CSMS

Cyber Security Management System

Conformity Assessment Scheme

for the CSMS Certification Criteria（IEC 62443-2-1:2010）

CSMS

JIPDEC

1 Purpose of the CSMS Conformity Assessment Scheme

The CSMS (Cyber Security Management System) Conformity Assessment Scheme (hereinafter the 'CSMS Scheme'*1) is a third-party certification scheme*2 for cyber security management systems on the Industrial Automation and Control System (IACS). The CSMS Scheme is aimed at contributing to the improvement of security of control systems in Japan, and ensuring and maintaining security measures to win the trust of all stakeholders.

*1: 'CSMS' in the CSMS Scheme refers to the security management system for control systems. (News release by the Ministry of Economy, Trade and Industry dated April 25, 2014).

*2: The CSMS Scheme was established by utilizing the outcome of the government project to develop certification infrastructures for securing the control system, one of the themes in the Ministry of Economy, Trade and Industry's project to develop global certification infrastructures, funded in the FY2012 supplementary budget.

2 CSMS Overview

Necessity of security measures for control systems

IACS refers to industrial automation and control systems that support social and industrial infrastructures in the fields of energies (electricity, gas, etc.), petroleum / chemical / steel plants, transportation (including railways), machinery, food production / processing, building management, etc.

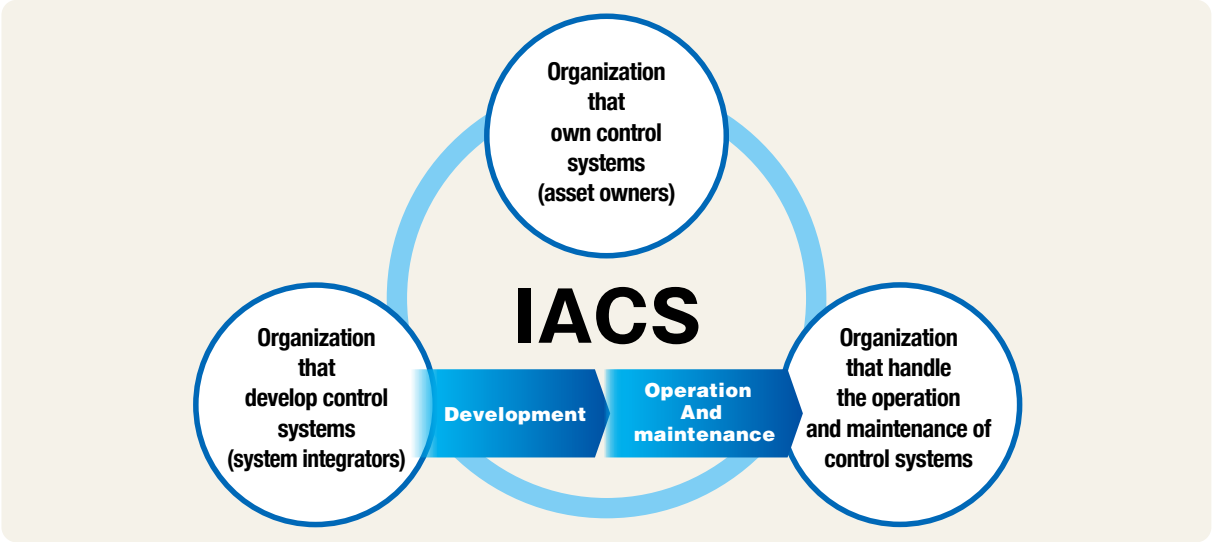
Conventionally, it was considered that there was no real security threat for IACS, as it was composed of dedicated systems, unconnected to external networks. However, IACS is increasingly becoming a potential target for cyber-attacks following the recent proliferation of general-purpose technologies developed for business application systems (computer and server infrastructures / environment, protocols such as TCP/IP), networks (remote operation, remote maintenance, etc.) and media (data extraction, parameter changes).

The shutdown of IACS with cyber-attacks could not only affect social infrastructures and business continuity, but also have serious impacts on the HSE*3. Accordingly, the introduction of CSMS has become essential to appropriately manage security measures, designed to protect each organization's IACS from cyber-attacks.

