Featured Articles

Trends and Developments in Security Standards for Secure Social Infrastructure Systems

Tsutomu Yamada
Tadashi Kaji, Dr. Info.
Toshihiko Nakano, Ph.D.

OVERVIEW: Consolidation of standards suitable for control systems is an urgent task that must be accomplished if control system security is to be improved. When it comes to control system security standards, the consolidation of industry standards is happening more quickly, but international standards are also being formulated with four out of the 13 documents of the IEC 62443 series of standards already published. Also, ISASecure EDSA and CSMS certification are standards for certifying conformance with security rules by control systems and control devices. The rapid acquisition of international certifications in terms of security is also important from the perspective of strengthening international competitiveness, and the Ministry of Economy, Trade and Industry is implementing a pilot project in order to enable the acquisition of these certifications from inside Japan. Hitachi is contributing to standardization activities aimed at the utilization of these standards.*

INTRODUCTION

GOVERNMENT agencies and industries in various countries are carrying out foundational activities aimed at improving the security of the control systems that support social infrastructures. In the past, on-site information has been utilized in operations and management in order to increase efficiency and productivity in social infrastructures and on factory floors. Also, aimed at increasing both affinity with information systems and development efficiency, information technology (IT) has been incorporated into many control systems, both in terms of operating systems (OS) and the field of network technology. At the same time, the Stuxnet computer virus, which was discovered in 2010, was created targeting specific control systems. This reminded many responsible parties, industries, and government agencies with a connection to control systems about the importance of security.

However, the additional installation of information system security technologies to control systems is often problematic. This is because since only limited computing power is available in controllers and various other types of devices, modifying configurations has a major impact on processing overhead. In general, the availability and integrity of the protected assets are given priority in control systems, and so the confidentiality that is emphasized in information systems has a relatively lower priority. Also, the facilities and external environments must also be protected, including the control devices themselves, in addition to information.

In other words, measures must be suited to the control systems if control system security is to be strengthened. Since control systems are used in countries around the world, it is effective to apply standards that can be evaluated from a shared, international perspective as security countermeasures and guidelines. This is why government agencies from various nations, standards bodies, and industry groups are working to formulate standards and guidelines in the area of control system security.

This article provides a general overview of control system security standards, representative standardization efforts, and trends as well as the current state of various types of certification systems aimed at improving security.

INTERNATIONAL AND INDUSTRY STANDARDS

Overview

When it comes to security standards, the ones in the field of IT are leading the way. For instance,

* ISASecure is a trademark of ASCI.

