Evolution of Control Platform

Security Measures for Production Control Systems

Masahiro Hashiguchi [*1] *Katsuhiro Takamatsu* [*1]

Many companies and organizations have introduced information technology (IT) to improve the efficiency of operations and to centralize high-density information into their information system. As a result, they need to take thorough measures to ensure the security of the information system. Production control systems also need similar security measures because they closely work together with the information system, but existing measures are not enough. This report describes the importance of security measures for production control systems, methods to check for potential threats and analyze vulnerabilities of the system, and other security measures in the IT environment.

INTRODUCTION

To improve the efficiency of operations, production control systems are working together more closely with information systems. As a result, security measures have become indispensable for production control systems though they have not been emphasized to date. Because many production control systems are used for critical infrastructure, some malware tries to attack them.

Security measures for production control systems, however, have hardly been introduced. This is because production control systems have used dedicated hardware, software, and protocols. However, such systems have recently been exposed to security threats as they introduce general-purpose technologies.

Security measures must be implemented from the viewpoint of the system. From this standpoint, Yokogawa identifies potential threats to customers' production control systems, analyzes their vulnerabilities, and proposes security measures. This paper describes these security measures. In addition, this paper outlines the security measures in the IT environment included in those security measures, and introduces tools to strengthen the security in the IT environment.

*1 Planning & Open Control Systems Development & Engineering Dept., Industrial Automation Systems Business Headquarters

NECESSITY OF SECURITY IN PRODUCTION CONTROL SYSTEMS

Cooperation with information systems and increase in security threats

The information system receives the benefits of general-purpose OSs (e.g., Windows, Linux) and the Internet, but is long exposed to security threats. Therefore, security measures have been introduced for this system. As it works closely together with the information system, the production control system also needs security measures.

Key infrastructure and production control systems

The production control system, which has thus become exposed to security threats, often serves as a key system of companies or society, such as a product manufacturing system or a system for critical infrastructure for electric power, water supply, sewerage, oil, or natural gas. If a production control system stops, it may have a big impact on society. Therefore, the system is protected by two kinds of security measures: one to prevent it from stopping and the other when it stops. These are described in the "Investigation of security measures" section.

Difference between production control systems and information systems

Comparing the production control system with the information system, they have some differences in assets to be protected, system environment, and system interface. The largest difference is the seriousness of damage in case of an incident. If the production control system fails, it may directly affect the human body, life, society, environment, etc. and cause serious damage. This is why tougher security measures are required for the production control system than for the information system.

TREND IN CYBER ATTACKS ON PRODUCTION CONTROL SYSTEMS AND AN EXAMPLE

Change in cyber attacks

Cyber attacks have changed from indiscriminate attacks to targeted attacks on specific users. The purpose of targeted attacks is to attack the system of a specific organization or business category and to exploit its protected assets or disrupt its operation. According to a report by the Ministry of Economy, Trade and Industry, Japan, the proportion of companies that experienced targeted cyber attacks increased to 33% in 2011, from 5.4% in 2007 [(1)].

The structure of malware used for targeted cyber attacks has also evolved. The old type was often a means for the creator to show off his knowledge or skills, thus most malware was relatively simple. However, recent malware is large-scale and elaborate designed to effectively attack a specific system.

Stuxnet

Stuxnet, which is one malware for targeted cyber attacks, was discovered in June 2010. This advanced malware exploits the vulnerability of both Windows and the software of a specific SCADA vendor.

According to a report by the Information-technology Promotion Agency, Japan, an independent administrative institution, Stuxnet is 500 Kbytes or more in size, which means that it is larger and more complex than any previous one [(2)].

The most notable fact about Stuxnet is that it was developed to attack a specific production control system and it succeeded in damaging some facilities [(3)].

THE CONCEPT OF YOKOGAWA'S SECURITY MEASURES FOR PRODUCTION CONTROL SYSTEMS

This chapter describes the concept of Yokogawa's security measures.

Identification of potential threats

Potential threats to systems are identified by the following procedures. First, assets to be protected are specified and then their potential threats are identified in consideration of the system environment and interface.

a) Assets to be protected

Assets to be protected are something to be protected in the system. Generally, they include customer information, order information, shipping information, confidential information about organizations and individuals, and system parameters (e.g., recipe information). Intangible assets such as those for operation and safety are also included.

b) System environment

In terms of security measures, vulnerability differs depending on the system environment, including the following items.

