Yokogawa's Commitment to Developing Secure Products That Contribute to Achieving the SDGs

Hiroshi Hoshino [*1] *Hirotaka Tsuji* [*1]

Plants and critical infrastructure are the foundation of society, and their long-term, stable operation must be ensured to maximize the availability of facilities and to keep providing products and services to customers. For this purpose, it is necessary to introduce secure products and equipment to protect the facilities against cyberattacks. This commitment also helps achieve a resilient social infrastructure defined in the SDGs (SDGs 9).

Addressing vulnerabilities is the basis of developing secure products. However, the priority of doing so is often lowered in the development process because it does not directly improve development efficiency and product functions (usability).

These problems cannot be solved by a single business unit. As a company responsible for social infrastructure, Yokogawa has been tackling this challenge by adopting a company-wide approach to governance, development, and a system to support them. This paper describes Yokogawa's commitment to the development of secure products. Specifically, these are the company's policy, organizational structure, process of developing secure system products (Secure Development Life Cycle: SDLC), and acquired international certifications.

INTRODUCTION

Cybersecurity threats are becoming a serious social issue as their targets spread to social infrastructure. Notorious examples are the 2015 and 2016 cyber-attacks in Ukraine, which shut off breakers in electrical substations. In the former incident, massive power outages affected 220,000 households for six hours. The 2017 cyber-attack targeting the safety instrumentation system of an oil plant in Saudi Arabia disrupted a program of the controller, causing the plant to shut down. If the system had been completely hijacked, it could have damaged the safety, environment, and human life. Clearly, the companies responsible for social infrastructure must keep taking measures for cybersecurity.

*1 Cybersecurity Management Department,
Lifecycle Service Business Division,
IA Systems & Service Business Headquarters

SECURITY MEASURES FOR LONG-TERM STABLE OPERATION OF FACILITIES

Asset owners of plants and critical infrastructure aim to achieve long-term stable operation to maximize the availability of their facilities and offer value to their customers and users, and so need to introduce secure products and protect them from cybersecurity threats. This is related to achieving SDG 9 "Build resilient infrastructure." This section explains Yokogawa's efforts to develop secure products and ensure long-term stable operation of facilities.

General Security Measures and Their Issues

There are various security measures for a control system, which is one of the main components used to operate plants and critical infrastructure. Yokogawa has long been developing security measures for control systems. Specifically, we provide operating system (OS) update programs so that control systems keep running stably. We also offer anti-virus software that can be used in combination with control equipment. This kind of support for securely managing and maintaining control systems reduces the risk of security incidents as well as shutdowns and allows equipment to keep operating stably for a long time.

Although OS update programs and anti-virus software are effective security measures for control systems, they do not prevent attacks on vulnerabilities in the control system software. A vulnerability is a security weakness in software which attackers could use to illegally obtain information or hijack the system. It is essential to eliminate such vulnerabilities to ensure the long-term stable operation of control systems.

Vulnerabilities must be carefully detected and addressed throughout all processes and even after shipment. However, doing so typically does not directly improve the functionality of products or improve the efficiency of development, and so may not receive priority in the development process. This dilemma is similar to difficulties in achieving the SDGs. Pursuing economic benefits may produce unintended side effects, creating vulnerabilities that may endanger the health of society. The SDGs were drawn up to overcome this problem. Both approaches try to avoid pursuing only convenience and efficiency.

Governance and Development Process as a Solution to Challenges

Individual business units cannot solve vulnerabilities by themselves. To address such problems while pursuing economic benefits, a company involved in social infrastructure needs to have appropriate corporate governance and development processes, as well as a system to support them. The following sections explain Yokogawa's efforts to develop secure products, focusing on the rules and systems for developing secure products, a process for developing secure system products, and efforts to obtain certifications.

MEASURES AGAINST CYBERSECURITY THREATS TO PRODUCTS

Yokogawa provides products and services that help build resilient social infrastructure. This section explains Yokogawa's corporate governance on how to manage the cybersecurity risk to products, how to develop secure products, and how to properly address vulnerabilities.

Managing Cybersecurity Risks to Products

To achieve long-term stable plant operation, customers need to introduce secure systems and then maintain the security level.

