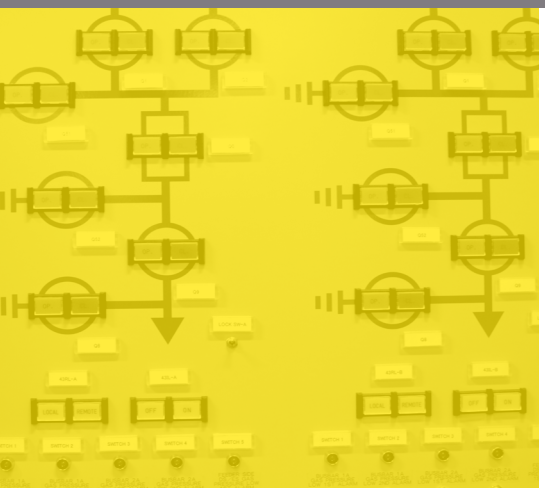
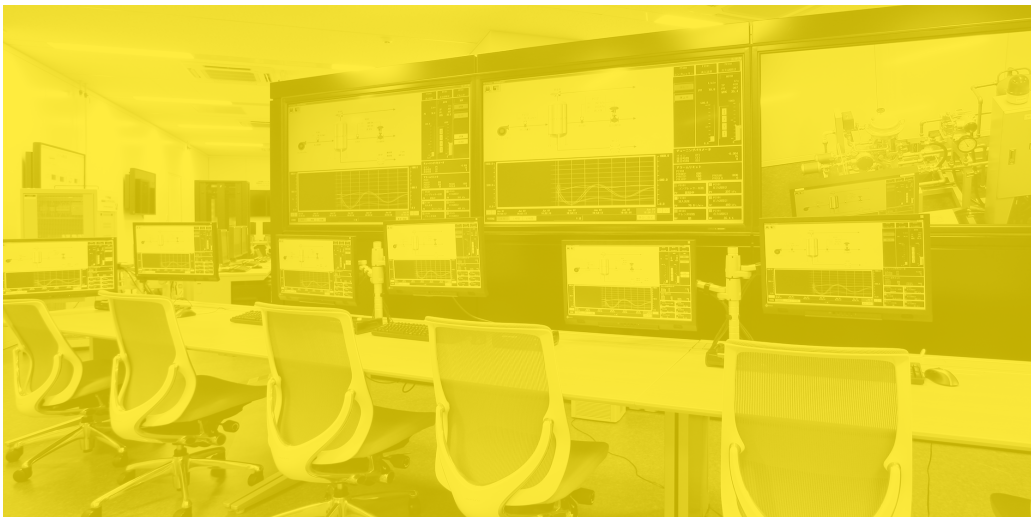
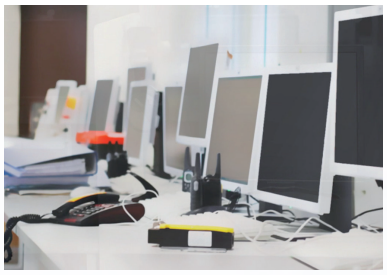
CSSC Certification Laboratory



ISASecure EDSA Certification



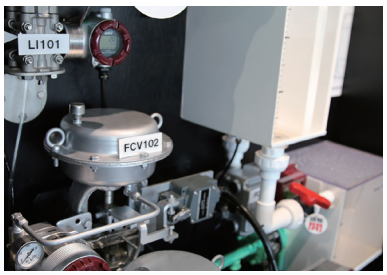

Preface

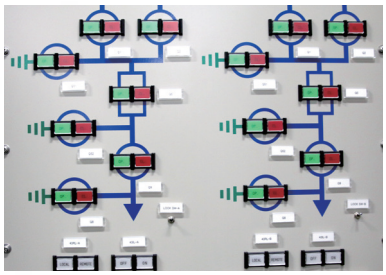
Cyber-attacks against Critical Infrastructure

Recently critical infrastructures have been moving toward computerization and networking. On the other hand, this also has brought about cyber-attacks. Actually these virtual issues have been increasingly becoming a real-world problem. If a large-scale cyber-attack succeeds in stopping critical infrastructures, it could wreak enormous damage on our daily lives and business activities. Because our daily lives totally depend on those infrastructures. Therefore security resilience is strongly required especially for such critical infrastructures as electricity, gas, water, railroad, aviation, oil, chemistry, etc.