*3: HSE stands for Health, Safety and Environment. It refers to the responsibility of protecting the health and safety for employees and surrounding communities, and managing and maintaining a high level of competency in the environment. (as defined in the IEC 62443-2-1 3.1.16)

Target Organization of CSMS

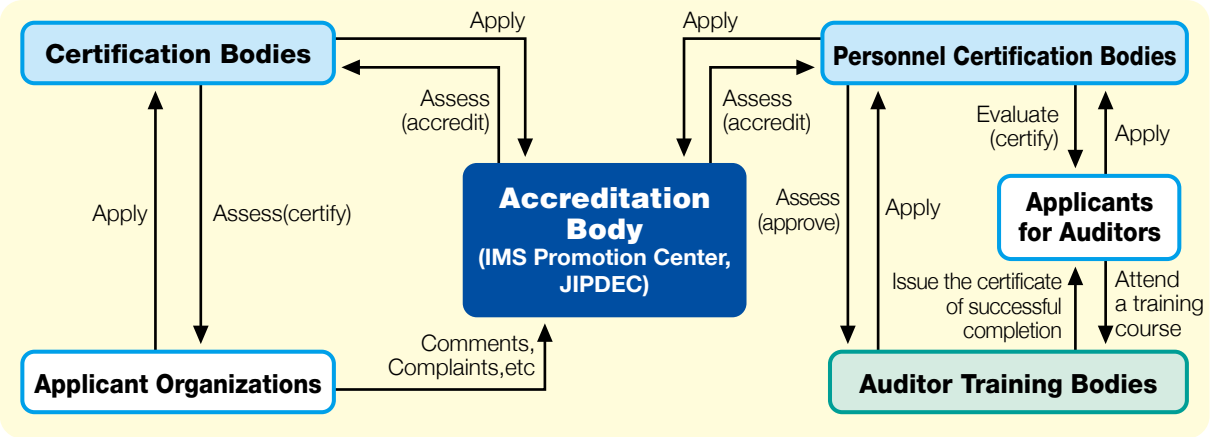
In view of the life cycle of control systems, CSMS covers organizations that own control systems, as well as organizations that handle the modification and maintenance of existing systems and system integrators that develop control systems.



3 Operation of the CSMS Conformity Assessment Scheme

The CSMS scheme has a comprehensive structure, composed of "certification bodies" that assess and certify an applicant organization's CSMS based on the CSMS Certification criteria; "personnel certification bodies" that certify and register CSMS auditors, and the "accreditation body" that assesses the competence of those bodies in implementing such tasks.

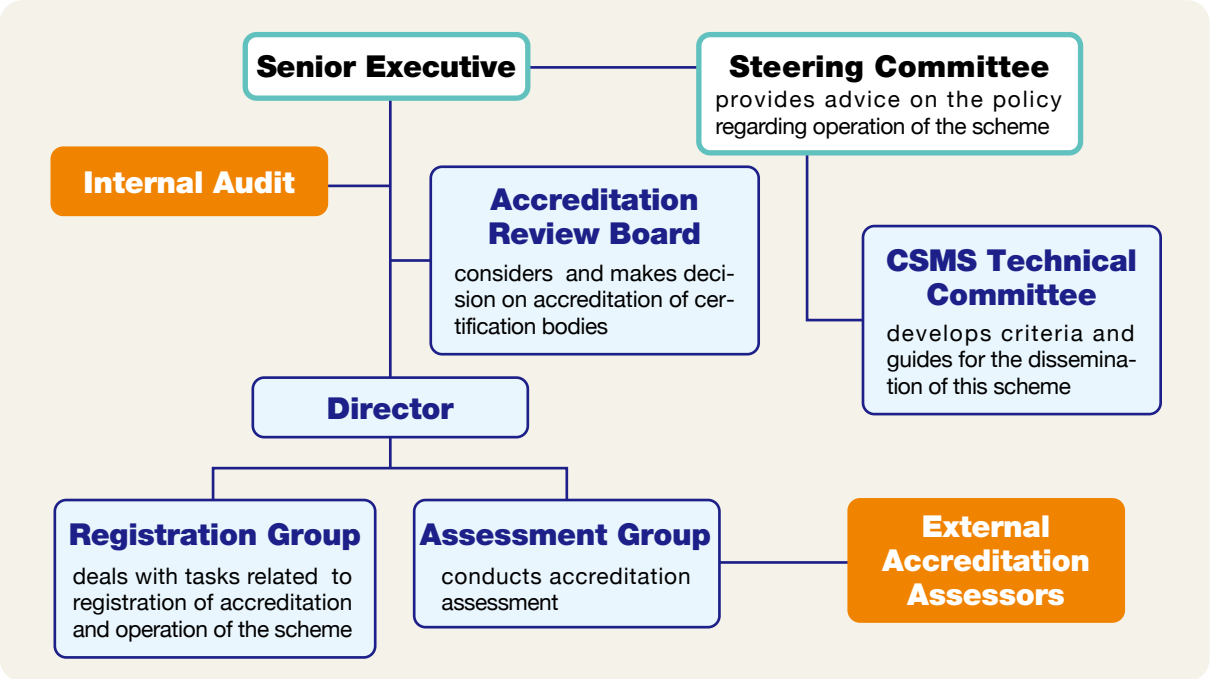
Structure of the Conformity Assessment Scheme