To help such customers, Yokogawa provides not only secure products but also countermeasures throughout the plant lifecycle, such as solutions to mitigate vulnerabilities after delivery and secure the operating environment. This issue cannot be solved by individual business organizations.

Therefore, Yokogawa launched a company-wide project in 2015 and drew up a basic policy for business organizations to work together with the same approach. Currently, each business organization shares the basic policy and maintains the security level of the systems at our customers' sites.

<<Basic Policy>>

The Yokogawa Group will work together with its customers on cyber threats to their assets to enable customers to continue their business safely and securely.

System for managing cybersecurity risk to products

Since a cyber-attack on Yokogawa's products could result in an opportunity loss for customers, Yokogawa considers this kind of risk as a management risk. Under the cybersecurity risk management system (Figure 1), product-related cybersecurity risks are monitored and reviewed by a person in charge of risk management and the risk management organization. The results of the review are reflected in the Group regulations as the response policy and standards. Under the supervision of the administrator, persons in charge of product planning and development and those in charge of service incorporate the Group regulations into their own management procedures and perform their tasks. Each business organization thus provides secure products and services to customers.

Activities for managing cybersecurity risk are audited by an audit organization and the results are reported to the board of directors meeting and managers meeting.

As mentioned above, activities related to cybersecurity risk for our products are supervised by Yokogawa's management. The Group recognizes the importance of long-term stable operation at our customers' plants and is working hard to achieve it.

Efforts to improve cybersecurity response

To maintain the security level of customers' systems, each business organization must work together. The same is true for managing internal information and related infrastructure.

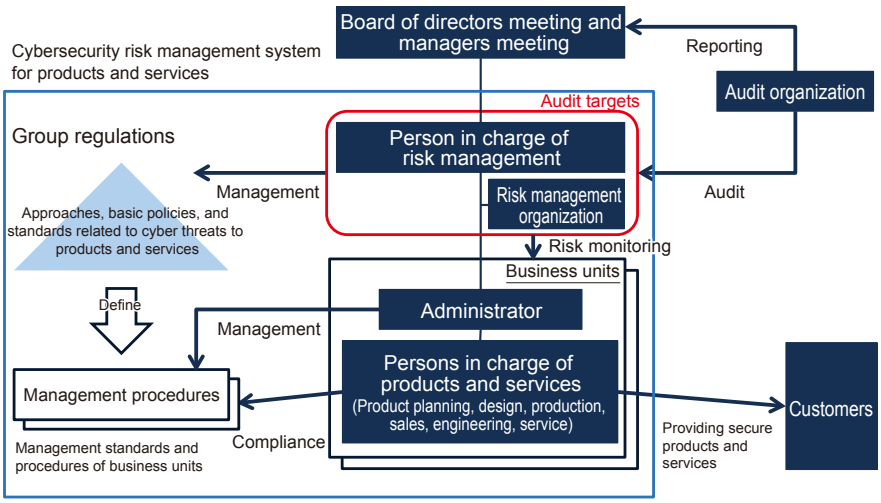


Figure 1 System for managing cybersecurity risks

If any confidential information about a product should leak, we must promptly inform those concerned of its impact and risk. For this purpose, the following organizations must work together: the Information Security Management System Office (ISMS Office), which controls information management; the Computer Security Incident Response Team (CSIRT), which addresses cyber incidents on information infrastructure; the Product Security Incident Response Team (PSIRT), which responds to cyber incidents on products; and persons in charge of the security business who provide solutions to customers.

Yokogawa has a cross-organizational information security committee for sharing cybersecurity information (Figure 2).

Under an officer responsible for security, the Information Security Committee consists of the ISMS office, CSIRT, departments in charge of product security, departments in charge of marketing that research information, and departments in charge of security business that provide solutions. This committee keeps abreast of the latest trends in cybersecurity and shares information to improve the Group's response to cybersecurity threats.

Efforts to Develop Secure Products

As a company responsible for social infrastructure, Yokogawa strives to eliminate vulnerabilities from its products to ensure the stable operation of customers' plants.