International Security Standards for Control Systems

Based on the background above, it is essential that control systems should be implemented with effective security countermeasures against various types of cyber-attacks, because critical infrastructures depend on the control systems. Such international standardizing organizations as ISA and IEC are examining and clarifying security requirements by promoting control system-oriented security standards of ISA/IEC 62443. In the standards, risk analysis is required especially from the viewpoint of influence to health, safety and environment (HSE). Furthermore, these standards have introduced the concept of security level as strength measuring tool of security countermeasures. The strength here means, in other words, something like the height of defensive wall or hurdle against attackers.





International Security Certification Standards

In order to attain secure control systems, it is important that each control device / component consisting of a control system should be secure, safe and always available. That's why control device vendors are trying to implement security functions based on the control system security standards of ISA/IEC 62443. In order to assure its implementation, the device needs to get some certification, so that the device could be judged if the security functions are actually and adequately implemented based on the international standards.

Internationally noted certification at present is ISCI(ISA Security Compliance Institute)'s EDSA(Embedded Device Security Assurance) certification(later EDSA certification). This certification is carried out by a third-party certification body.

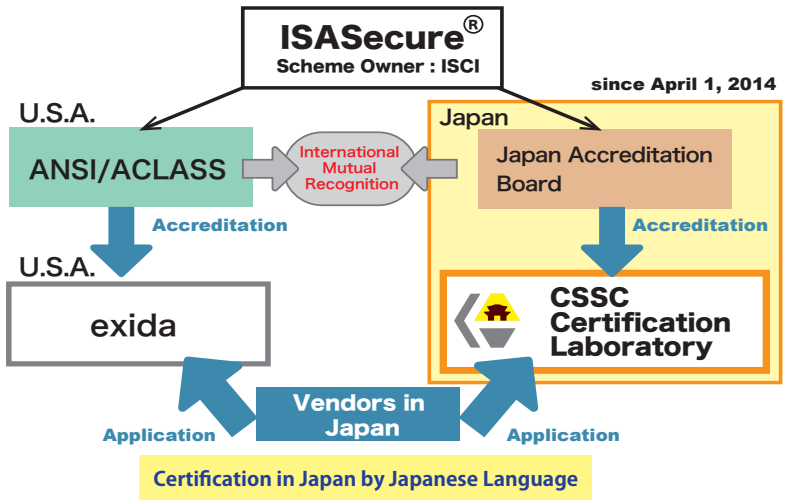
International Framework Based on Mutual Recognition

EDSA Certification provided by CSSC Certification Laboratory is an international framework based on mutual recognition (See the figure on the next page). Previously, in order to obtain EDSA certification, applicants used to apply to a USA-based certification body and prepare all documents in English. But now you can apply for it much easily, because you can apply directly to the Japan-based CSSC Certification Laboratory and prepare documents in Japanese only. EDSA certification obtained in Japan passes overseas now, and this should be beneficial for control device vendors in exporting their products, because this could enhance their competitiveness.

EDSA Certification Scheme Expanding in Japan

EDSA certification globally passes by international mutual recognition

EDSA certification, as the figure below shows, is a product certification program that passes not only in Japan, but also all over the world, by introducing internationally mutual recognition. JAB (Japan Accreditation Board) has authorized that CSSC Certification Laboratory met all ISCI defined EDSA standards for both of laboratory accreditation and product certification body accreditation. Since April 2014, CSSC Certification Laboratory has been starting to assess/evaluate control devices for EDSA certification and issue EDSA certificates for those devices successfully passed it.

