Ideal Solutions Derived from Field Surveys −Cybersecurity Countermeasures for Next-generation Plants−

Takashi Sekido [*1] *Shoichi Doi* [*1]
Katsunori Iijima [*1] *Kentaro Hayashi* [*1]

The Industrial Internet of Things (IIoT) has increasingly been used in business. Various systems are connected to networks, and many devices are connected to these systems via networks. As the IIoT spreads worldwide, not only devices but also communications between plants in Japan and overseas will connect beyond the boundaries of companies. However, although network-based devices connected via IIoT create new business opportunities, networking also brings new threats and challenges due to the connectivity itself.

Yokogawa's IT infrastructure for the next-generation factory strives to meet the requirements of "safe and secure operation," "flexible and scalable system," and "quick information-gathering and correct decision-making" to build the optimal factory for the IIoT environment. This paper describes the key points of next-generation plant network security and Yokogawa's security measures for control systems based on plant IT network issues, verification of the latest technology, and installation and operation in actual plants.

INTRODUCTION

The industrial internet of things (IIoT) has actively been investigated, developed, and introduced into factories, aiming to create new value and use it for business by interconnecting various "things" via networks and communicating data. In factory manufacturing sites, devices have conventionally communicated in limited environments as listed below, but are now being connected to the factory IT infrastructure and sharing data.

- Servers and PCs in closed environments
- Security cameras and various sensors
- Wearable devices

As various devices become interconnected and factory systems become more complex, the departments that manage and operate factory IT infrastructure as well as information systems departments are facing new challenges such as increasingly sophisticated cyberattacks and regulations on major infrastructure business entities.

This paper describes the key points to realize the IT infrastructure that next-generation factories require, based on customer issues, concerns and site feedback.

*1 Lifecycle Service Business Division, Business Incubation Department, IA Systems and Service Business Headquarters

NEW CHALLENGES FOR FACTORY IT INFRASTRUCTURE ARISING FROM IIOT

To improve the environment for the IIoT, the first task is to survey the current status and identify the risks of factory IT infrastructure. Traditionally, factory IT infrastructure has been arranged in a layered structure with each layer dedicated to each function. In contrast, factory IT infrastructure of the IIoT age must be designed taking into consideration not only the horizontal and vertical "connections" within a factory but also the "extendability" including connections with the intracompany WAN and the internet. To respond to such structural changes, it is essential to identify the current status and latent risks before taking any action.

Next, new challenges that have not been considered in traditional factory IT infrastructure must be tackled, such as monitoring network conditions and cybersecurity measures, to design the IT infrastructure for next-generation factories and achieve continuous management. To solve such challenges, advanced network security engineers are required. However, such engineers are rarely available in factories, and in many cases the factory IT infrastructure is managed concurrently by the personnel in charge of instrumentation of manufacturing equipment. Therefore, to achieve design and management of factory IT infrastructure smoothly, a system is required that can be easily introduced and managed in factories without professional engineers, and whose management status can be shared with the information systems department of the headquarters.

The third challenge is risk management. It is very difficult to identify risks through a survey of the current status, plan measures, and manage the risks continuously. In fact, cyberattacks are becoming more and more sophisticated yearly and serious damages by cyberattacks have been reported. Cybersecurity is a business risk. Hence, it is required for executives to understand it as a crucial managerial issue and make invest in security in advance, such as establishing a system of security training, management, operation, audit, etc. However, currently, not many customers have a system for identifying the status of factory IT infrastructure and assessing risks. Figure 1 shows the recommended risk management of IT infrastructure that the next-generation factory should consider.

EFFECTIVE SOLUTIONS

Usually, Yokogawa analyzes the current status based on global standards, such as IEC62443 or the National Institute of Standards and Technology (NIST) SP800 series, to solve the challenges in work sites and of site managers who have difficulties in exactly identifying the situation. As a result of the analyses, management measures that seem to be effective are selected, broken down into executable items, and are proposed to customers as tangible solutions. Regarding the challenges described above, three solutions that are commonly effective for most factories are described below.

Current Status Survey and Risk Diagnosis of Factory IT Infrastructure and IT Assets

A survey of the current status of factory IT infrastructure is imperative for analyzing the current status of the connections among the devices and networks existing in a factory. Yokogawa focuses on identifying the current network status. The identification operation starts with the following steps.