To develop secure products without vulnerabilities, we have defined management standards and procedures in the Yokogawa Group Design Standards. For each development process, we make sure that the criteria of security design are

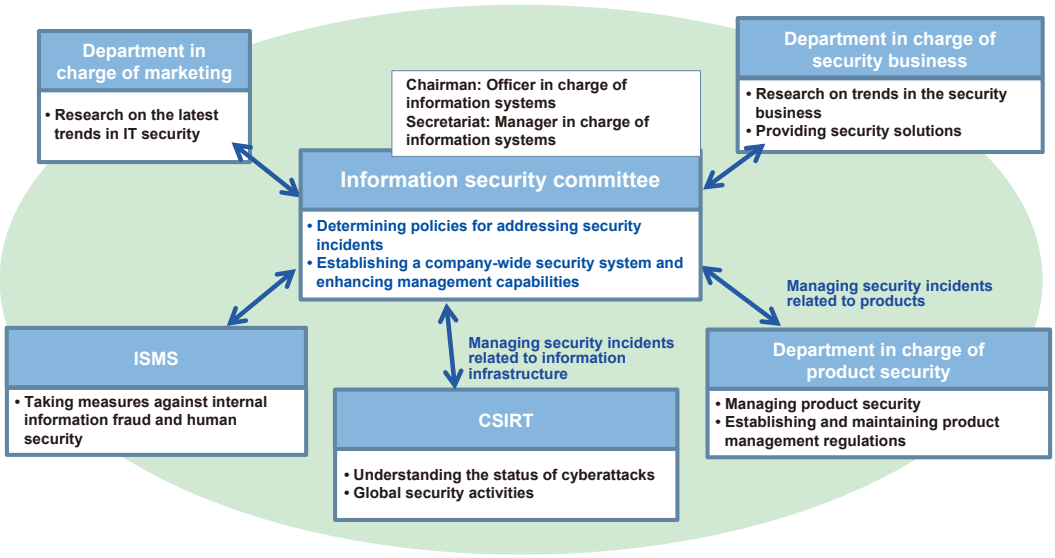


Figure 2 Information-sharing system

satisfied in the quality management system.

To keep up with evolving cyber threats, the Engineering Standards are regularly reviewed by a cross-organizational product security committee. The committee also takes the lead in developing guidelines and tools for secure products and supports the departments in charge of development.

Based on these efforts, we make sure that each product meets the strict security requirements of our customers. Regarding control system products, we are actively obtaining security certifications, as described in the section "EFFORTS TO DEVELOP SECURE CONTROL SYSTEM PRODUCTS."

How to Handle Product Vulnerabilities

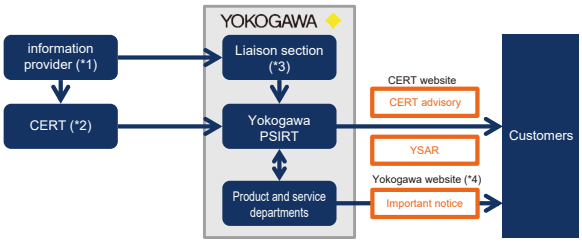
Customers need to manage cybersecurity risks to strengthen and stabilize plant operation. For this purpose, it is essential to identify the vulnerabilities of equipment installed in plants and countermeasures. Yokogawa discloses such information to help customers manage their cybersecurity risks. Coordination with internal and external parties (information providers, persons in charge of products and services, and so on) is necessary to obtain and disclose appropriate information. The following sections describe the process and system for handling vulnerability information, from acquisition to disclosure.

Process and system for handling vulnerabilities

Yokogawa has set up Yokogawa PSIRT, an organization for handling product vulnerabilities, and discloses relevant information to customers following a vulnerability handling process based on the ISO/IEC30111 international standard (Figure 3).

