by limiting the applications that run on the system, and by using whitelist-based security products that circulate in the market and have been checked for compatibility (see Fig. 2).

(2) Whitelisting devices connected to networks

Networks are whitelisted by limiting the devices that may be connected to the network (see Fig. 3). Hitachi has released a product that detects unauthorized connections. It can be installed outside the network and after-the-fact, enabling installation with affinity to both new and existing systems (see Fig. 4).

(3) Whitelisting control network communication

Control networks contain physical production lines or production control systems, enabling communication recipients to be determined in advance,

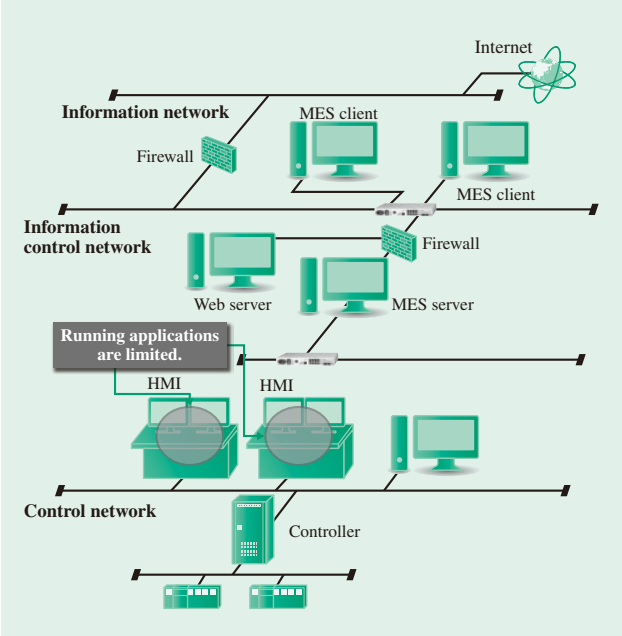

Fig. 2—Whitelisting of Applications.
The applications that run on the HMI are limited to protect the system.

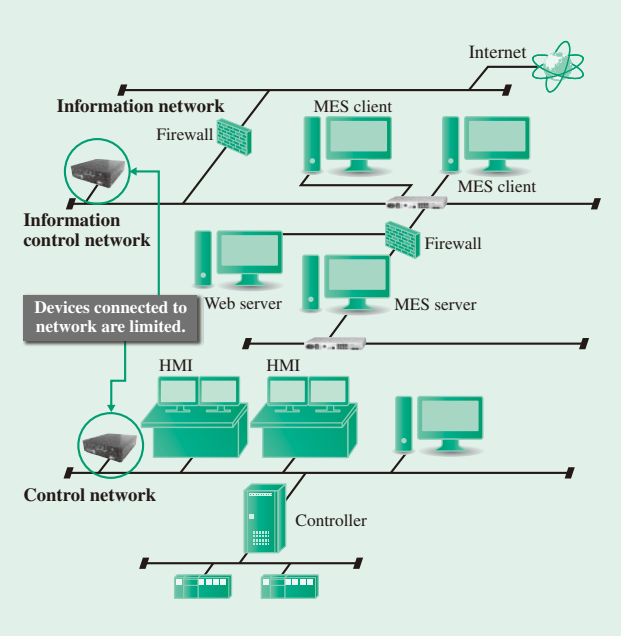

Fig. 3—Whitelisting of Devices Connected to Network.
The devices that can be connected to the network are limited to protect the system.

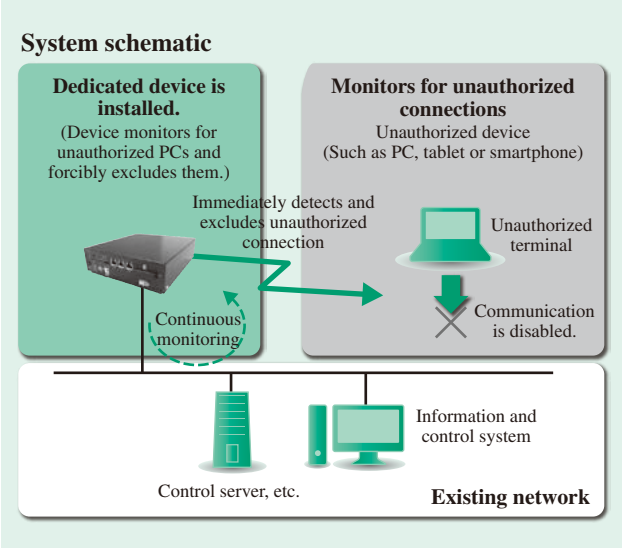

Fig. 4—Unauthorized Connection Detector.
This detector detects and automatically excludes attempts to connect unregistered devices to the network, to prevent the threat of cyber-attacks.

