Consulting Support for Control System Security

Gen Kinoshita [*1] *Yasuhiro Niii* [*1]

As the number of cyber crimes soars globally, the number of security incidents involving control systems is also increasing. This is because control systems are shifting from their original technologies to general-purpose commercial IT. This imposes the same security risk on control systems as on information systems.

As a security countermeasure for control systems, Yokogawa recommends the "defense in depth" strategy, which is achieved by a best mix of measures in technology, management, and operation. Appropriate security policies are key to the implementation of this strategy. By offering consultation based on knowledge obtained through a wealth of experience in supplying control systems and developing international standards, Yokogawa helps control system users establish security policies with the best approach.

This paper introduces both how to draw up security policies and Yokogawa's security consulting services.

INTRODUCTION

Nowadays, as the threat to security of control systems grows, users' awareness of security risk is increasing. However, it is not easy for users to design and implement security measures by themselves. Many users ask Yokogawa to examine measures for strengthening the security of their systems at each of their plants.

Such requests are based on customers' reliance on Yokogawa's activities as follows. Yokogawa has set up laboratories specializing in security to verify the latest threats and vulnerabilities, and is developing leading-edge security measures for control systems. Yokogawa has been contributing for many years to formulating the IEC/ISA international standards for control system security. In addition, Yokogawa has accumulated best practices for security refined by leading worldwide users, and has established the foundations able to respond to users' needs. On the basis of these results, Yokogawa has launched consulting services for developing a view of security policy and measures as a part of the consulting menu for control system security to achieve safe and secure system operation.

In addition to preparing protective measures against known threats, it is essential to prepare measures to quickly detect, respond to, and recover from unexpected incidents.

For this purpose, "a way of thinking" as security policy must be established first, and then measures based on the policy must be introduced.

SECURITY ISSUES IN CONTROL SYSTEMS

Conventionally, control systems adopted their own original OS and communication protocol, and a dedicated closed network. However, to satisfy market requirements including efficient operation, quick business decision and cost reduction, control systems in recent years are applying a general-purpose OS such as Windows, UNIX or Linux, and applying an open network based on TCP/IP protocol.

As a result, control systems are facing the same security risks as information systems. This means that the safety myth of control systems depending on a configuration using closed networks has now disappeared.

Even though control systems use general-purpose technologies, the same security measures as for information systems, including introduction of the information security management system (ISMS), cannot be applied to control systems. This is because, unlike information systems, control systems need to operate 24 hours a day, 365 days a year, and thus their availability is regarded as important. Accordingly, such measures for security incidents as isolation, interruption and shutdown usually taken in information systems are not suitable for control systems.

In addition, security measures requiring system shutdown such as applying OS security patches cannot be easily taken. The renovation interval of an information system is usually 3

[*1] Consulting Dept.2, Solution Business Division,
Yokogawa Solution Service Corporation

to 5 years, while that of a control system is 10 to 20 years [1]. Control systems are sometimes obliged to use the OSs for which vendor support is terminated, and they need to be continuously operated with vulnerabilities included in them.

On the premise of the availability of prioritized operation, approaches different from information systems must be considered for control systems.

When examining a security policy peculiar to control systems and introduction of measures according to the policy, ensuring staff responsible for security and establishing an executive organization are also issues to be resolved. For this purpose, a certain amount of management resources and support by top management are necessary.

Identifying security risks peculiar to each user's company is another issue. Of course, it is necessary to prepare measures for them.

Yokogawa offers the consulting services for developing a view of security policy and measures, in which optimum approaches and measures for these issues are sought from the users' viewpoint.

CONSULTING AND SUPPORT SERVICES FOR SECURITY

To resolve the issues described above, it is important to establish the security policy first. For establishing the security policy, a basic security policy, i.e., a company-wide policy on security, and functional security policies, i.e., organization-specific policies, are developed first. Then, functional security management standards, standard operating procedures (SOP), and system design documents are prepared in accordance with the basic and functional security policies. In this section, Yokogawa's security services through consulting are explained focusing on the procedure for drawing up the security policy most important while considering security.

Prerequisite Security Policy

The security policy, which the consulting services support to draw up, consists of four layers as shown in Figure 1.

