Control System Security Anticipating the Coming Age of IoT

UNO Tohei, SUGIURA Masashi

Abstract

The target of information communication technology (ICT) has now gone beyond the boundaries of corporate information systems and is currently widespread and covering many sectors, which includes business platforms for production and services as well as for social infrastructures. Recently the use of control system has become more and more significant. However, those particularly in the private sector and also the security measures of factories or plants do still tend to be inadequate. Based on interviews with company personnel this paper attempts to explain the background to the importance of security measures, the characteristics of control systems, issues related to security measures and the orientation of such measures.

Keywords

control system, cyber security, CSMS, EDSA, SDN.

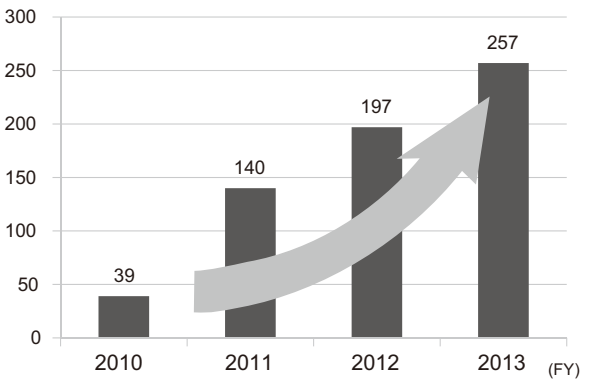
1. Introduction

The computerization of society has caused the information communication technology (ICT) to go beyond the office boundaries of the use of business systems and of information systems. IT is now disseminated throughout wider fields, such as being embedded in factories and in products, as well as in homes and general social infrastructures. Significant benefit is thereby provided in these sectors by achieving improved convenience and efficiency. On the other hand, malicious cyberattacks and misuse/abuse by internet users are increasing threat risks to the protection of information and assets and the safety/security of satisfactory business continuity and on society in general.

Although the security measures applied to corporate information systems and communications networks continue to attract keen attention, those for the control systems supporting business operations do still tend to be inadequate. In this paper, our discussions will focus on the present and future measures adopted by companies for their control systems.

2. Background to the Need for Control System Security

Since the malware cyberattack known as Stuxnet on the Iranian nuclear facilities in 2010, cyberattacks abroad have been increasing, particularly at energy plants and key equipment manufacturing sites (**Fig. 1**). Two kinds of malware were additionally found in 2014 as the signs of a further increase



FY:Fiscal Year (1st October to 30th September)
* Compiled based on "Year in Review 2012" and "Year in Review 2013" by ICS-CERT.

Fig. 1 Number of cyber incidents dealt with by U.S. ISC CERT.

in attacks became evident. For example; the control system of an American automobile factory was infected by a virus from a PC brought in from outside and the production line was stopped causing damage assessed at 1.7 billion yen, an oil pipeline was exposed to a cyberattack and a German steel plant was infected by malware and was consequently unable to stop the furnace in the normal manner, which led to significant damage due to equipment failure. Similar incidents also occurred in Japan. According to the control system vulnerability information reported to the Information-technology Promotion Agency (IPA), serious threats are on the increase such as that the entire systems was overtaken by malicious cyberattack from remote locations, or other serious threats such as leakage of large amounts of system information (**Fig. 2**).

In the following, we will discuss how companies consider the impact of increases in security incidents related to control systems and what measures they intend to take, based on fieldwork survey reports including hearing surveys.

Three types of background can be listed that indicate the security of control systems is gathering importance.

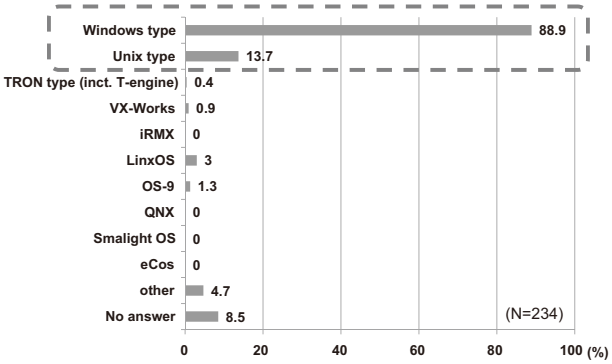
Firstly, because of the overseas deployment of such information under the accelerated globalization of business due to M&A and other causes, it is more and more recognized as a critical issue that the risk of confidential information leaks, such as operational know-how, procedures and design information is increasing.