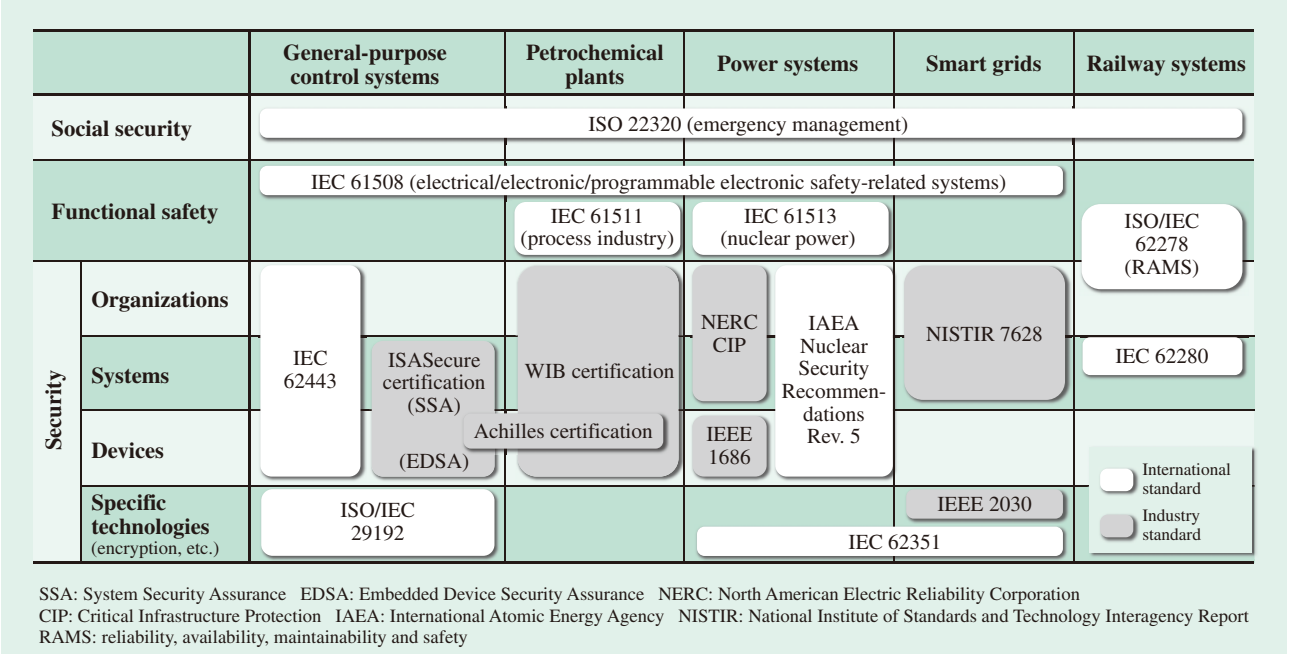

Fig. 1—Overview of Standards Related to Control System Security.
The diagram indicates which standards in each field are international, and which are industry standards.

Common Criteria (ISO/IEC 15408[1]) is utilized in the procurement of security related products. In order to counter the same threats as exist in the IT field, many control system security standards reference physical security standards[2] as well as IT security standards. Of these interrelated standards, this article will focus in particular on trends in control system security standards.

Fig. 1 shows an overview of international and industry standards regarding control system security. The diagram indicates which standards in each field are international, and which are industry standards. In addition to security standards, functional safety standards with a close relationship to the safe operation of control systems are included.

Starting in the 2000s, standards came together comparatively quickly in each industry, in response to the demands of control system user. In the diagram, this would be the ISASecure standard[3], the WIB standard[4], and Achilles certification[5]. In many cases, certification frameworks have also been provided along with the standards. These companies and organizations are in the business of guaranteeing that products that comply with the standards achieve a certain level.

As a related trend, the president of the USA is moving forward with security efforts in the area of countering the threat of cyber-attacks[6]. The National Institute of Standards and Technology (NIST) has also issued a cybersecurity framework[7]. While this framework is not legally binding, it does act as a guideline for ensuring corporate security, and the trend towards treating this guideline as a de facto standard must be noted.

Although they are lagging a bit behind the industry standards, international standards are being launched. At present, work is being done on consolidating the IEC 62443 standards, which address control systems overall. Also, in order to protect the crucial infrastructure of power systems, the US government has prepared the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)[8] as a security standard for the power industry, and the standard has already gone into effect.

Hitachi has established guidelines for the secure construction of control systems based on the specifications demanded by these standards. In order to construct a system whereby continuous security measures are possible, these guidelines are utilized while following the security implementation policy for control systems as described in the featured article “Control System Security for Social Infrastructure” (see p. 277 in this issue).

IEC 62443

IEC 62443 is a series of international standards that is drawing attention. The overall framework is shown in Table 1.

TABLE 1. General Framework of IEC 62443 Standards
The general framework of IEC 62443 standards is provided below.

Standard No.	Standard name	Overview
IEC/TS 62443-1-1 (published)	Terminology, concepts and models	Terms, concepts, and model definitions
IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Terms and abbreviations
IEC 62443-1-3	System security compliance metrics	System safety evaluation criteria
IEC/TR 62443-1-4	IACS security life cycle and use case	IACS security life cycle and use cases
IEC 62443-2-1 (published)	IACS security management system - Requirements	IACS security management system requirements
IEC 62443-2-2	IACS security management system - Implementation guidance	IACS security management system implementation guidelines
IEC/TR 62443-2-3	Patch management in the IACS environment	Guidelines regarding patch management methods for IACS
IEC 62443-2-4	Requirements for IACS solution suppliers	Security practices for IACS equipment vendors
IEC/TR 62443-3-1 (published)	Security technologies for IACS	List of security technologies that can be used in IACS
IEC 62443-3-2	Security levels for zones and conduits	Safety assurance levels for zone and conduit concepts
IEC 62443-3-3 (published)	System security requirements and security assurance levels	System security levels and corresponding function requirements
IEC 62443-4-1	Product development requirements	Component development process rules
IEC 62443-4-2	Technical security requirements for IACS components	Component security function requirements

IACS: Industrial Automation and Control System

IEC 62443 is comprised of a total of 13 documents. The IEC 62443-1-x series comprises general standards, and deals with basic concepts, models, and terminology. The IEC 62443-2-x series is for asset owners, and deals with security policies as well as the systems used to manage organizations and people. The IEC 62443-3-x series is for system integrators, and deals with the technology requirements of control systems. The IEC 62443-4-x series is for equipment vendors, and deals with the security requirements of the control devices that constitute a system.

