Trends in Industry Standards and International Standards for Industrial Automation Control System Security

Tatsuaki Takebe [*1]

Several security standards have been proposed for industrial control systems. Standardization activities began in the United States and Europe and their results were then studied in Japan. Oil and gas, chemical, and electric power industries have produced results. Non-profit organizations in each industry contributed to standardization and governmental organizations also helped them. In addition, public and private research institutes have been participating in these activities to identify issues on security in industrial control systems and have been providing solutions. Among them, ISA99 has been playing the key role in investigating industrial control systems security from wide ranging perspectives .

ISA99 developed ISA 62443, which defines reference model and reference architecture for an industrial control system connected to corporate information systems via DMZ, and defines the security requirements for organizations, control systems, and control devices. The international standards IEC 62443 series is combination of ISA 62443 series and WIB 2.0. A security evaluation and certification standard was developed by the ISA Security Compliance Institute referencing the IEC 62443 series. It is expected to be used for security certification in industrial control systems and to enhance the security of the systems. This paper summarizes industry and international standards for security, including those described above.

INTRODUCTION

Industrial control systems, which were composed of their own OSs, communication protocols and a dedicated closed network in their early days, have evolved to achieve high functionality, added value, and productivity, by incorporating general-purpose IT technologies and components, following the shift to open system architecture. When security problems were found in general-purpose IT technologies or components, they have been addressed for business IT systems, while the efforts to address to these issues of process control systems have just recently begun. As shown in Figure 1, security-attacking tools and techniques have been evolving year by year and their operations have become simpler, lowering the threshold of knowledge required for attacks. This shows a risk that almost anyone can be an attacker. The fact that these attacking tools have been intended for general IT and COTS components implies that they can now be applied to control systems which use many of those general-purpose IT components.

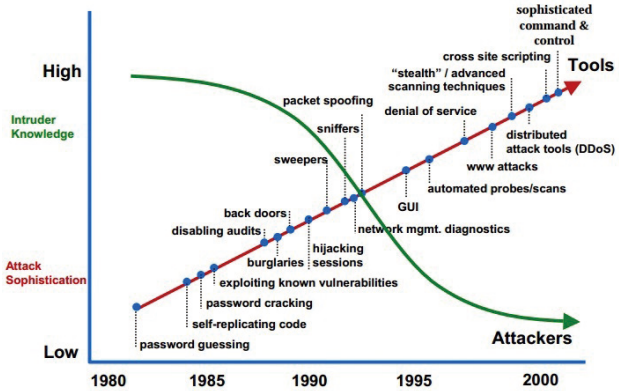

Figure 1 Attack sophistication vs. intruder technical knowledge
(from CMU/SEI-2002-SR-009, page 10)

Due to the importance of control systems and the serious impacts when security incidents occur in control systems, the security of control systems has been attracting a great deal of attention. Meanwhile, many activities have been initiated to ensure security for critical infrastructures such as electric power, oil and gas, chemical and pharmaceutical, water and

*1 Strategic Intellectual Property and Stan Standardization Dept., Marketing Headquarters

sewerage, transportation, and communications industries. These activities will ensure security and formulate standards in each industry, eventually contributing to establishing international standards.

This paper describes the security standardization activities for industrial automation control systems in the United States, Europe, and Japan, and then explains the trends in international standards.

TRENDS IN THE UNITED STATES

Overview

NIST [Note 1)] started the activity of Process Control Security Requirements Forum (PCSRF) [(1)] based on the ISO/IEC 15408 standards and published the supervisory control and data acquisition (SCADA) protection profile. NIST also published the Guide to Industrial Control Systems (ICS) Security as special publication 800-82, which outlines characteristics and guidelines for security of control systems.