Secondly, it is also recognized as an important issue that information security incidents run the risk of threatening social infrastructures, plant safety and environmental conservation. In the Japanese Basic Act on Cyber Security enacted in November 2014, the Japanese Government assumed leadership against such threats by identifying 13 major businesses that are critical in supporting the social infrastructures, and extensive damage could be inflicted on social environments if such enterprises are adversely affected by security incidents. The government advises industries to adopt suitable countermeasures by establishing security-related safety standards, and requests submissions of incident reports and the sharing of related information.

As stated above, an environment for adopting cyber security measures in close collaboration between the government and private sectors is currently being created in Japan. Unlike the conventional security measures of the past, the recent cyber security measures involve management issues such as business stability and social responsibility.

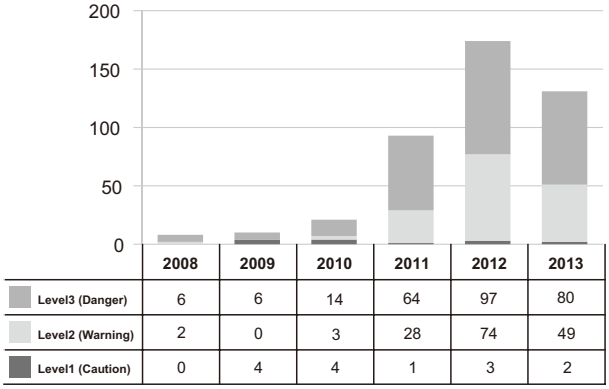
The third type is the background of the control system itself. This concerns the accelerated opening and networking of factories and plants. So far, it has often been said, "a factory is composed of proprietary technologies and protocols of system vendors so that the security risk is small. It is safe because it is not subject to external influences."

Fig. 3 shows the result of a 2009 survey by the Japanese Ministry of Economy, Trade and Industry, showing that about 90% of plant facilities utilize general-purpose OSs. **Fig. 4** displays results of the same survey, showing that about 40% of plant facilities have external connections. The same survey



* Compiled based on "Report on Actual Status Survey of Threats Caused by Application of Universal IT on Industrial Systems and Countermeasures Against Them (March 2019)" of Japanese Ministry of Economy, Trade and Industry.

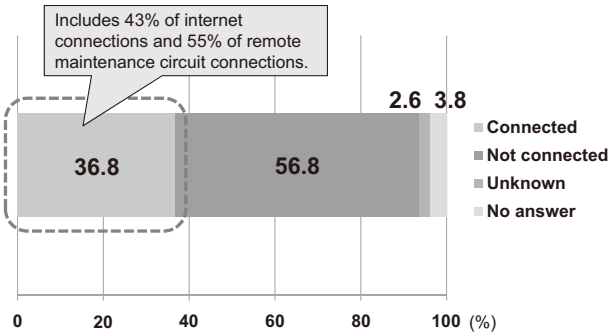
Fig. 3 Utilization of OSs in plant maintenance (number of terminals).



	2008	2009	2010	2011	2012	2013
Level3 (Danger)	6	6	14	64	97	80
Level2 (Warning)	2	0	3	28	74	49
Level1 (Caution)	0	4	4	1	3	2

* Compiled based on "Vulnerability Countermeasures Information Database JVN iPedia Registration Status [2013 4th Quarter (Oct. – Dec.)]"

Fig. 2 Breakdown of the degrees of seriousness of vulnerability of industrial control system software.



* Compiled based on "Report on Actual Status Survey of Threats Caused by Application of Universal IT on Industrial Systems and Countermeasures Against Them (March 2019)" of Japanese Ministry of Economy, Trade and Industry.

Fig. 4 Connection to external networks.

also indicates that 70% of plant facilities use USB devices for data input/output and maintenance.

More recently, the global factory concept and networking are required to deal with fresh business needs. Such new businesses have emerged from the concepts of "process innovation" and "product innovation" that are based on wireless LAN, tablet terminals, Industry 4.0 and Industrial IoT.

3. Control System Characteristics

In this section, we will review the representative characteristics of the control systems and consider the issues related to control system security.

Fig. 5 shows a diagram of a typical control system configuration.

Separate to the office network, there are three network layers; these are the control information network, the control system network and the field network.

We define the area enclosed by broken lines in the figure as the control system and enumerate their characteristics as follows:

- **Systems emphasizing availability**
  With priority on real-time control operations, this kind of system is simple and few of such systems adopt security measures. In addition, in order to eliminate effects on the control operations these systems are rarely updated by means of patching, etc.
- **Systems emphasizing connectability**
  As this kind of system is connected to various field devices, such systems often use interfaces and protocols that are open to the public.
- **Long service period**
  Because the system is used for 10 or 20 years, there are not a few cases in which no longer supported OSs and applications are often embedded and continue to run.
- **High vendor dependency**
  This kind of system puts priority on availability, and such systems often rely on the control system vendors for their maintenance, administration and maintenance.
- **Role allotment in organizations**
  The role allotment most often applied is to let the IT systems department manage the parts of the control system network, shown above Fig. 5 and let the engineering or production technology department manage those shown below. The most frequent outcome of this arrangement is an inadequacy of collaborations from the viewpoint of information security or a lack of human resources that are capable of understanding both the information and the control systems.