An overview of the standards in the IEC 62443 series that have already been published is provided below.

(1) IEC/TS 62443-1-1[9]

Stipulates basic security requirements for control systems. The seven requirements are access control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability.

(2) IEC 62443-2-1[10]

Describes risks that the asset owner must manage in systems, and the cybersecurity management system (CSMS).

(3) IEC/TR 62443-3-1[11]

General catalog of security technologies. Describes certification, filtering and access controls, encryption and data certification, managed audit monitoring, software management for personal computers (PC) and other devices, and physical security.

(4) IEC 62443-3-3[12]

Defines four security levels of detailed function requirements for protecting system security according to the seven requirements mentioned above.

Four of the IEC 62443 documents listed in this table have already been published, and the remaining documents are still being formulated at present by the International Electrotechnical Commission (IEC) Technical Committee (TC) 65/Working Group (WG) 10. In order to continuously improve the security of control systems, Hitachi is working with members of the IEC National Committee while contributing to the documentation process.

CERTIFICATION STANDARDS

Clarification of the criteria used to evaluate security coverage and robustness is advisable for asset owners when security is to be adopted for control systems. A security certification framework is an effective way to evaluate security functions. Representative examples of frameworks include ISASecure and CSMS certifications.

ISASecure

The ISA Security Compliance Institute (ISCI)[3] is a subordinate body of the International Society of Automation (ISA)[13] industry group headquartered in the USA. ISASecure is a framework for certifying that the security criteria established by the ISCI are met. The ISCI prepares certification programs for everything that is certified, including Embedded Device Security Assurance (EDSA) certification for control devices, and System Security Assurance (SSA) certification for control systems. Standards have been already been published and certification has begun for EDSA[14], but not yet for SSA.

EDSA certification involves the following three categories of inspection (see Fig. 2):

(1) Communication Robustness Testing (CRT)

Verifies the control device's communication

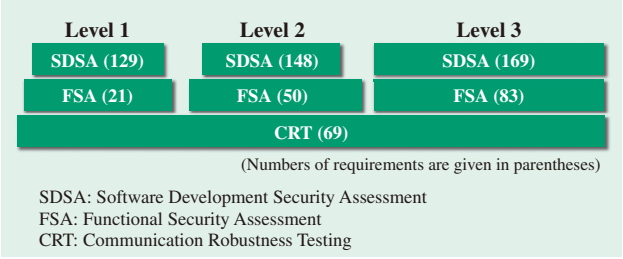

Fig. 2—Numbers of EDSA Certification Requirements. Security test requirements are stipulated based on the certification level to be acquired.

protocols [Ethernet, Address Resolution Protocol (ARP), Internet Protocol (IP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP)]. Specialized tools certified by the ISCI are used to verify normal operation during the protocol inspection.

(2) Functional Security Assessment (FSA)

Verifies the control device's security functions.

(3) Software Development Security Assessment (SDSA)

Verifies the processes used to develop control devices.

With EDSA certification, the CRT uses the same tests at all levels to verify compliance, whereas the FSA and SDSA verifies test items according to the three levels.

CSMS

The CSMS is a management system whereby the asset owner manages risk to a control system while continuously maintaining security. In the case of information systems, this is associated with the control system version of the information security management system (ISMS) established with ISO/IEC 27001. Certification standards are expected to be enacted based on IEC 62443-2-1.

Fig. 3 shows the flowchart for achieving CSMS as illustrated by example in IEC 62343-2-1 Annex B[10]. The achievement of CSMS starts with justifying the CSMS program with the management team [see (1) in the diagram]. Next, threats, probability of realization of threats, vulnerability types, and results are presented [see (2) and (3) in the diagram]. Furthermore, based on the organization's risk tolerance, appropriate policies and organizations are established in order to execute countermeasures [see (4) in the diagram], and countermeasures are selected and adopted [see (5) in the diagram]. After adoption, whether or not the organization conforms with CSMS policies and procedures is verified, as well as effectiveness and the need for any changes in targets [see (6) in the diagram].