Impartiality, Transparency and Objectivity of the CSMS Scheme Operation

To ensure impartiality, transparency and objectivity of the CSMS scheme, some committees have been set up in JIPDEC: one of them is the Steering Committee comprised of academic and relevant industry experts, and another one is its sub-committee, the Technical Committee. The accreditation review board, which is comprised of experts, has also been set up to consider and decide accreditation of certification bodies and personnel certification bodies.

For further information on the activities on these committees, please visit our website
http://www.isms.jipdec.or.jp/org/index.html



4 Benefits of developing and managing CSMS

By developing and managing CSMS, an organization can gain the following benefits:

●Reduce risk of cyber attacks

The development and management of CSMS enhance organizational understanding of risk management, leading to security initiatives with a higher sense of purpose. Implementing security measures based on CSMS can also reduce risk of cyber-attacks.

●Strictly adhere to the best practice guidelines for security controls on IACS administrators

Ensuring that the administrators of IACS adhere to the best practice guidelines can reduce the possibility of a security incident caused by human errors or organizational factors. Also, implementing educational curriculum including incident trainings can enhance awareness on security.

●Facilitate continual improvement of security measures

By developing and managing CSMS, the organization can conduct practical revision of its security guidelines, clarify the application states of these guidelines among its sites, and continually improve its security measures through such activates. In addition, developing and managing CSMS enables the organization to gain confidence in and have convincing justification for design, delivery and installation concerning the security of control systems.

5 Benefits of achieving CSMS certification

By achieving CSMS certification, an organization can gain the following benefits:

●Provide objective proof for organizational cyber security management system

Obtaining CSMS certification can not only strengthen the organization's cyber security management system,but also provide objective proof to show external parties that the organization fulfills its social responsibility.

●Receive security checks from a third-party viewpoint

The third-party audit by auditors from a certification body highlights areas that are difficult to detect in self-checks.

●Reinforce the strength of an organization's brand

CSMS certification is third-party proof that the system supplied by an integrator can be established in the highly secured environment, thereby reinforcing the strength of an organization's brand.

6 CSMS Certification Criteria

The framework for security management system is necessary for an organization handling IACS development and management in order to achieve a fundamental security improvement. The IEC 62443 series of standards includes IEC 62443-2-1 on the security management system for IACS, as one of the standards that can be applied to formulate control system security. Based on the IEC 62443-2-1, the 'CSMS Certification Criteria (IEC 62443-2-1:2010)' (hereinafter 'CSMS Certification Criteria') have been developed as the certification criteria for security management systems in the field of IACS.

■IEC 62443 series

- IEC 62443-1：Defining terminology, concepts and models for this series of standards as a whole
- **IEC 62443-2：Security management system for organizations**
- IEC 62443-3：System security requirements and technical overview
- IEC 62443-4：Security functions and development process requirements for components (equipment and devices)

7 Structure of the CSMS Certification Criteria

The CSMS Certification Criteria specify general requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented CSMS within the context of the organization's overall business activities and risks it faces.