- Checking all network wirings and the connection status of switches and hubs (by interview and field survey).
- Examining the sources and destinations of all transmissions, and visualizing and checking what kinds of communication are going on.
- Checking the terminal information and risks of all systems.

The information acquired by the survey is reproduced in a simulated (virtual) environment, cross-checked against

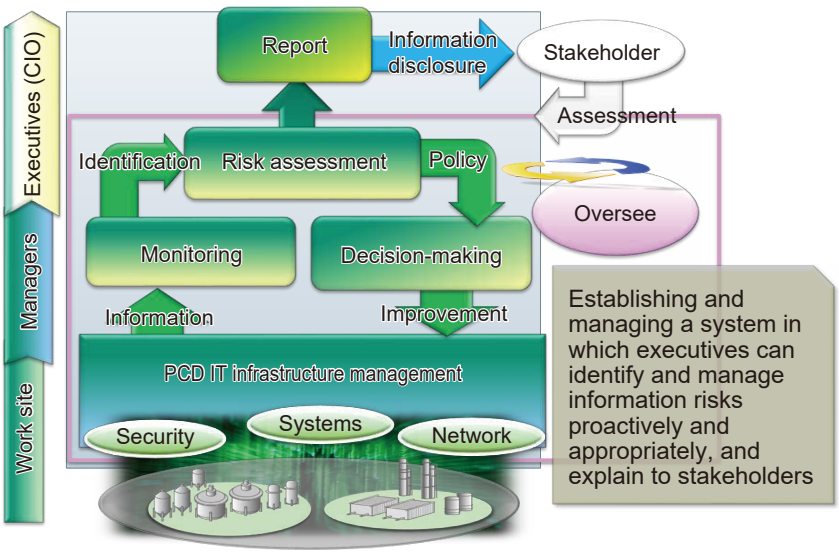

Figure 1 Risk management in the next-generation factory IT infrastructure

a cyberattack database (a database of existing vulnerabilities and cyberattack techniques including attack scenarios), and visualized. Based on the results, vulnerable points in the customer's environment and the measures required to protect the customer from attacks are examined according to the requests of the customer. Finally, measures for improving the factory IT infrastructure and strengthening security are proposed to the customer.

Example of Effective Enhancement and Improvement by Virtual Network Technology

Recently, software defined networking (SDN) is drawing attention in the IT industry. SDN refers to networks and their architectures that control communications dynamically by means of software.

With the conventional network technology, network devices such as routers and switches must be arranged and wired depending on the particular system, location, and facility. In contrast, SDN enables centralized control, construction and modification of the network easily because SDN can construct a virtual network freely for each system by means of software that integrates physical network devices and wiring.

An example of reforming a customer's factory IT infrastructure is described below. The challenges in this IT infrastructure were revealed by field surveys, and the reform was based on SDN and global standards. When using the conventional network design method, physical and logical networks are closely interlinked through locations and IP addresses, and hence sometimes cannot conform to global standards. In contrast, SDN enables physical and logical networks to be separately designed. Therefore, it is possible to design logical networks conforming to global standards, while keeping physical networks in the current conditions as much as possible. In particular, independent virtual networks can be constructed for each system freely by means of software, even in a physical network environment in which all factory systems are located on the same segment, allowing free communications among different systems.

As an application, secure networks can be achieved by partitioning and segmentation. For example, systems that bear security risks to new threats due to termination of vendor support can be grouped together and isolated on a virtual network, so that they cannot communicate directly with the outside.

In SDN, the physical networks and the logical networks that operate on them are separated so that it is possible to separate the networks virtually without modifying the IP addresses of the existing terminals for introducing SDN. Moreover, in an increasing number of cases, many sensor devices are newly mounted in a factory to collect data in an effort to promote the IIoT. In such cases, an IIoT-dedicated virtual network can be constructed on a common physical network, being isolated from other virtual networks.

Surveillance Service to Monitor the Status of Factory IT Infrastructure

Yokogawa offers a service for the integrated surveillance of factory IT infrastructure, in response to a wide variety of needs ranging from individual optimization of overseas factory IT infrastructure to integrated factory management driven by the headquarters. Traditionally, each factory of a customer has managed the operation of its own factory IT infrastructure. Therefore, IT engineers had to be employed at each factory. However, it is not easy today to assign enough IT engineers to each factory, and in many cases persons in charge of field instrumentation are concurrently responsible for the factory IT infrastructure. Also, in some cases management is not unified among factories, while in other cases it is not managed at all. To improve this situation, under this service Yokogawa provides support for operating and managing factory IT facilities on behalf of the customer, thus maintaining the factory IT infrastructure, which is managed by the factories individually, at a constant level.