CSMS certification involves verifying whether or not the asset owner can implement the flowchart for managing security maintenance.

VARIOUS TRIAL CERTIFICATIONS

From the perspective of strengthening competitiveness, in order to successfully deploy control systems overseas, it is important to rapidly acquire certifications that are accepted internationally. Therefore, the Ministry of Economy, Trade and Industry is leading a pilot project in order to enable the domestic acquisition of the two aforementioned certifications in Japan.

Agencies within Japan already provided a framework for the information system security standards ISMS and ISO/IEC 15408, and the goal is to prepare the same type of framework for control systems as well. The Control System Security Center (CSSC) technological research association is conducting a pilot EDSA certification program. The Japan Information Processing Development Center (JIPDEC) has a pilot certification program for CSMS certification.

Certification criteria and guidelines are being prepared for both EDSA and CSMS certification. Hitachi is cooperating with responsible organizations in the establishment of both types of certification, and provides security solutions for customer systems while applying these standards.

CONCLUSIONS

Establishing security standards for control systems and achieving certification will help raise levels of security even further. Hitachi is contributing to standardization activities in order to develop the infrastructure of security technology.

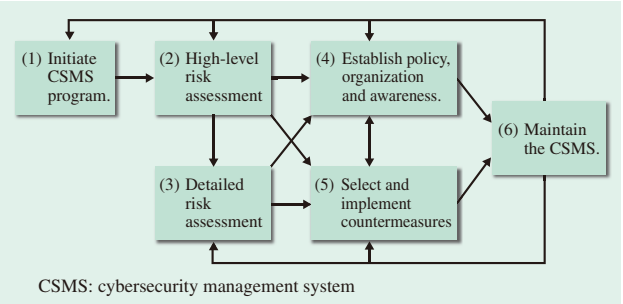

Fig. 3—CSMS Achievement Flowchart. Procedures are stipulated for control system risk assessment and security maintenance management.

Since it will take some time before security in control systems is seen from the perspective of international standards, other measures must also be implemented. To this end, it is important to comply with international and industry standards while at the same time engaging in research and development supporting the latest security technology and providing solutions.

REFERENCES

(1) ISO/IEC, "ISO/IEC 15408, Information Technology—Security Techniques—Evaluation Criteria for IT Security—"
(2) U.S. Department of Defense, DoD Manual 5100.76-M, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives."
(3) ISA Security Compliance Institute, http://www.isasecure.org/
(4) WIB, http://www.wib.nl/
(5) Wurldtech, Wurldtech Certification, http://www.wurldtech.com/product_services/certifications/
(6) President's Council of Advisors on Science and Technology, "Report to the President Immediate Opportunities for Strengthening the Nation's Cybersecurity" (Nov. 2013).
(7) NIST, "Framework for Improving Critical Infrastructure Cybersecurity" (Feb. 2014).
(8) NERC, CIP Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
(9) IEC: IEC/TS 62443-1-1, "Terminology, Concepts and Models" (July 2009).
(10) IEC: IEC 62443-2-1, "Establishing an Industrial Automation and Control System Security Program" (Nov. 2010).
(11) IEC: IEC/TR 62443-3-1, "Security Technologies for Industrial Automation and Control Systems" (July 2009).
(12) IEC: IEC 62443-3-3, "System Security Requirements and Security Levels" (Aug. 2013).
(13) ISA, http://www.isa.org/
(14) ISCI, "ISASecure Program Description," http://www.isasecure.org/ISASecure-Program.aspx

ABOUT THE AUTHORS

Tsutomu Yamada

Department of Energy Management Systems Research, Hitachi Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of embedded computer architecture, network systems and cybersecurity for industrial control systems. He is a Professional Engineer, Japan (Information Engineering). Mr. Yamada is a member of the IEEE, the International Society of Automation (ISA), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Society of Instrument and Control Engineers (SICE).

Toshihiko Nakano, Ph.D.

Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Tadashi Kaji, Dr. Info.

Infrastructure Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of information security technology. Dr. Kaji is a member of the IEEE Computer Society.