■ 4.2 Risk analysis

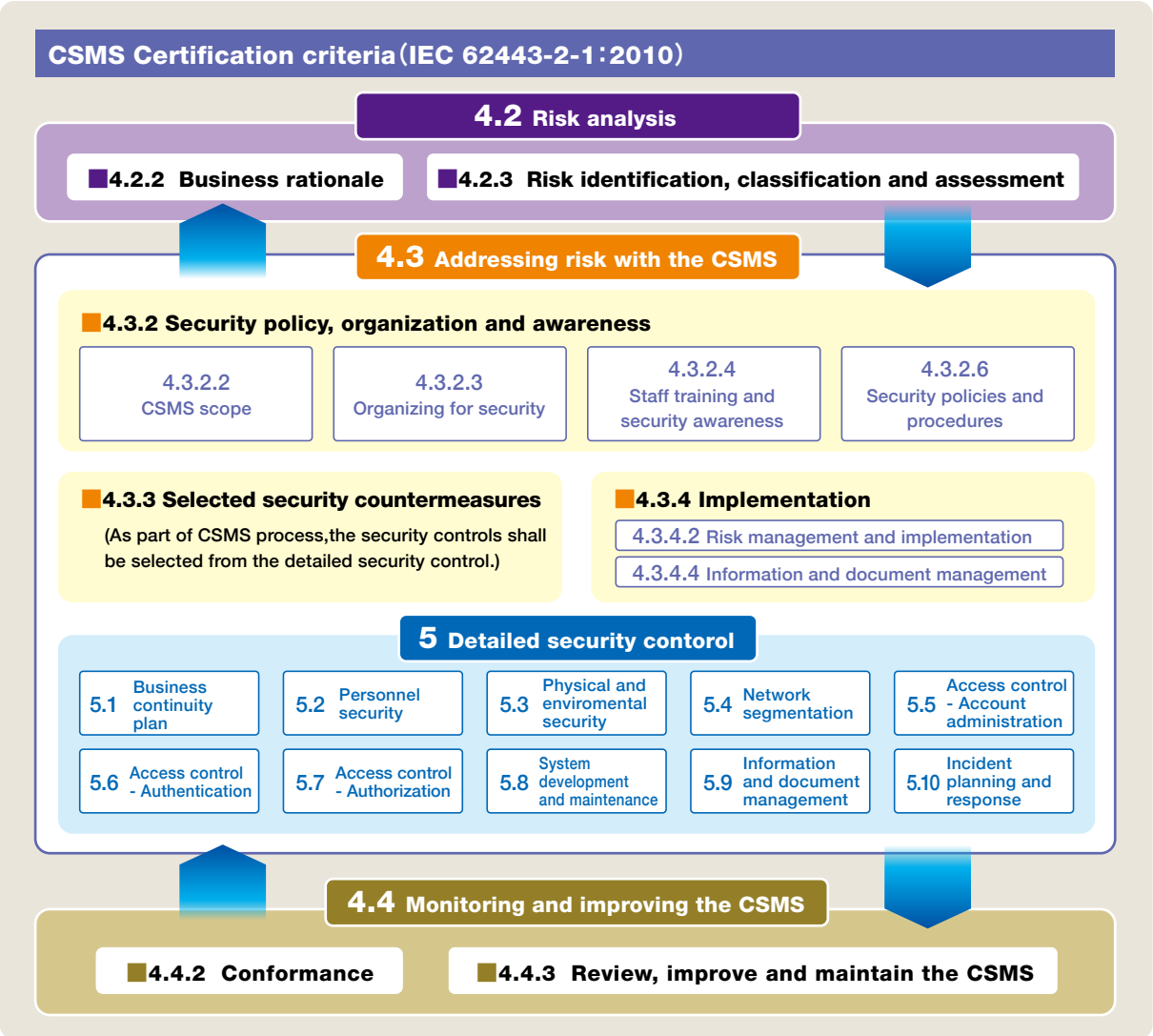
- 4.2.2 Business rationale: Identify and document the unique needs of an organization to address cyber risk for IACS.
- 4.2.3 Risk identification, classification and assessment: Identify the set of IACS cyber risks that an organization faces and assess the likelihood and severity of these risks.

■ 4.3 Addressing risk with the CSMS

The organization shall select controls as CSMS security measures from those listed in '5. Controls'. It shall then produce a 'Statement of Applicability' that contains selected controls and justifications for inclusions, and also excluded controls and justifications for exclusions.

■ 4.4 Monitoring and improving the CSMS

- 4.4.2 Conformance: Ensure that the CSMS developed for an organization is followed.
- 4.4.3 Review, improve and maintain the CSMS: Ensure that the CSMS continues to meet its goal over time.