Figure 3 Vulnerability handling process

Yokogawa PSIRT actively gathers information from both inside and outside Yokogawa, collaborating with JPCERT/CC and ICS-CERT. In the verification process, obtained information is forwarded to persons in charge of development and service to determine whether any products are affected. In the severity evaluation process, Yokogawa PSIRT works with persons in charge of development and service of relevant products to assess the significance of the vulnerability. In the release process, the organization discusses the timing and content of the disclosure with external information providers, ICS-CERT, and persons in charge of development and service. Based on the results, Yokogawa PSIRT works with persons in charge of development and service to prepare a Yokogawa Security Advisory Report (YSAR) and discloses the information to customers on Yokogawa's website and other media. For coordination with internal and external stakeholders, the organization follows the Information Security Early Warning Partnership Guidelines established by the JPCERT Coordination Center (JPCERT/CC) and the Information-technology Promotion Agency (IPA), both of which are coordination organizations for vulnerability information in Japan. Figure 4 outlines the activities of Yokogawa PSIRT.



(*1) People who provide vulnerability or threat information, such as researchers or customers
(*2) Computer emergency response teams such as JPCERT/CC and ICS-CERT
(*3) Yokogawa Group' s service centers and liaison sections
(*4) https://www.yokogawa.com/us/solutions/products-platforms/announcements/

Figure 4 Activities of Yokogawa PSIRT

Yokogawa PSIRT follows international standards and guidelines for handling vulnerabilities and delivers useful information to customers to help them manage risks. The organization is systemizing the process to respond to the increasing volume of vulnerability information. This effort will help improve the efficiency in the Group and provide information to customers in a timely manner.

Providing vulnerability information

Yokogawa discloses product vulnerability information extensively to help customers manage risk. In addition to the investigated and evaluated vulnerability information, we disclose the countermeasures prepared by our development staff to our customers both in and outside Japan. The information is available on our website[1], Japan Vulnerability Notes (JVN)[2] compiled by JPCERT/CC and IPA, and the vulnerability database[3] of ICS-CERT, a global organization for coordinating vulnerability information on control system products.

We also disclose our basic policy on vulnerability handling[4] on Yokogawa's website to help customers and society understand our stance on vulnerability and help them with their risk management.

We received a certificate of appreciation from JPCERT/CC in 2015 for our vulnerability handling[5]. Specific reasons were our outstanding contribution to cybersecurity measures and our pioneering role as a control system vendor.

EFFORTS TO DEVELOP SECURE CONTROL SYSTEM PRODUCTS

Based on Yokogawa Group Design Standards for developing secure products described in the section "Efforts to Develop Secure Products," each development department has its own process. This section introduces the IEC 62443-4-1 international standard[6], which we refer to in developing the process for our products and its examples.

IEC 62443-4-1 International Standard

IEC 62443, an international standard for control system security, specifies requirements for various players involved in industrial control systems (asset owners, service providers, and control equipment product suppliers). IEC 62443-4-1 requires control equipment product suppliers to provide a multi-layered defense-in-depth framework in their development process to take security measures in their design. The practices listed in Table 1 are what control equipment suppliers should do in their development process.

Table 1 Security requirements specified by IEC 62443-4-1 for the development process

Practice (acronyms)	Main objective
Security management (SM)	Building a system for developing secure products
Specification of security requirements (SR)	Defining the security requirements and use conditions
Secure by design (SD)	Security design based on defense-in-depth strategy
Secure implementation (SI)	Secure coding
Security verification and validation testing (SVV)	Documentation and implementation of security-related tests
Management of security-related issues (DM)	Handling identified vulnerability
Security update management (SUM)	Providing security updates
Security guidelines (SG)	Providing users with information necessary for integration

Arranging the Secure Development Life Cycle (SDLC)

The SDLC is Yokogawa's process for developing secure system products in accordance with IEC 62443-4-1. Its purpose is to develop products that do not contain vulnerabilities. The SDLC consists of the six phases described in Figure 5. We develop secure products by minimizing vulnerabilities in the outputs of each phase and identifying vulnerabilities early in the development phase. Each phase is described in the following sections.

Figure 5 Secure Development Life Cycle (SDLC)

Required specification phase

The main purpose of the required specification phase is to understand the requirements and usage conditions of the product, develop a security development system and an action plan, and define security requirements and external specifications. To support these activities, security experts who execute and review security-related activities are appointed for each product. In addition, each development department provides training and education programs on the IEC 62443-4-1 standard to develop future security experts.