Figure 2 shows the details of the surveillance service, in which a unique architecture is defined with the surveillance

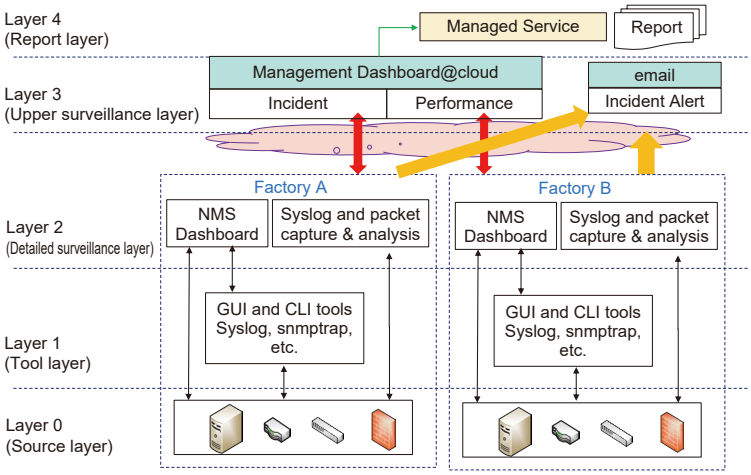

Figure 2 Surveillance architecture

layer divided into five. Layer 0 (source layer) includes data-holding devices that are the surveillance sources. Layer 1 (tool layer) captures and processes the data from Layer 0 devices, using the surveillance tools attached to individual devices and various other tools, such as syslog and snmptrap, belonging to the OS of the Network Management System (NMS) server. Layer 2 (detailed surveillance layer) consolidates and visualizes the data using NMS tools and log analysis tools. Then, Layer 3 (upper surveillance layer) integrally monitors the status of multiple factories using dashboards on the cloud. Finally, Layer 4 (report layer) prepares and issues monthly and other reports, based on the information from the lower layers.

In actual surveillance, an alert mail is issued in Layer 3 first where the status on the dashboard must be checked. Then, the details are drilled down to explore the cause using the tools of lower layers. Finally, coming back to Layer 4, the status is reported to the customer.

An additional function of this surveillance service is being developed to enable preliminary operation tests in a clone environment for the cases of network addition or modification. Since errors in design or setting may cause network failures, conducting a preliminary test in a virtual environment will reduce the risks associated with network modification operations. Figure 3 shows an overview of the surveillance service.

In the surveillance service, the data from IT infrastructure of the customer's factories are collected and analyzed, and the statuses of their IT asset management, operation, and security are visualized on the dashboard. Then the health of the IT infrastructure is analyzed. If some unusual status is found, it is immediately reported to the customer. Even if the IT infrastructure is operating without any abnormality, the operation status is reported to the customer as a monthly IT report. If a security incident or device failure occurs, Yokogawa reacts quickly to restore the normal state, by responding remotely and dispatching maintenance engineers.

Through this service, Yokogawa solves customers' challenges in responding to network failures, maintaining security, quickly developing IT infrastructure, and securing human resources, and supports the next-generation factory IT infrastructure connected to the worksites.

YOKOGAWA'S EFFORTS TO SUPPORT CUSTOMERS' SECURITY ACTIVITIES AND SYSTEM SOUNDNESS THROUGHOUT THE SYSTEM LIFECYCLE

Yokogawa's system and its efforts to support customer systems throughout their lifecycle are described below.

Information Security Committee

Yokogawa defines a system lifecycle to be the entire period from product development to system introduction and operation. By supporting customers' security activities throughout the system lifecycle, Yokogawa strives to reduce the risks to critical infrastructure arising from cyberspace. To improve the response capability to cyberattacks, Yokogawa has established a committee composed of personnel in charge of security from product development, engineering, service, and other divisions, and is rolling out the initiative across the organization.