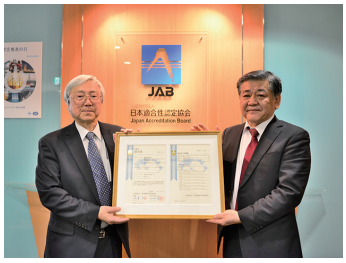


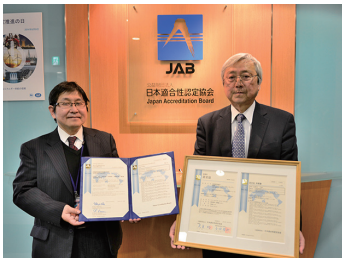
The figure shows an international program, under which each member is internationally and mutually recognized.
JAB (Japan Accreditation Board) has authorized that CSSC Certification Laboratory met all requirements required for ISASecure EDSA certification body.

ISASecure EDSA certification body as Japan's first or world's second

CSSC Certification Laboratory is now the Asia's first or world's second EDSA certification body. Now applicants in Japan are able to obtain internationally-recognized EDSA certification without going overseas nor translating all documents into English. One of our goals is to strengthen the security of critical infrastructures in Japan. And the other is to enhance competitiveness of Japanese vendors those who develop and export control devices.

EDSA certification business by CSSC Certification Laboratory is consistent with Japanese government policy on establishment of domestic assessment/ evaluation and certification body for control systems, because it is based on “Cybersecurity Strategy - Toward a world-leading, resilient and vigorous cyberspace - (June 2013)” developed and decided by Information Security Policy Council in June 2013.





Left: Mr.Kobayashi(left), Director of CSSC Certification Laboratory and Mr.Kume, Managing Director of JAB.
Right: Mr.Yoshimatsu(left), Evaluation Center Director of CSSC Certification Laboratory

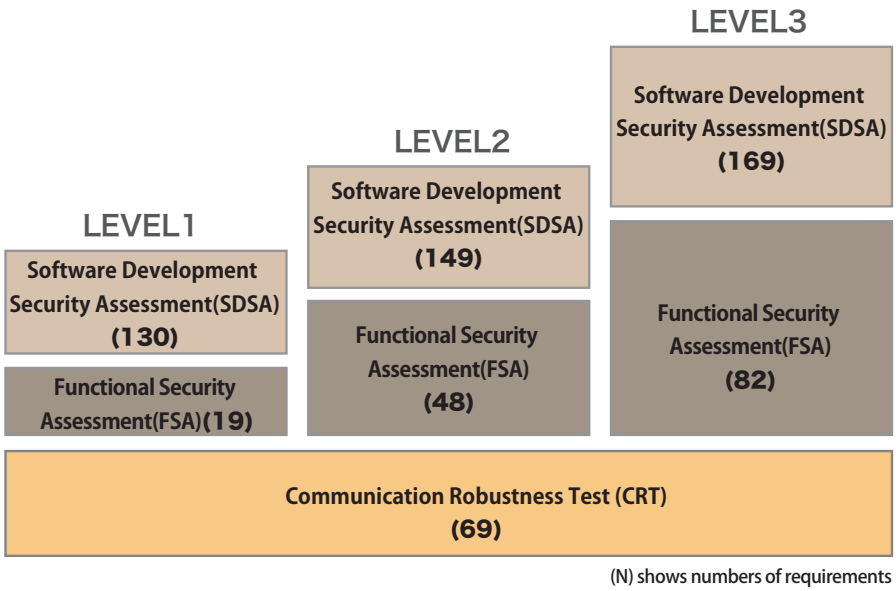
ISASecure EDSA Certification

Three Certification Technical Elements

ISCI has developed specifications for ISASecure EDSA certification (EDSA certification, later), using the framework of ISA/IEC 62443 standards. EDSA certification is a security assurance-related certification scheme for control devices and run by a scheme owner of ISCI. The certification includes the following three certification technical elements. In order to obtain EDSA certification, you need to pass all the three technical elements at the same time.

- **Technical Element No.1 :**
  Security assessment on each stage of software development (SDSA : Software Development Security Assessment)
- **Technical Element No.2 :**
  Assessment on implementing security functions
  (FSA : Functional Security Assessment)
- **Technical Element No.3 :**
  Communication Robustness Testing
  (CRT : Communication Robustness Testing)

Security is now categorized into three levels.
Regarding technical element no.3 of CRT test, the number of requirements is constant regardless of its level. On the other hand, the number of the requirements for SDSA or FSA increases according to its level.