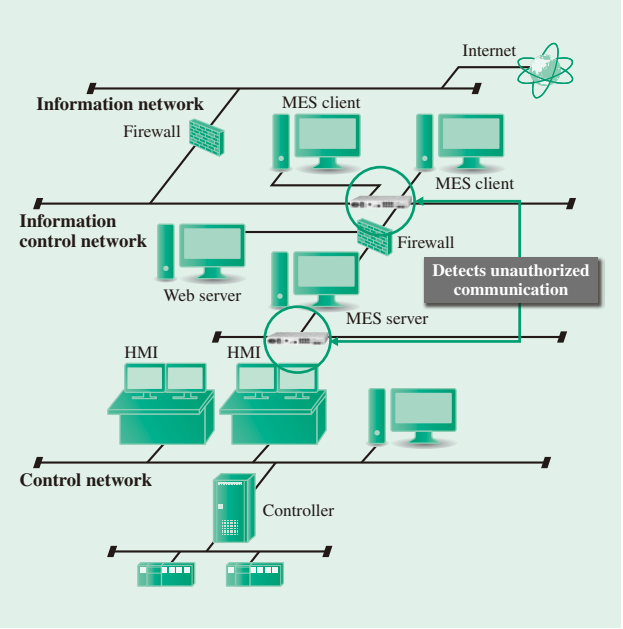

Fig. 5—Whitelisting of Control Network Communication.
A tool for detecting unauthorized communication is added to the network to protect the system.

and detection of unauthorized communication. These characteristics can be used to enable communication whitelisting (see Fig. 5).

Unauthorized communication can be detected using the network switch for industrial control systems product released by Hitachi (see Fig. 6), or a product provided by a specialist security vendor. To ensure affinity between these products and the protected systems, it may be possible to define control network types in terms of the templates proposed by Hitachi, enabling easy installation at the site. These types can be defined by evaluating and investigating combinations of systems, taking into account whether they are new or existing systems.

Fig. 6—Network Switch for Industrial Control Systems.
It has been made more environmentally resistant, enabling installation in site equipment. In addition to providing typical network functions, it detects and automatically excludes unregistered communication.

CONCLUSIONS

This article has discussed some examples of template-based security measures that take site workload into account and enable easy installation, while conforming to the characteristics of the protected production line or production control system.

Hitachi will continue to value Hitachi company technology, while providing security ecosystems that serve as total solutions for protecting client systems. These solutions are created by appropriately combining different security products, and are used to protect products such as Hitachi's integrated instrumentation system, and Hitachi's digitally integrated monitoring control system.

REFERENCES

(1) H. Osonoi et al., "Information and Control Platform for Utilization of Plant Data," Hitachi Review **65**, pp. 70–76 (Jun. 2016).
(2) S. Okubo et al., "Plant Monitoring and Control System for Building Secure Systems," Keiso **58**, No. 12, pp. 34–37 (Dec. 2015) in Japanese.

ABOUT THE AUTHORS

Shigenori Kaneko

Control System Platform Development Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of component products for control systems. Mr. Kaneko is a member of the Information Processing Society of Japan (IPSJ), The Society of Instrument and Control Engineers (SICE), and the Society of Project Management (SPM).

Kazunobu Morita

Industrial Manufacturing Solution Division, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in the industrial production solutions business.

Tomoyuki Sunaga

Industrial System Engineering Department, Industrial Manufacturing Solution Division, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in coordinating industrial instrumentation systems.

Hitoshi Murakami

Management & Development Group, Instrument & Control Systems Sales Division, Instrument & Control Systems Division, Hitachi High-Tech Solutions Corporation. He is currently engaged in business planning for industrial instrumentation systems.

Makiko Murakami

Control System Platform Development Department, Control System Platform Development Division, Services & Platforms Business Unit, Hitachi, Ltd. She is currently engaged in the development of middleware software for industrial instrumentation systems.

Katsumi Hanashima

Control System Platform Development Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in coordinating middleware software development for industrial instrumentation systems.