Based on the above, we may say that the control systems feature very high vulnerability and security risks because they are subjected to open networking while the security measures

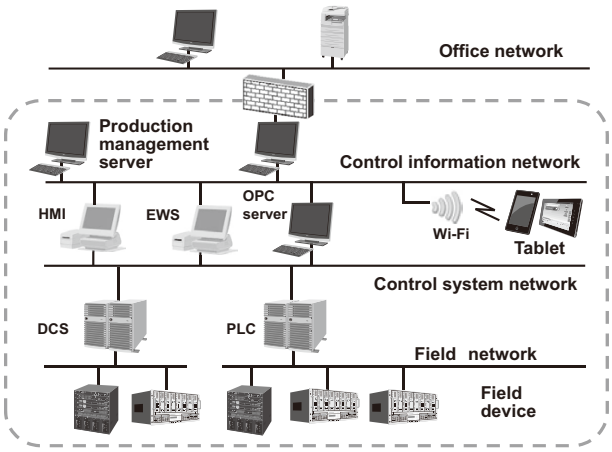


Fig. 5 Control system configuration diagram.

for systems are either not taken or are not possible to be taken. Consequently, the following three issues become the main ones that are related to the control system security.

(1) Fostering an information security consciousness against the control system
(2) Introduction of measures and actions according to the control system characteristics
(3) Measures collaborated with the suppliers.

4. Proposals of Control System Security Measures

In this section, we propose the possible measures to be adopted against the three issues enumerated in section 3.

4.1 Fostering Consciousness of Information Security of Control System

A framework of what should be done regarding control system security is given by the CSMS (Cyber Security Management System) based on the IEC62443-2 international standard, which is the control system version of the ISMS (Information Security Management System) for the security of information systems. Whether or not individual systems are certified by the management assessment of the CSMS, it is still beneficial that management takes appropriate measures by using the requirements of the assessment as a reference.

4.2 Introduction of Solutions according to the Characteristics of Each Control System

- **Segmentation of networks**
  Segmentation of networks according to the security level makes it possible to prevent invasion and expansion of malware and improve the security of the environment in which terminals are used even after the expiration of their support periods. Specifically, it is essential to divide

the office network and control networks with a firewall, or the like to ensure security by adopting the SDN (Software-Defined Networking) technology. Consequently, the network security can be assured by re-routing them to a securer network even if any unsupported terminal is connected to a network or if a packet that displays suspicious behavior is received.

- **Introduction of individual authentication management**

  Since individuals engaged in work in a factory or plant have high mobility and are not limited to being corporate employees, it is difficult to apply individual authentication by ID or password. In such cases, it is possible to adopt composite countermeasures to ensure both physical and cyber security.

  These countermeasures include for example enablement of control system operations exclusively for offices under surveillance or to authenticate individuals by means of face recognition by a monitoring camera. It is also possible to combine the individual authentication and the SDN described above in order to effectively limit the networks each individual can access.

Other suitable security measures for the office domain, such as the white list type application control and the control of devices such as USB devices may also be utilized fully.

4.3 Measures Collaborated with Suppliers

For information systems, it is a widely adopted practice to define the security requirements as nonfunctional requirements at the time of procurement and operation. For the control systems, too, the need to define the requirements for secure development and operation is increasing. In relation to the CSMS conformity assessment, there is another product assessment system called the EDSA (Embedded Device Security Assurance). Its framework is also applicable for checking the security function of the control system to be introduced.

5. Conclusion

A significant majority of enterprises now recognize the importance of control system security and tend to feel that the currently adopted countermeasures are inadequate. The management of control systems and factories is extremely challenging because it cannot be separated from the global security management that inevitably involves overseas subsidiaries.

We feel strongly that the information system (IS) departments must make use of their expertise in order to lead the field from a standpoint that is close to management. This will be achieved by transcending the boundaries that exist between the office and factory and the parent enterprise and group companies as well as those that afflict the relationships of various countries.

Authors' Profiles

UNO Tohei
Senior Manager
Consulting Business Division

SUGIURA Masashi
Senior Expert
Cyber Security Strategy Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.10 No.1 Special Issue on Enterprise Solutions to Support a Safe, Secure and Comfortable Life
- Value Chain Innovation Linking "MAKE," "CARRY" and "SELL" -

Vol.10 No.1
December, 2015

Special Issue TOP