DHS [Note 2)] established the Process Control Systems Forum (PCSF), in which more than 330 organizations including those from the governments, universities and industries participated. The DHS activities, deliverables of various subjects on security standards, tools, education and training, security requirements, and security test methods of control systems were created. These activities have been taken over by the Industrial Control Systems Joint Working Group (ICSJWG), and the meetings are held twice a year. In these meetings, themes of the presentation range from research to actual operation, including problems, results, countermeasures, and trends in the industries regarding control system security. ICSJWG meetings gather participants from broad range sectors like governments, universities, asset-owners, vendors, system integrators, and security consultants.

In addition, the Control Systems Security Program (CSSP) established by DHS conducted a security evaluation on control systems, summarized its results in a report, Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems, and urges the concerned parties to take measures. In this report, program codes, web services, network protocols, network design, patch controls, authentication, encryption, and others are identified as the major causes of introducing vulnerabilities.

DHS also offers advanced security training at INL [Note 3)], which includes one-day practice after four-day training. During the practice, participants are divided into an attacking team (Red Team) and a defending team (Blue Team), and practice security attack and protection on a small plant prepared for this purpose. The participants in this practice are awakened to difficulties in defensive security operations and the seriousness of damage caused by attacks, and they become determined to promote security for control systems.

As for the advanced security conference, the SCADA Security Scientific Symposium (S4) organized by Digitalbond, Inc. [Note 4)] is well known. The conference provides presentations by researchers on advanced security technologies and the latest topics, and an additional half-day to one-day seminar. The presentations focus on recent vulnerabilities, methods for finding vulnerabilities, security measures, and operational techniques in control systems.

Trends in the industries

In the oil and gas industries, oil and natural gas companies and the DHS Science and Technology (S&T) Directorate are promoting the LOGIIC [Note 5)] project. This project has published research results and measures on security subjects of greater interest, and is still continuing its activities. The API [Note 6)] published the API 1164, a guidance document regarding security of pipeline systems. In this document, physical security is also considered to ensure pipeline security.

The chemical and pharmaceutical industries are continuously making great efforts on the security activities, because their plants are equipped with processes that may cause serious or fatal damage once a security incident occurs. For example, Chemical Industry Data eXchange (CIDX), summarized the methods to assess vulnerabilities in Cybersecurity Vulnerability Assessment Methodologies. The key members of this publication are closely related to the ISA99 described later, and contributed to the prototype draft of the ISA 62443-2-1 defining management specific to control systems. This activity was taken over by the ChemITC [Note 7)] and is still continuing.

In the electric power industry, NERC [Note 8)] has established the standards for critical infrastructure protection (CIP) as NERC-CIP series standards to ensure the reliability of the security of electric power suppliers, the number of which in the US is much larger than that in Japan. These standards are used for audits, and penalties are charged or correction orders are issued to the organizations that do not observe these standards.

TRENDS IN EUROPE

In the UK, the National Infrastructure Security Coordination Centre (NISCC), an inter-departmental centre of the UK government that will be formally established in the future, documented and released the Good Practice Guide for process control and SCADA security focusing on the following seven key themes.

Theme 1 - Understand the business risks

Theme 2 - Implement secure architecture

Note 1) National Institute of Standards and Technology, http://www.nist.gov/
Note 2) Department of Homeland Security, http://www.dhs.gov
Note 3) Idaho National Laboratory, http://www.inl.gov
Note 4) Digital Bond Inc., http://www.digitalbond.com
Note 5) Linking to the Oil and Gas Industry to Improve Cybersecurity, http://logiic.automationfederation.org
Note 6) American Petroleum Institute, http://www.api.org
Note 7) Chemical Information Technology Center, http://chemitc.americanchemistry.com
Note 8) North American Electric Reliability Corporation , http://www.nerc.com/

Theme 3 - Establish response capabilities
Theme 4 - Improve awareness and skills
Theme 5 - Manage third party risks
Theme 6 - Engage projects
Theme 7 - Establish ongoing governance

CPNI [Note 9)] has taken over these guides.