(N) shows numbers of requirements

Reference : ICSJWG Spring 2011, (ASCI) "Validating the Security Assurance of Industrial Automation Products"

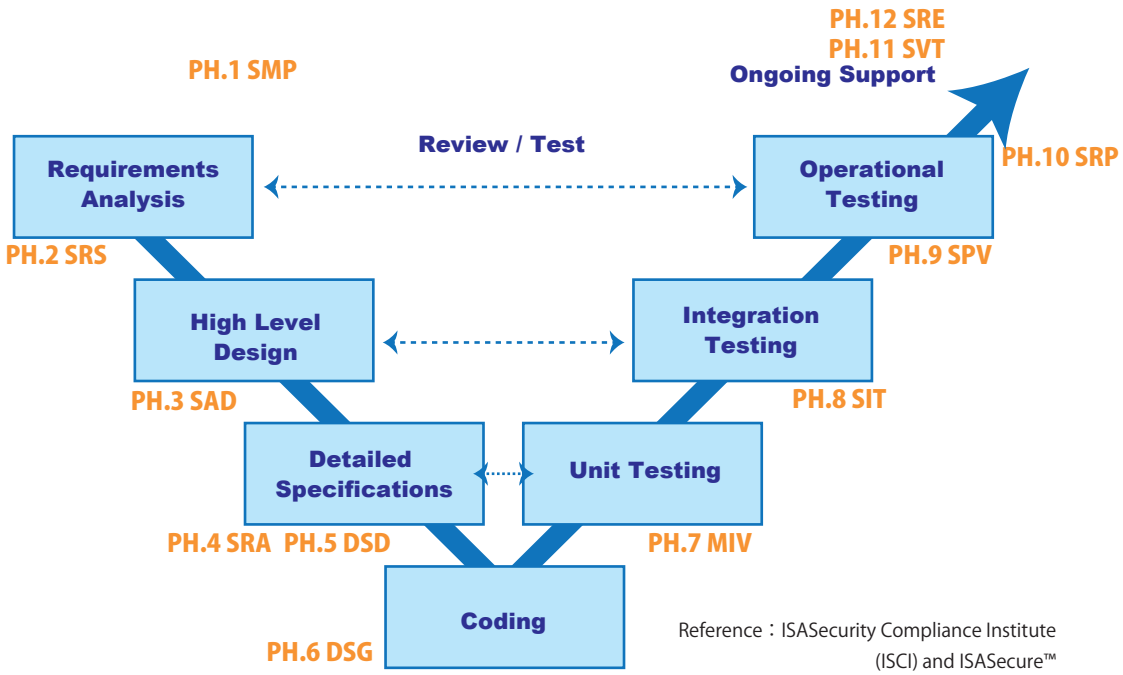
Technical Element No.1 : Security process assessment on each phase of software development

SDSA : Software Development Security Assessment (EDSA-312)

1. Assess security process of software development for targeted control devices

2. Assess development documents and records for validating PDCA process

Auditors from a certification body visit an applicant's site to examine documents submitted for certification and interview the product developers. In SDSA, for instance, they audit that each security activity phase has been implemented based on the V-shaped development model shown in the figure below. The objective of this assessment is to promote the introduction of security into software development lifecycle.



Reference：ISASecurity Compliance Institute (ISCI) and ISASecure™

No.	Activity Phase
PH1	Security Management Process(SMP)
PH2	Security Requirements Specification (SRS)
PH3	Software Architecture Design (SAD)
PH4	Security Risk Assessment and Threat Modeling (SRA)
PH5	Detailed Software Design (DSD)
PH6	Document Security Guidelines (DSG)
PH7	Module Implementation & Verification (MIV)
PH8	Security Integration Testing (SIT)
PH9	Security Process Verification (SPV)
PH10	Security Response Planning (SRP)
PH11	Security Validation Testing (SVT)
PH12	Security Response Execution (SRE)

Technical Element No.2 : Assessment on implementing security functions

FSA : Functional Security Assessment

1. **Assess security functions for targeted control devices**
2. **Assess security functions and initialization of the targeted devices based on EDSA-311 requirements. And judge if they are in conformance with the requirements or not.**
3. **Validation by independent test: Some of the requirements need to be validated by actually running and checking the real product.**

Auditors from the certification body audit based on documents for users or development, documents especially submitted for audit, and testing results on the control device. Main audit requirements are shown in the table below.