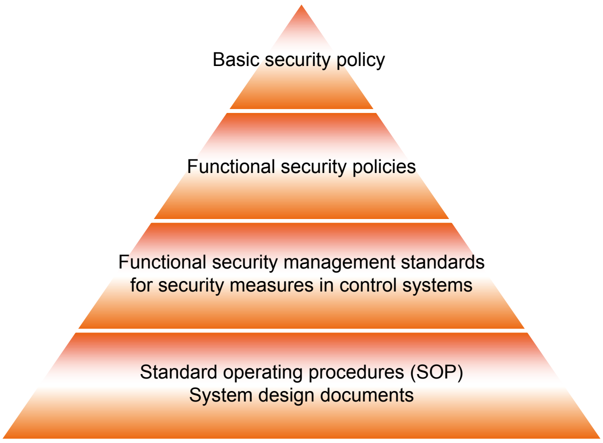
Basic security policy
Functional security policies
Functional security management standards for security measures in control systems
Standard operating procedures (SOP)
System design documents

Figure 1 Security policy

1) Basic security policy

This highest-level policy, which is often included in corporate management principles and business plans, is a basic concept for ensuring security in control systems. This aims for the whole organization to act on a unified philosophy, and defines a corporate principle on security on the basis of a consensus with the top management.

2) Functional security policies

These policies are prepared for each system, equipment or production line in accordance with the basic security policy. Each system, equipment or production line requires its own policy.

3) Functional security management standards

For security measures in control systems, these standards define interpretations and approaches of each functional security policy based on the basic security policy.

Specific activities for the security measures and design standards regarding security in the systems and networks must be defined in the functional security management standards. These standards need to be determined so that users can maintain the security level set by them.

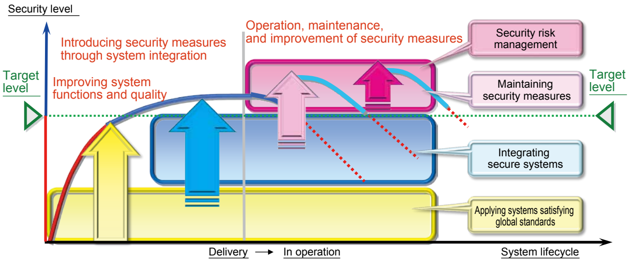
Security level
Target level
Introducing security measures through system integration
Improving system functions and quality
Operation, maintenance, and improvement of security measures
Security risk management
Maintaining security measures
Target level
Integrating secure systems
Applying systems satisfying global standards
Delivery → In operation
System lifecycle

Figure 2 System lifecycle and its security level

Figure 2 shows the relation between the system lifecycle and the security level to be maintained through users' measures.

As shown in the figure, implementing measures once cannot maintain the security level. Even if the security level is secured at the time of system introduction or renewal, continuous improvement such as by maintaining security risk management and security measures is required, because the system will become obsolete over time due to environmental changes [1]. In addition to the policy and measures for maintaining the security level, the management framework and roles of the persons concerned to practice each measure must be defined in these standards.

4) Operating procedures and system design documents

In order to practice measures in accordance with the defined security level, to operate systems after introducing measures, and to perform security design for the system to which measures are applied, it is important to finally break down the functional security management standards into operating procedures and system design documents.

Yokogawa calls the set of items (1) through (4) the security policy.

Consulting Activity

The consulting services for developing a view of the security policy and measures consists of the five steps as shown in Figure 3 so that users can select any combination of steps depending on their security status.

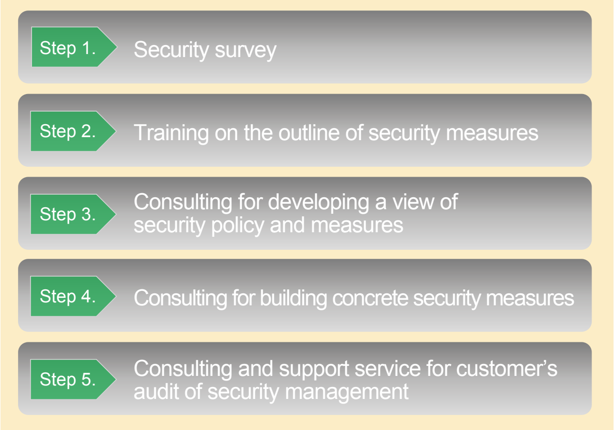
Step 1.
Security survey
Step 2.
Training on the outline of security measures
Step 3.
Consulting for developing a view of security policy and measures
Step 4.
Consulting for building concrete security measures
Step 5.
Consulting and support service for customer's audit of security management

Figure 3 Consulting procedure

1) Step 1: Security survey

A feasibility study is conducted to survey the current security status of users by using an original questionnaire in terms of three aspects: aspects of preventive measures against security incidents, mitigation measures to minimize the impact caused by security incidents, and recovery measures in case of system stop due to a serious impact. This helps users understand the current situation of security including security ensured by physical means, security in organization and personnel and security status from the viewpoint of technology, management and operation.