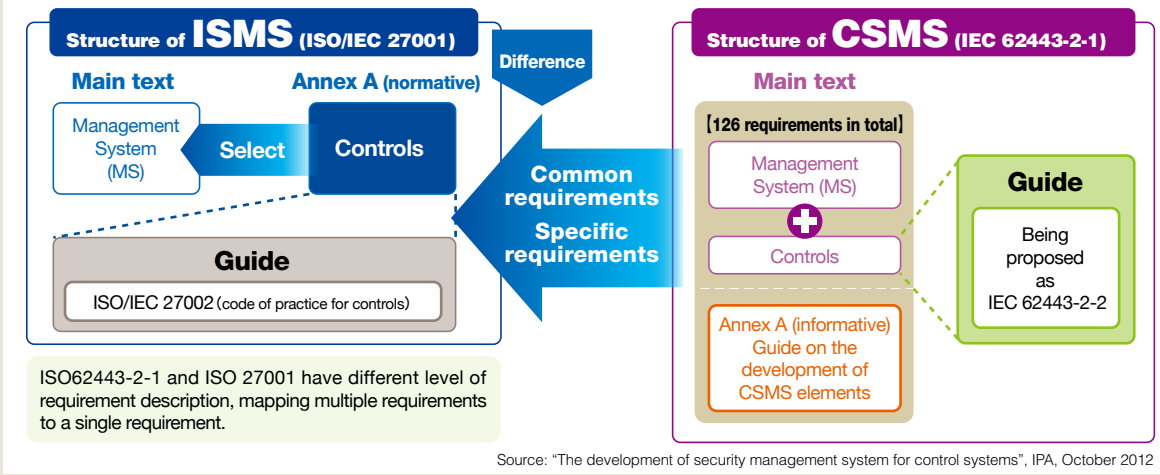


8 Relationship between CSMS and ISMS

IEC 62443-2-1 has been developed by reference to ISO/IEC 27001 with additions specific to control systems. They therefore share a number of similar requirements. For this reason, a company that has already acquired ISMS (Information Security Management System) certification is considered to satisfy the most of the CSMS requirements.

ISMS focuses on the leakage of information which should be protected, and in many cases, tend to emphasize Confidentiality, Integrity and Availability (CIA) in that order. In comparison, CSMS regards 'operation suspension' as the event that should be avoided most, and therefore emphasizes Availability, Integrity and Confidentiality (AIC) in that order, while also taking HSE into account.

Comparison between IEC 62443-2-1 and ISO/IEC 27001

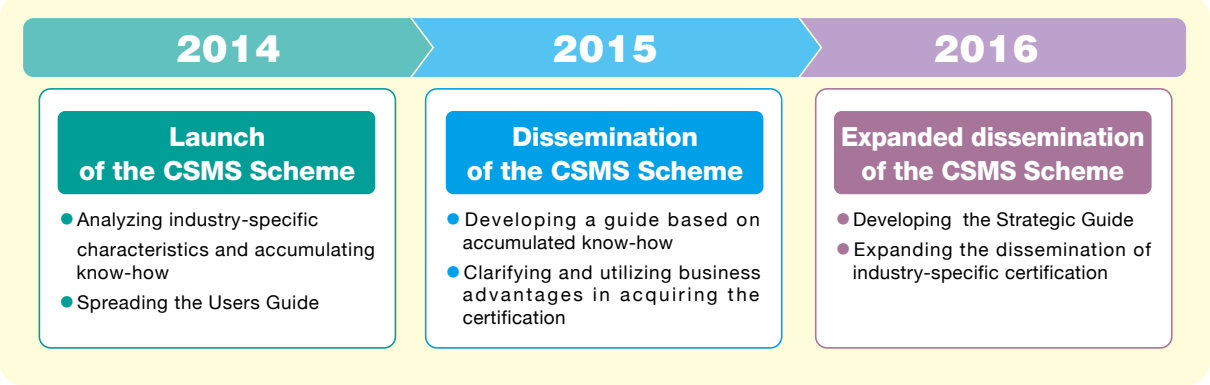


Source: "The development of security management system for control systems", IPA, October 2012

9 Dissemination of the CSMS Scheme

From the perspective of management systems, the development and management of CSMS have the effect of continually improving the effectiveness of security measures on control systems. Disseminating CSMS is therefore an important approach for industrial and social infrastructures. It is expected that, by spreading CSMS certification services by accredited certification bodies, organization's control system will strategically utilize their CSMS certification in expanding international business.

If many of the control system owners, operation / maintenance services and system integrators acquire CSMS certification, the security measures for control systems are expected to improve continually across our society.

