Yokogawa's Comprehensive Approach to Cyber Security for Industrial Control Systems

Nobuaki Konishi [*1]

Cyber security is a major concern for industrial control systems. This paper describes Yokogawa's comprehensive approach to cyber security for industrial control systems. First, it takes a look at cyber security issues regarding industrial control systems and summarizes Yokogawa's basic policy on them. This policy, focusing on a lifecycle approach and "Defense-in-Depth" proposed by Yokogawa, can be the basis for enhancing security in control systems. Then, this paper describes various actual measures based on the policy.

Considering cyber security at the stage of product development, Yokogawa prevents design defects that may lead to vulnerability of its products. A laboratory of Yokogawa specializing in security has established security measures suitable for control systems, based on the experience obtained by Yokogawa through the supply of control systems over many years. These measures are used for system construction and operation. Finally, this paper describes how Yokogawa handles vulnerability when it is detected in its products. With these security activities, Yokogawa will continue to help customers stably operate control systems.

INTRODUCTION

Cyber security must be taken into account for operating recent industrial control systems. One of the reasons is the introduction of information system technologies into control systems. By using information system technologies, control systems have been enjoying the merits owing to connection to information systems but, at the same time, have become exposed to the security risks inherent to information systems. Because the attacking techniques are becoming more sophisticated day by day, simply introducing technical measures is not enough to protect control systems. Comprehensive strategic measures are required.

This paper, firstly, summarizes security issues and the current status of control systems. Then it states the basic policies and Yokogawa's security measures to deal with the issues. Lastly, it describes the security measures that Yokogawa offers during product development, system engineering and the maintenance support period.

PROBLEMS AND CURRENT STATUS OF CONTROL SYSTEM SECURITY

Security Problems of Control Systems

Modern control systems have been utilizing the benefits of information communication technologies to acquire new capabilities and reduce costs. This is, so to speak, the introduction of commercial off-the-shelf (COTS). While COTS has brought demerits such as security problems, it has also brought the various merits of information systems into control systems. Specifically, control systems have the following problems [(1)].

- Contamination of vulnerability risks due to shift to open architecture
  Control systems incorporate the vulnerability inherent to COTS.
- Obsolescence of security measures due to long-term operation
  Control systems are operated for 10 to 20 years, while attacking techniques become more sophisticated year by year. As a result, the security measures installed at the beginning of the operation may be insufficient to prevent the attacks.
- Restricted introduction of security functions due to availability prioritized operation
  Because system availability is highly prioritized in the operation of control systems, new security measures cannot be easily introduced to them. Moreover, the measures themselves may disturb the system operation and thus there is a case where its introduction is postponed until confirmation that there are no problems.

Actual Damage Caused by Attacks

Security problems have been actually arising in control systems. For example, malware originally targeting information systems has damaged control systems, resulting in several plant shutdowns. In 2010, it is widely reported that a malware called Stuxnet [(2)] targeted control systems. In this way, damage to control system security is already spreading and the immediate introduction of measures is required.

*1 Systems Business Division, IA Platform Business Headquarters

ACTIVITIES FOR CONTROL SYSTEM SECURITY IN AND OUTSIDE JAPAN

Activities in Japan

■ Activities of the government

In February 2009, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) established the CEPTOAR-Council to enhance security of critical infrastructures. In accordance with this, the Ministry of Economy, Trade and Industry launched various activities. For example, the Task Force on Control System Security was established in October 2011 to promote strengthening security measures for critical infrastructures in Japan.

■ Activities of public institutions

In March 2012, the Control System Security Center (CSSC) was established. Yokogawa is an original member.

CSSC is a certification body accredited by ISASecure® Embedded Device Security Assurance (EDSA) Certification, and has started certification services. The ISASecure EDSA certification is a certification assuring control system security. Meanwhile, the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) established a certification program for a cyber-security management system (CSMS) for industrial automation and control systems. Yokogawa has acquired the first CSMS and ISASecure EDSA certification in Japan.

■ Standardization activity

The IEC62443 series are international standards for control system security and are being discussed by the Japanese National Committee of IEC TC65/WG10. The Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) serves as the secretariat of the committee. The ISASecure EDSA and CSMS certification programs described above are based on the IEC62443 series.

Activities outside Japan

■ USA

NIST Note 1) documented Guide to Industrial Control Systems (ICS) Security as SP 800-82 [3], one of the SP 800 series. Idaho National Laboratory offers free security training [4] using actual control systems. ISA Note 2) is promoting standardization of security measures as the ISA99 series.