SMi Group Ltd. [Note 10)] in the UK holds conferences on smart grid cyber security and on oil and gas cyber security. Presentations and seminars in those fields serve to enhance interests and consciousness among stakeholders.

In the Netherlands, TNO [Note 11)] released the SCADA Security Good Practices for the Drinking Water Sector. This includes guidelines for the water utility industry but is also useful for other industries that use SCADA.

The WIB 2.0 created by the Working-party on Instrument Behavior (WIB), a Hague-based process automation users' association, defines the security requirements for control system providers. In the latest version, WIB 2.0 aims to simplify the asset owners' acceptance test procedures and to raise the security assurance level of the acquiring process control systems by the security maturity levels of the process control systems suppliers.

There are many communities relating to control system security in Europe. For example, the Meridian Process Control Security Information Exchange (MPCSIE) holds information exchange meetings every year, and the European Network and Information Security Agency (ENISA) is releasing deliverables such as security initiatives for smart grids and control systems.

TRENDS IN JAPAN

In Japan, the activities for control system security have been accelerated from around 2007 to 2008. In 2010, a workshop on cyber security and economy was initiated, sponsored by the Ministry of Economy, Trade and Industry. The interim report of the workshop emphasizes the importance of the efforts for ensuring control system security. In 2011, a control system security study taskforce was initiated to start investigation on the issues for enhancing control system security. The taskforce discussed the following:

- Promoting international standardization
- Constructing testbed
- Developing evaluation and certification scheme
- Establishing incident response framework
- Developing human resources
- Raising public security awareness among process control system users' community

In line with these activities, the CSSC [Note 12)] was established in 2012 and a test bed was constructed in 2013 in Tagajo City, Miyagi Prefecture. Since the hardware is ready, CSSC is expected to provide training courses including practice of security offense and defense using the test bed, and services of finding zero-day security problems and the countermeasures with explanation to the parties concerned. Developing human resources with skills able to provide such training and services is considered to be a challenge for CSSC.

As for other activities for control system security in Japan, IPA [Note 13)] is investigating overseas control system security and releasing the reports, and JPCERT/CC [Note 14)] has translated overseas documents related to control systems into Japanese and published their translations.

INTERNATIONAL STANDARDS

The organization that has a large number of participants and has reached the establishment of international standards is the ISA99 committee of the ISA [Note 15)]. The ISA99 committee has created drafts for international standards as ISA 62443 series, which were deliberated in IEC TC65/WG10 by members worldwide, and approved to be the international standard as IEC 62443 series. At present, the IEC 62443 series consists of 13 documents as shown in Table 1. Among these, IEC 62443-1-1 [(2)], IEC 62443-2-1 [(3)], IEC 62443-3-1 [(4)], and IEC 62443-3-3 [(5)] have already been published.

Table 1 Overall structure of IEC 62443
(reproduced from the ISA99 Working Product List)

ISA Reference	IEC Reference	Title
ISA-62443-1-1	WP-1-1|IEC/TS 62443-1-1	Models and Concepts
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master Glossary of Terms and Abbreviations
ISA-62443-1-3	IEC 62443-1-3	System Security Compliance Metrics
ISA-TR62443-1-4	IEC/TR 62443-1-4	Security Life Cycle and Use Cases
ISA-62443-2-1	IEC 62443-2-1	Requirements for an IACS Security Management System
ISA-TR62443-2-2	IEC/TR 62443-2-2	Implementation Guidance for an IACS Security Management System
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch Management in the IACS Environment
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS Solution Suppliers
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security Technologies for IACS
ISA-62443-3-2	IEC 62443-3-2	Security Risk Assessment and System Design
ISA-62443-3-3	IEC 62443-3-3	System Security Requirements and Security Levels
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements
ISA-62443-4-2	IEC 62443-4-2	Technical Security Requirements for IACS Components

To promote security evaluation and certification based on these standards, ISCI [Note 16)] was established by ISA, and the ISCI has prepared standards for evaluation and a certification framework. The certification program using those standards and the framework are already working, and some devices for control systems have already been certified. On top of the device certification, system security evaluation for control