2) Step 2: Training on the outline of security measures

Yokogawa provides customers with a security manual that summarizes Yokogawa's best practices and basic concept of the security measures in control systems. Customers can learn the concept of those security measures by themselves. Lectures are held as required.

These two steps have the purpose of helping customers identify issues in their current security environment and understand the concept of the security measures in control systems.

3) Step 3: Consulting for developing a view of security policy and measures

Yokogawa helps customers to draw up their own security policy. The scope of the support includes the basic security policy, functional security policies, and approaches in the functional security management standards in Figure 1.

During the consulting, Yokogawa gives customers objective advice on their examining policies and countermeasure plan under investigation from the viewpoint of effectiveness, consistency and exhaustiveness.

The first stage of this step is risk assessment. Potential risks are listed considering feasible growing threats, asset value and negative impact on business such as losing business opportunities, degradation of brand power and incidents causing social problems. Then these listed risks are categorized into those in physical system structure, personnel, networks, individual systems, business continuity and others and are assessed in terms of prevention, mitigation, and recovery aspects as in Step 1.

After the assessment, the identified risks are prioritized, and the corresponding functional security policies and functional security management standards are summarized mainly by customers. Yokogawa gives customers advice on the customers' examination process and its results, and then the policies and standards are finally decided under the agreement among persons involved. Then, customers proceed with documentation of their official security policy.

For consulting deliverables, Yokogawa provides an activity report that summarizes the content and results during investigation and discussion on the functional security policies and functional management standards on the basis of the risk assessment.

4) Step 4: Consulting for building concrete security measures

Security measures are introduced based on the decided security policy. For deciding security settings for systems provided by Yokogawa, and for introducing functions to enhance security in networks and endpoints such as server and client PCs, Yokogawa helps customers draw up security requirement specifications.

5) Step 5: Consulting and support service for customers' audit of security management

Yokogawa offers consulting services supporting customers' internal audits.

Before starting security management operation, training based on the documents and procedures describing the security policy are given to staff in responsible organizations, and their responsibilities are assigned. In the operational phase, internal audit is conducted to properly monitor whether the defined security level is maintained and whether the organization can respond to external environmental changes.

Prior to customers' internal audits, Yokogawa analyzes their daily incidents, disclosed vulnerability information and best practices in the industry. On the basis of these results, Yokogawa supports customers' internal audits through consulting, so it can contribute to their effective risk assessment and the improvement in their security policies and procedures.

CONSULTING FOR ESTABLISHING CSMS

The cyber security management system (CSMS) certification program for industrial automation and control systems was established in April 2014, led by the Ministry of Economy, Trade, and Industry. This program certifies organizational management in the development and operation processes of control systems in accordance with the IEC62443-2-1 international standard.

Simply stated, CSMS is a management system for control systems as ISMS for OA information systems. Yokogawa obtained the world's first CSMS certification for its DCS engineering.

Yokogawa has acquired the world's first CSMS certification for its DCS engineering. One of the reasons why Yokogawa aimed to get this certification is to ensure social credibility in that the company is providing control systems with high-level security.

Another reason is to assist customers' CSMS introduction. Yokogawa helps control system users understand the CSMS through the experience in acquiring the certification, and assists their introduction to the environment for continuously maintaining their security level, that is, their introduction of a cyber-security management system. Customers can proceed with establishing security measures for their control systems by building a CSMS. Meanwhile, Yokogawa will accelerate the expansion of the CSMS through its consulting.

CONCLUSION

Yokogawa proposes a concept called security lifecycle based on the defense-in-depth strategy, in which system operation and measures for security are continuously improved in terms of prevention, mitigation, and recovery aspects. Yokogawa offers products, engineering, and services in accordance with this concept.

Yokogawa believes that users can achieve safe and secure plant operation by establishing the cyber-security management system based on the security lifecycle, cooperating with Yokogawa, offering and constructing control systems, and improving themselves through friendly rivalry. Yokogawa strives to do its best every day.

REFERENCES

(1) ARC Advisory Group, ARC White Paper: Yokogawa's Comprehensive Lifecycle Approach to Process Control System Cyber-Security, 2011, https://www.yokogawa.com/nl/iab/pdf/vigilantplant/iab-arc-scrty-en.pdf