Security in Product Development

Yokogawa has established the basic policy and measures criteria for the security control of products. By implementing them in product development processes, Yokogawa is striving to eliminate vulnerabilities from products and improve security. Especially, the products of CENTUM VP and ProSafe-RS, which are the core products of Yokogawa, have

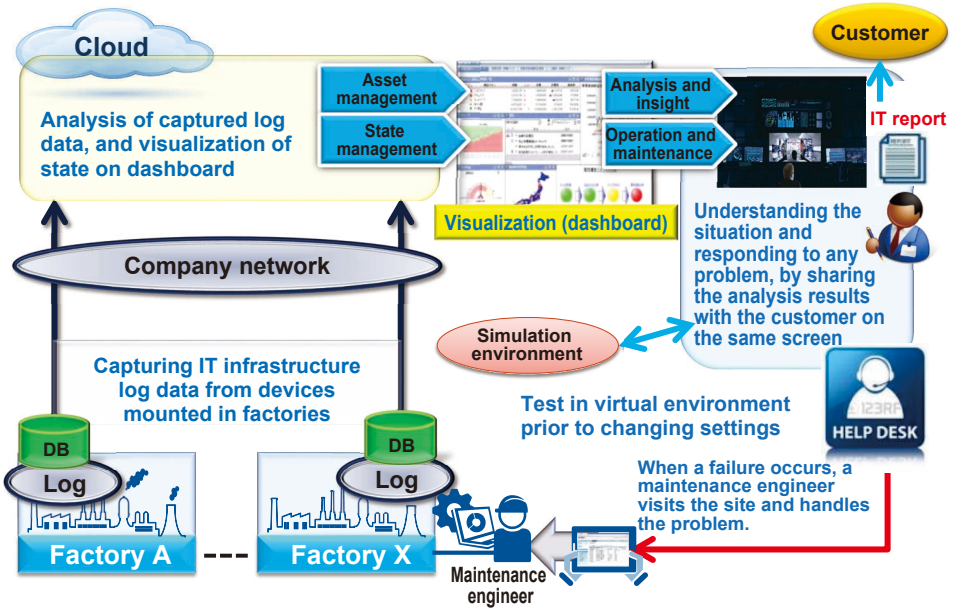

Figure 3 Image of Yokogawa's surveillance service

obtained the ISASecure Embedded Device Security Assurance (EDSA) certifications by the ISA Security Compliance Institute (ISCI), which is a global security authentication organization, to ensure the quality of security. The handling of vulnerabilities found after product delivery is determined by Yokogawa's Product Security Incident Response Team (PSIRT), in collaboration with related departments within Yokogawa and external Computer Security Incident Response Team (CSIRT) organizations. As soon as the response is determined, the relevant information including the countermeasures is released on a public agency database, Japan Vulnerability Notes (JVN), and on Yokogawa's website.

Security in Engineering

The Security Laboratory of Yokogawa takes the initiative in investigating and developing security technologies and supporting the introduction of security measures into systems. Thus, Yokogawa pursues unified and secure implementation of security in system integration. To offer stable engineering quality to customers, in-house security training is provided to engineers. Especially, Yokogawa encourages engineers to obtain the Global Industrial Cyber Security Professional (GICSP) certification, which is a security engineering measure related to industrial control systems.

Security in Service

Yokogawa offers Security Risk Communication, in which customers can talk with us about recent incidents and cyber threats. Customers and Yokogawa examine how to proceed with security measures by sharing the latest information on cyber security risks. The Security Risk Communication has been held at about 300 offices in Japan and 200 offices overseas, and some 3,000 people have attended.

Responding to Incidents by Cross-functional Organization

The IEC62443 global standard and the guideline by NIST, Cyber Security Framework, require measures to be prepared in advance for security incidents during plant operation, so that such incidents can be dealt with quickly and appropriately.

Yokogawa supports customers in establishing more robust systems by designing security policies with the customer, by preparing response procedures in the case of a cyber incident, and by providing training based on built policies and procedures. When an actual incident occurs, Yokogawa forms a cross-departmental response team in Yokogawa, and at the same time, service engineers are dispatched to the customer's site. This response team supports investigation of the cause and recovery work, in collaboration with the Yokogawa engineers at site.

CONCLUSION

This paper summarized the challenges and the ideal state of next-generation factory IT infrastructure, to prepare for the accelerating shift toward the IIoT and the explosive growth of factory data by digital transformation (DX). In addition, examples of Yokogawa's solutions using SDN were described. Furthermore, the security activities of Yokogawa to maintain system soundness throughout the system lifecycle from product development to system delivery and operation were introduced.

In the future, the risk of cyberattacks is expected to increase due to sophisticated attacks targeting industrial infrastructure. Yokogawa will strive to offer optimal solutions to help customers ensure safety and security in their efforts toward "connected factories" in the IIoT age.