Requirements	
AC: Access Control	**User Authorization, User Authenticaiton, System Use Notification, Session Locking/Termination**
UC: Use Control	**Device Authentication, Audit Trail**
DI: Data Integrity	**Data in Transit, Data at Rest**
DC: Data Confidentiality	**Data in Transit, Data at Rest, Crypto**
RDF: Restrict Data Flow	**Information Flow Enforcement, Application Partitioning, Function Isolation**
TRE: Timely Response to Event	**Incident Response**

EDSA scheme related documents

EDSA scheme related documents roughly translated into Japanese can be downloaded free from the following ISCI website. Here you can find technical specifications, accreditation/ recognition, symbol and certificate, structure, external reference documents and so on.

http://isasecure.org/ISASecure-Program/Japanese-ISASecure-Program.aspx

Technical Element No.3 :
Communication Robustness Testing

CRT : Communication Robustness Testing

1. ISCI recognized testing device sends testing packets to DUT (Device Under Test) and checks if DUT maintains its services or not.

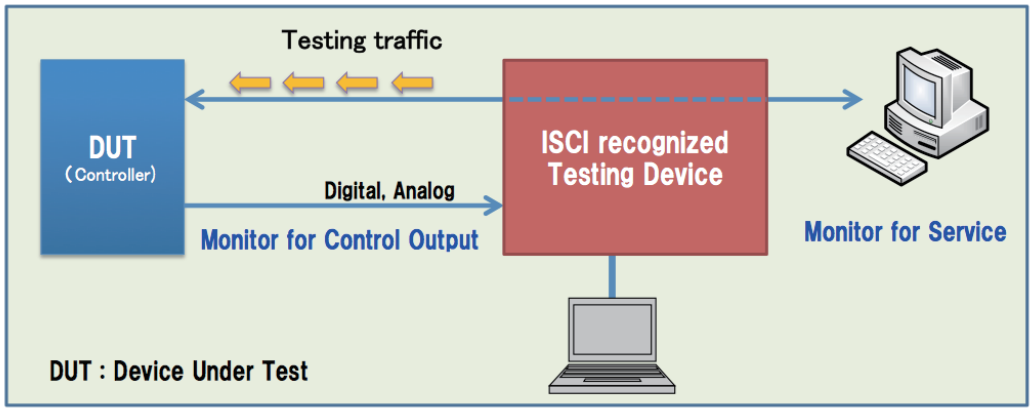
2. The pass/ fail criteria is based on whether DUT maintains the essential services or not. This testing requires not only a controller but also HMI, actually.

3. ISCI recognized testing device is used in CRT. Please see the following URL.

http://www.isasecure.org/Supplier-Resources/Recognized-Test-Platforms-for-CRT.aspx

Auditors of the certification body conduct communication robustness testing on the control devices brought into the certification body. The communication protocols currently consist of the following six types for the target communication robustness testing.

EDSA-401 IEEE 802.3(Ethernet ARP IPv4 ICMPv4 UDP TCP



■ Essential services

Check if the services using the following functions are adequately maintained or not

① Control loop
- Function to output specified signal

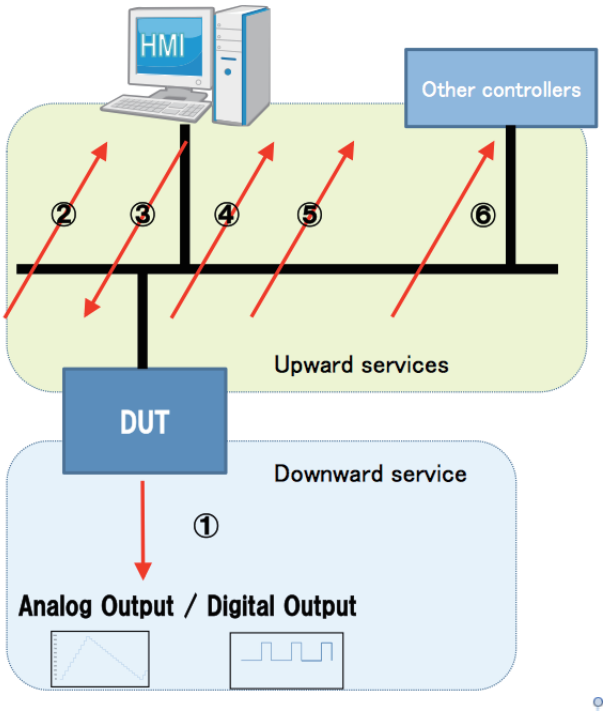
② Process Viewing
- Function to provide process viewing at an adequate timing