Design phase

The main purpose of the design phase is to eliminate as many vulnerabilities as possible that might be created during the design process. In this phase, we design specific features to meet security requirements based on external specifications and check the overall structure of the software in terms of security. We also perform threat analysis to identify the assets to be protected, their interfaces, and possible threats. To support these activities, we have formulated a guideline for developing secure products, which summarizes the points that must be taken into account during threat analysis and designing.

Implementation phase

The main purpose of the implementation phase is to eliminate as many vulnerabilities as possible that might be created during the implementation process. When implementing software based on the design documents, it is necessary to identify and remove code that may cause security problems such as buffer overflows. To support this activity, we use a static code analysis tool, which can identify source code issues that may be overlooked in human reviews.

Verification phase

The main purpose of the verification phase is to make sure that the product does not have any known vulnerability and that security functions are effectively implemented. In this phase, we not only confirm the validity of the security functions implemented to satisfy security requirements, but also conduct security tests with various techniques, such as identifying potential target areas, checking open-source software issues, and conducting fuzzing tests of communication. To support these activities, we use commercial testing tools and improve the efficiency of testing.

Release phase

The main purpose of the release phase is to verify that the necessary efforts have been carried out throughout the development process and that the product is virus-free at the time of shipment. To support these activities, security experts perform a final check with a checklist.

Maintenance phase

The main purpose of the maintenance phase is to address post-shipment vulnerabilities. We collaborate with the aforementioned vulnerability handling organizations, classify reported vulnerabilities, and report vulnerabilities found during development. It may be necessary to apply security patches when any vulnerability occurs in the Microsoft Windows operating system (the platform of our products). In this case, we provide the information necessary for each product as a paid service.

Efforts to Obtain Security Certificates

In 2014, Yokogawa received the ISASecure Embedded Device Security Assurance (EDSA) security certification from the ISCI[7] for the CENTUM VP integrated production control system and the ProSafe-RS safety instrumented system,

both of which are Yokogawa's OpreX Control and Safety System products. In January 2020, Yokogawa's department responsible for developing control systems obtained the ISASecure Security Development Lifecycle Assurance (SDLA) certification from the ISCI for its Secure Development Life Cycle. The latest acquisition is evidence that not only the individual control system products but also Yokogawa's development processes comply with the international standard IEC 62443-4-1.

CONCLUSION

Companies involved in social infrastructure are responsible for making sure that systems for their products operate stably for a long time. For this purpose, it is necessary to continuously work on cybersecurity measures and remain accountable for these efforts. Yokogawa has established a system to address cybersecurity threats to its products and shoulders its responsibilities. We have also obtained external evaluations and certifications for each development system so that our efforts in developing secure products are backed objectively. Through the development of these secure products, Yokogawa will contribute to building a resilient social infrastructure (SDG 9) as well as achieving a Circular Economy, one of Yokogawa's Three Goals towards 2050.

REFERENCES

(1) Yokogawa Electric Corporation, "Yokogawa Security Advisory Report List," https://www.yokogawa.com/library/resources/white-papers/yokogawa-security-advisory-report-list/ (accessed on September 15, 2020)
(2) JPCERT/CC, IPA, Japan Vulnerability Notes (JVN), https://jvn.jp/ (accessed on September 15, 2020)
(3) ICS-CERT website, https://www.us-cert.gov/ics/ (accessed on September 15, 2020)
(4) Yokogawa Electric Corporation, Yokogawa Group Vulnerability Handling Policy, https://www.yokogawa.com/solutions/products-platforms/announcements/vulpolicy/ (accessed on September 15, 2020)
(5) "JPCERT Coordination Center presents a certificate of appreciation to collaborators for cybersecurity activities," (in Japanese) https://www.jpcert.or.jp/press/priz/2015/PR20150820-priz.html (accessed on September 15, 2020)
(6) IEC, IEC 62443-4-1 "Security for industrial automation and control systems–Part 4-1: Secure product development lifecycle requirements," 2018
(7) ISA Security Compliance Institute (ISCI), https://www.isasecure.org/en-US/Certification (accessed on October 4, 2020)