■ Europe

Many European countries standardized and published security measures for control systems. In particular, in the UK and the Netherlands, collections of good practices [5], [6] are released to the public. There are many communities about control system security in Europe; the MPCSIE Note 3) and the ENISA Note 4) are representative examples.

■ International standardization activities

The IEC TC65, a committee for industrial-process measurement, control and automation, is promoting standardization of control system security as the IEC62443 series.

SECURITY MEASURES PROVIDED BY YOKOGAWA

This chapter describes Yokogawa's basic concept on control system security and introduces its current activities. Each activity is described in the article of this issue.

Basic Concept

Yokogawa recommends an approach for mitigating risks in the security problems that control systems are facing. In this approach, lifecycle approach and defense in depth are employed as basic strategies, and technical, operational, and managerial controls are taken for mitigation.

■ Lifecycle approach

The effects of introduced security measures gradually become less effective because security threats including new types of cyber-attacks increase. Therefore, continuous maintenance of security measures is required to maintain their effectiveness. Figure 1 shows Yokogawa's support for the security activities of customers over the entire product lifecycle, from product development, implementation of security measures during system integration to security management during operation. Owing to these activities considering the product lifecycle, customers can lower the security threat to an acceptable level at all times without incurring excessive costs.

Figure 1 Lifecycle approach

Defense in depth

Figure 2 shows the strategy of defense in depth, which Yokogawa advocates as a guideline in introducing security measures. In this strategy, securing safety is most important. Next to this, control functions required for production activities and maintaining the healthiness of control systems constituting the bases for production are important. In addition

Note 1) National Institute of Standards and Technology, http://www.nist.gov/
Note 2) The International Society of Automation, https://www.isa.org/
Note 3) Meridian Process Control Security Information Exchange, http://meridianprocess.org/Default.aspx
Note 4) European Network and Information Security Agency, http://www.enisa.europa.eu/

to them, technical, operational and managerial controls for security must be taken. By improving these security measures through continuous lifecycle activities, customers can secure prevention and mitigation of risks to control systems and prepare for contingencies.

Figure 2 Defense in depth

Product Design and Development Phase

Yokogawa employs security-conscious approaches from the design and development phase.

Security for control system products

To avoid introducing vulnerabilities into products during the development phase, Yokogawa has defined the secure development lifecycle and is practicing said lifecycle. In this lifecycle, security is taken into account to avoid introducing vulnerabilities into products in requirement, design, implementation and verification phases. Yokogawa has acquired ISASecure EDSA certification, a certification assuring control system security, for two products: the CENTUM production control system and the ProSafe-RS safety instrumentation system. More details on the content of this section are described in the paper "Efforts for Enhancing Security in Control Systems" in this issue.

Security for wireless systems

Control systems have been introducing field wireless technologies, but they haven't been completed. One of the reasons is the cyber security issue. Yokogawa applies the ISA100.11a international standard for industrial wireless whose specifications are defined with security considerations taken into account. Because experts on wireless and instrumentation as well as on security are involved in formulating ISA100.11a specifications, devices using its protocol can be used safely. More details on the content of this section are described in the paper "Strong Security Measures Implemented in ISA100.11a Wireless System" in this issue.

Engineering Phase

Even if each component of a control system is secure, the system as a whole still has the possibility of introducing vulnerabilities. To respond to such situation, Yokogawa offers security consulting in the engineering phase. For smooth introduction of systems considering security, Yokogawa offers security consulting services for formulating security policies, and security engineering for introducing technical controls based on the policies.

Security consulting support

When considering security measures, control system users must first define security policies. They must clearly define the objects to be protected in the security policies and identify the threats to these objects, and then they implement the security measures effective against the identified threats. However, all control system users are not overly familiar with the security measures. Thus, Yokogawa offers consulting services based on plenty of experiences in introducing security measures to systems of various business types and system scales. The services cover areas from supporting users to define their security policies to proposing security measures to be introduced. More details on the content of this section are described in the paper "Consulting Support for Control System Security" in this issue.

Security Engineering

During system integration, the technical controls for each system component determined according to the user's security policies are introduced and integrated while considering security. However, it may cause system shutdowns unless proper engineering is performed considering the requirements and operation conditions specific to the control system. Especially for a large-scale system, optimum managerial controls must be introduced to suppress excessive costs.