③ Command
- Function to respond to upper system command at an adequate timing

④ Process Alarming
- Function to provide process alarming at an adequate timing

⑤ Essential historian data
- Function to provide essential historian data at an adequate timing Opt-out possible

⑥ Peer to peer control communication
- Transmission function of peer to peer control communication
- Opt-out possible

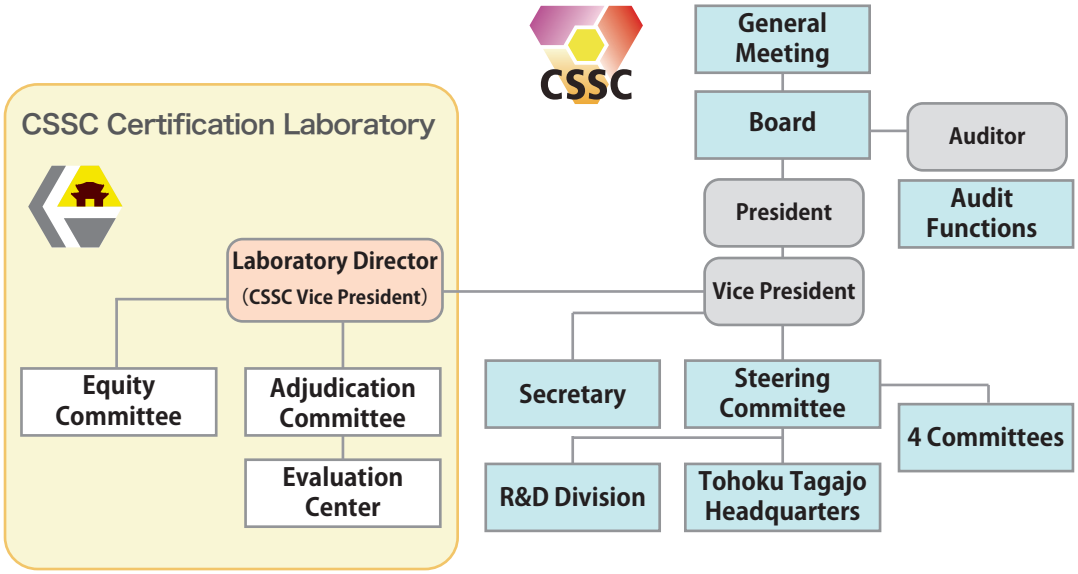


CSSC Certification Laboratory(CSSC-CL)

Certification Business is carried out independently from CSSC other departments

CSSC Certification Laboratory is an organization that is located in CSSC but independent from any other departments in CSSC.

As the figure below shows, CSSC-CL is, independently from other departments, doing impartial and fair certification business.



Application Fee for EDSA Certification

Detailed technical Items and period necessary for EDSA certification depend on the complexity and structure of the control system. The exact EDSA certification cost will be fixed based on a meeting.

Please get in contact with us for details.

Contact

Control System Security Center
CSSC Certification Laboratory

4-1 Sakuragi 3-chome Tagajo City, Miyagi 985-0842 JAPAN
TEL : 81-22-353-6751 Mail : info@cssc-cl.org
Web site : http://www.cssc-cl.org

Please see contact on our website regarding complaints or appeals.

Translated in English in December 2014
CSSC Certification Laboratory

4-1 Sakuragi 3-chome Tagajo City, Miyagi 985-0842 JAPAN
TEL +81-22-353-6751 FAX +81-50-3153-0000
http://www.cssc-cl.org