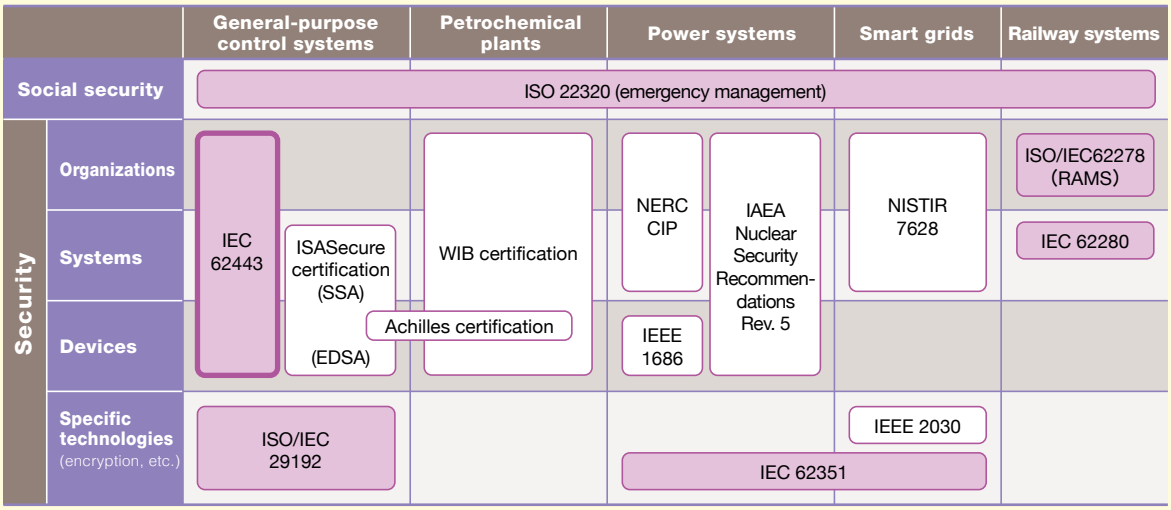


10 Standards associated with control system security

In the field of control systems, in addition to IEC 62443 series of standards for general use, there are individual control system standards for each relevant sector – critical infrastructure sectors such as electricity including the smart grid, gas, water and sewerage, railway and aviation, and manufacturing industry sectors with high proportion of organizations involved in control systems. Among those standards, CSMS can be widely applied to the sectors.

Overview of CSMS-related standards

Source:Hitachi Review Vol. 63 (2014), No. 5



SSA(System Security Assurance),EDSA (Embedded Device Security Assurance) ,NERC (North American Electric Reliability Corporation) ,CIP (Critical Infrastructure Protection) ,IAEA (International Atomic Energy Agency) ,NISTIR (National Institute of Standards and Technology Interagency Report) ,RAMS (Reliability,Availability,Maintainability and Safety)

····International standard
····Industry standard

11 Trends of the IEC 62443 series

CSMS certification is intended for control system owners, organizations providing operation / maintenance services and system integrators. In contrast, EDSA certification is for products and equipment. The ISA Security Compliance Institute (ISCI) provides a certification program for control system components (products). The standards used as the basis for the program have been reflected to the IEC 62443 series.

Category	Main target	Standard code	Standard name
Common	Overall	IEC/TS 62443-1-1:2009	Terminology, concepts and models
		IEC/TR 62443-1-2	Master glossary of terms and abbreviations
		IEC 62443-1-3	System security compliance metrics
		IEC/TR 62443-1-4	IACS security life cycle and use case
Security programs	Control system owners and administrators	IEC 62443-2-1:2010	Establishing an industrial automation and control system security program
		IEC 62443-2-2	Operating an industrial automation and control system security program
		IEC/TR 62443-2-3	Patch management in the IACS environment
		IEC 62443-2-4	Requirements for IACS solution suppliers
Systems	Control system developers	IEC/TR 62443-3-1:2009	Security technologies for industrial automation and control systems
		IEC 62443-3-2	Security levels for zones and conduits
		IEC 62443-3-3:2013	System security requirements and security levels
Components	Components	IEC 62443-4-1	Product development requirements
		IEC 62443-4-2	Technical security requirements for IACS components

★The draft titles may be subject to change.

Reference: Information-Technology Promotion Agency, Japan

Registration No. 5662324

● Contact Information ●

Roppongi First Building, 9-9 Roppongi 1-chome, Minato-ku Tokyo, 106-0032

JIPDEC IMPC

TEL ＋81-3-5860-7570　FAX ＋81-3-5573-0564

URL http://www.isms.jipdec.or.jp/

Document No. JIP-CSMS120-1.0(E)

JIPDEC IMPC

Roppongi First Building, 9-9 Roppongi 1-chome, Minato-ku Tokyo, 106-0032

TEL ＋81-3-5860-7551　FAX ＋81-3-5573-0560

URL http://www.jipdec.or.jp/

December 2014