Yokogawa has established best practices for control system security measures based on the experience and knowledge in delivering many control systems to users over many years. More details on the content of this section are described in the paper "Security Engineering for Control System" in this issue.

OPERATION AND MAINTENANCE PHASES

In the operation phase, maintenance to keep the security measures effective is required. Even customers who have not introduced security measures can introduce the following measures in this phase.

Endpoint Security Measures

Among the components of a control system, endpoints such as PCs and servers are most likely to suffer from damage by malware infection. To prevent this, security measures for endpoints are crucial. The endpoint security measures are not completed only through their one-time introduction during engineering or operation, but also require periodic updating and maintenance. Yokogawa offers technologies to protect endpoints and a service framework to maintain the effectiveness of the security measures. More details on the content of this section are described in the paper "Endpoint Security for Industrial Control System" in this issue.

Network Monitoring Service

For stable operation of control systems, stable operation of their networks is indispensable. For this purpose, administrators must properly understand the conditions and usages of the network. Yokogawa has developed a network traffic visualization system. This system visualizes the

network traffic without disturbing the control systems, and thus helps operators other than network experts easily understand the communication conditions of the network. More details on the content of this section are described in the paper "A Network Traffic Visualization System for Industrial Control Systems" in this issue.

Vulnerability Handling

In 2014, Yokogawa disclosed that multiple products including the CENTUM integrated production control system had vulnerabilities that threatened the security of the products, and provided patches for them to customers. This is because Yokogawa considered that the security measures for control systems had become a critical requirement of customers, and judged that releasing information to the public and offering the measures were important for achieving customer satisfaction that is inherent to Yokogawa's corporate philosophy. In this way, Yokogawa is making efforts for prompt delivery of accurate information to reduce security risks at customer sites. More details on the content of this section are described in the paper "Yokogawa's Approach to Enhancing Security of its Products and Handling of their Vulnerability" in this issue.

Partnership

Yokogawa concluded a partnership agreement with McAfee, Inc. to provide a comprehensive, high-value-added security solution for control systems. By fusing McAfee's IT security technologies and Yokogawa's control technologies on the basis of this agreement, Yokogawa will offer optimum security measures for control systems.

SECURITY COMPETENCE LABORATORY

To cope with the ever-evolving malware and attacks, the countermeasure technologies must also keep evolving. For this purpose, Yokogawa established the Security Competence Laboratory (SCL) dedicated for security technologies. Its main laboratory is located in Singapore, and others are located in Tokyo, Japan, Bangalore, India, and Dallas, the USA. In the SCL, researchers specializing in security are studying the latest IT security technologies and looking for ways to integrate them into control systems. The research results are summarized as best practices.

CONCLUSION

This paper summarizes Yokogawa's security measures for control systems. In each phase of introducing and operating a control system, security measures are introduced on the basis of the strategies of lifecycle approach and defense in depth. Therefore, security is taken into consideration from the design phase of each component of a control system, and during the engineering phase, security measures based on the knowledge accumulated so far are integrated into control systems. Furthermore, Yokogawa offers various services to keep the security level high at all times.

As already mentioned, security measures are not completed only by one-time introduction. Periodic reviews and renewal as necessary of the measures are crucial for stable operation of control systems. Yokogawa will continue to offer efficient security measures in the future.

REFERENCES

(1) IPA Security Center, A Study on Control System Security of Critical Infrastructures and IT Service Continuation, Information-technology Promotion Agency, Japan, 2009 in Japanese, https://www.ipa.go.jp/files/000013981.pdf
(2) McAfee, Virus information (Stuxnet), Intel Security, http://www.mcafee.com/japan/security/virS.asp?v=Stuxnet
(3) K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82, National Institute of Standards and Technology, 2011, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
(4) Idaho National Laboratory, National SCADA Test Bed Program, INL, http://www4vip.inl.gov/research/national-supervisory-control-and-data-acquisition-test-bed/
(5) Centre for the Protection of National Infrastructure, Supervisory control and data acquisition (SCADA), CPNI, https://www.cpni.gov.uk/advice/cyber/scada/
(6) Netherlands Organization for Applied Scientific Research, Critical infrastructure protection, TNO, https://www.tno.nl/en/focus-area/defence-safety-security/cyber-security-resilience/critical-infrastructure-protection/