- Operation environment: general clerical workplace, access-controlled area, data center
- OS: general-purpose OS, dedicated OS
- Communications: Internet, private network (VPN), intranet
- Human resources: temporary worker, regular employee with security knowledge

c) System interface

In terms of security measures, vulnerability differs depending on the system interface with the outside including the following items.

- Communication protocol: DCOM, HTTP, RPC, Vnet (or Vnet/IP), FOUNDATION fieldbus™ Note 1)
- Functions that can be operated through the user interface
- File types that can be referred to or modified through the file interface: log file, configuration file
- Devices connected via the sensor controller interface: sensors, actuators, etc.

Considering the system environment and interface, possible potential threats to the assets to be protected are as follows.

- Leakage of customer or recipe information to other companies
- Information leakage or operation shutdown due to unauthorized access through remote access functions
- Operation shutdown due to falsification of order or recipe information
- System down or leakage of confidential information caused by malware

Vulnerability analysis

The vulnerability analysis analyzes the vulnerability of the system to the identified potential threats. As an example, consider the possibility of leakage of customer and recipe information to other companies. If the system allows any person to view and copy recipe information, this is recognized as vulnerability in the system and security measures are required against it.

Meanwhile, the vulnerability analysis sometimes reveals that a potential threat is not a real menace. For example, information leakage or shutdown due to unauthorized access

Note 1) Fieldbus communications protocol proposed by the Fieldbus Foundation™

through remote access functions seems to be a real threat. In actual operation, however, remote access requires a special device that is accessible to only a limited number of people. Therefore, the feasibility of this threat is negligible.

Investigation of security measures

After the vulnerability analysis for assets to be protected is completed, security measures against the vulnerability of the system are listed. Although the system can be secured with all these measures, adopting all of them is not realistic because of various constraints on operation and costs. Therefore, customers should select security measures by weighing the operation and costs.

Meanwhile, some production control systems serve as systems for critical infrastructure for electric power, water supply, sewerage, oil, or natural gas, etc. If they stop, it would seriously affect the human body, life, society, environment, etc. Therefore, systems for critical infrastructure require security measures to prevent them from stopping and those to minimize damages in case they stop. The former type of measure can secure availability by preventing unnecessary packets from entering the system even when it receives DoS Note 2) /DDoS Note 3) attacks. The latter type of measure can minimize an infection by malware by dividing the network of the system into multiple segments even when part of the system is infected by malware.

Determination of security measures

When determining security measures, we should examine the balance of three elements: confidentiality, integrity, and availability (CIA) [4]. Table 1 shows an example of potential threats and security measures in terms of CIA.

Means for security measures

When investigating specific means for measures determined in the previous section, there may be several means available. For example, against the threat of leakage of customer or recipe information to other companies, effective security measures may include appropriate authorization based on an access control list (ACL-based authorization), or data protection. The ACL-based authorization can be achieved not only by programming but also by using ACL-based authorization provided by the OS. Thus, roughly categorizing, there are three types of security measures available.

- Security measure by incorporating functions into products
  With this type of security measure, security is secured by incorporating functions for security measures into products. This includes a function to require authorization by two or more persons for an important operation. This is advantageous in terms of security strength because it incorporates the security function into products. However, it may cause problems in development costs or responsiveness of the development.
- Security measure by using IT environment
  With this type of security measure, security is secured by the IT environment where products operate. For example, the ACL-based authorization provided by a general-purpose OS can be used to prevent unauthorized persons from referring to or modifying operation data. Compared with the security function incorporated in products, its introduction cost is lower and its flexibility is higher, but its security strength is often insufficient because of its high versatility.
- Security measure by operation control
  With this type of security measure, security is secured by controlling operation of the system. This includes defining an operation rule to change the password periodically. Compared with the type by incorporating functions in products and by IT environment, its introduction cost is lower, but its strictness is lower and it increases the burden on operators.

Table 1 Potential threats and security measures in terms of CIA

Potential threats		Security measures
Confidentiality	Leakage of customer or recipe information to other companies	Appropriate ACL-based authorization, and data protection (e.g., by encryption or signature)
	Information leakage and operation shutdown due to unauthorized access through remote access functions	Appropriate ACL-based authorization, and protection of communications data
Integrity	Operation shutdown due to falsification of order or recipe information	Appropriate ACL-based authorization, and protection of data
Availability	Operation shutdown due to DoS/DDoS attacks	Prevention of inflow of unnecessary packets (Firewall/L3SW *1) and making communication protocols robust
	System down and leakage of confidential information due to malware	Measures using software for security measures (antivirus software)
		Divide the network of the system into multiple segments to minimize infection by malware

*1: Layer 3 Switch

Changing threats

Threats to the system change as the system environment changes or new vulnerabilities in the system interface are discovered. Therefore, the results of identification of potential threats, vulnerability analysis, investigation of security measures, determination of security measures and means for security measures, described in earlier sections, must be periodically reviewed.