Note 9) Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk
Note 10) SMi Group Ltd., http://www.smi-online.co.uk
Note 11) Netherlands Organization for Applied Scientific Research, http://www.tno.nl
Note 12) Control System Security Center, http://www.css-center.or.jp
Note 13) Information Technology Promotion Agency, http://www.ipa.go.jp
Note 14) Japan Computer Emergency Response Team Coordination Center, http://www.jpcert.or.jp
Note 15) The International Society of Automation, http://www.isa.org
Note 16) ISA Security Compliance Institute, http://www.isasecure.org/

systems composed of embedded control devices with HMI, engineering station, servers, structured in the Zones and Conduits will be started soon.

The IEC 62443 series consists of four parts. Part 1 (IEC 62443-1) defines common items such as concepts, models, and terms.

Part 2 (IEC 62443-2) defines the security of organizations possessing control systems; in other words, the security policies and management systems in those organizations. Certification programs based on the IEC 62443-2-1 for a cyber-security management system (CSMS) for industrial automation and control systems have been initiated, which certify security management systems of control system users. The IEC 62443-2-4 is under constructive discussion in IEC TC65/WG10 while incorporating the opinions of vendors and system integrators to resolve overlapping with other documents of the IEC 62443 series, and to document the judgment by assessors based on their tacit knowledge during the certification process. The results are scheduled to be released as the standard soon.

Part 3 (IEC 62443-3) defines, for system integrators, detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1. FRs are identification and authentication control (FR1), use control (FR2), system integrity (FR3), data confidentiality (FR4), restricted data flow (FR5), timely response to an event (FR6), and resource availability (FR7). System integrators determine the security level required for the system for each FR for reducing risks of the control system to the required level, next determine the required SRs based on them, and then design and implement the selected SRs.

Part 4 (IEC 62443-4), currently discussed for standardization, covers security of devices, appliances, and applications constituting control systems, and is planned to define assurance requirements and functional requirements for equipment vendors. Prior to its formal standardization, the ISCI has started the ISASecure® EDSA certification program based on the IEC 62443 framework focusing on the security of embedded devices. The content defined for this certification program is proposed to be reflected in the IEC 62443-4.

In this way, the IEC 62443 series is being established as the basis for security certification for control systems, and the certification programs based on these standards are expected to improve the security level of control systems as a whole.

CONCLUSION

The industrial and international standardizations of control system security are directly contributing to the security improvement in control systems. Especially, the IEC 62443 series is evolving day by day as the standards suitable for control system security with the help of the activities of ISA99, IEC TC65/WG10, WIB, ISCI, and ISO/IEC JTC 1 SC 27, a standardization subcommittee of the Joint Technical Committee ISO/IEC JTC 1. In addition, the IEC 62443 series is used as the base of CSMS certification, security maturity certification, and evaluation and certification of security of control devices and systems. While resolving problems found during those evaluations and certifications, this series is expected to satisfy the demands of the times.

Yokogawa is an association member of the CSSC and is contributing to its security activities in Japan. Yokogawa also participated in several working groups including those for international standardization activities. In addition, Yokogawa immediately earned embedded device security certification based on the ISASecure EDSA and earned CSMS certifications. Yokogawa will continue to contribute to standardization activities to improve security measures for control systems.

REFERENCES

(1) Keith A. Stouffer, Joseph A. Falco, et al., "The NIST Process Control Security Requirements Forum (PCSRF) and the Future of Industrial Control System Security," TAPPI Paper Summit - Spring Technical and International Environmental Conference, 2004, pp. 1337-1344
(2) IEC/TS 62443-1-1 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
(3) IEC 62443-2-1 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
(4) IEC/TR 62443-3-1 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems
(5) IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

* All products or other names mentioned in this document are either trademarks or registered trademarks of their respective holders.