Note 2) Denial of Service attack
Note 3) Distributed Denial of Service attack

Security standards for determining security measures

The vulnerability analysis must be carried out extensively to determine security measures. It is effective to refer to NIST SP800-82 [5], etc.

SECURITY MEASURES IN IT ENVIRONMENT

As described above, there are three types of security measures for the system product: security measure by incorporating functions into products, by using the IT environment, and by operation control. This section introduces security measures using the IT environment (hereafter referred to as "IT security"), which were released in September 2011 for common use among Yokogawa's system products.

Features of IT security

IT security for the system products of Yokogawa is a measure to enhance the security strength of the Windows PC environment, where the software of the system products run, by using the security function of Windows (hereafter this enhancement is referred to as "hardening"). The major feature of this measure is automatic hardening of the PC by a tool (hereafter this tool is referred to as "IT security tool"). Because hardening of the PC can be carried out with the IT security tool, it is possible to reduce the engineering man-hours and human errors caused by manual work, thus preventing the creation of new vulnerabilities.

Features of IT security tool

The IT security tool has the following features.

a) Basic policy of All-deny

After making the PC as robust as possible, the IT security tool allows access control settings required for each product. As a result, it can reduce the omission of security settings. Figure 1 is a conceptual diagram of this setting scheme.

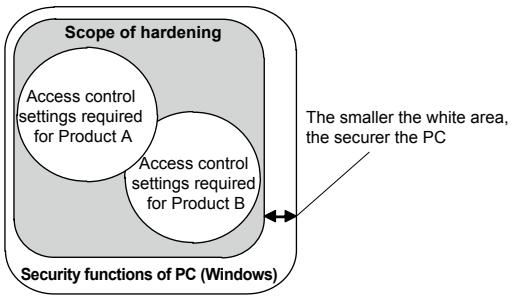

Figure 1 Conceptual diagram of IT security setting

b) Reduction of setting work during system configuration

Automatic hardening of the PC with the IT security tool can reduce the engineering man-hours. Even when Yokogawa's system products exist or work together in the same PC, additional settings for one system product do not affect the operation of another product. Figure 2 is a conceptual diagram of the setting flow.

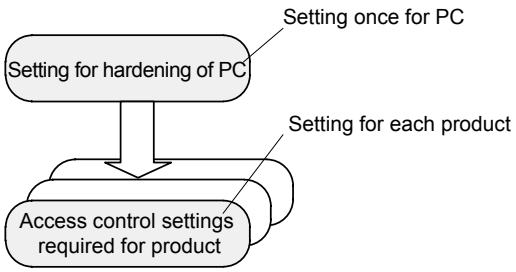

Figure 2 Conceptual diagram of setting flow

Hardening of PC

Hardening of the PC is a technique to enhance security strength by reducing the vulnerability within the PC. The major items for the hardening supported by IT security are as follows.

- File access control
- Registry access control
- COM/DCOM access control
- Setting of Windows Firewall

(total 11 items including others)

CONCLUSION

This paper has clarified the difference between the production control system and the information system, and described the tactics used to attack them. Then it proposed procedures for identifying potential threats, analyzing vulnerabilities, and implementing security measures. It also outlined security measures by the IT environment and introduced the functions of the IT security tool.

Yokogawa, as a solution supplier of production control systems, has been providing security measures from the viewpoint of the system. Taking its system products as a core product for the solution, Yokogawa will continue to provide security measures from the viewpoint of the system.

REFERENCES

(1) Information security policy room, "Announcement and implementation of information security measures based on recent trends," Ministry of Economy, Trade and Industry, Japan, 2011
(2) "Report on new types of attack," IPA Technical Watch, Information-technology Promotion Agency, Japan, 2010
(3) William J. Broad, John Markoff, David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," The New York Times, January 15, 2011
(4) ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security management, 2005
(5) NIST SP800-82, Guide to Industrial Control Systems (ICS) security, 2011