ISA Security Compliance Institute

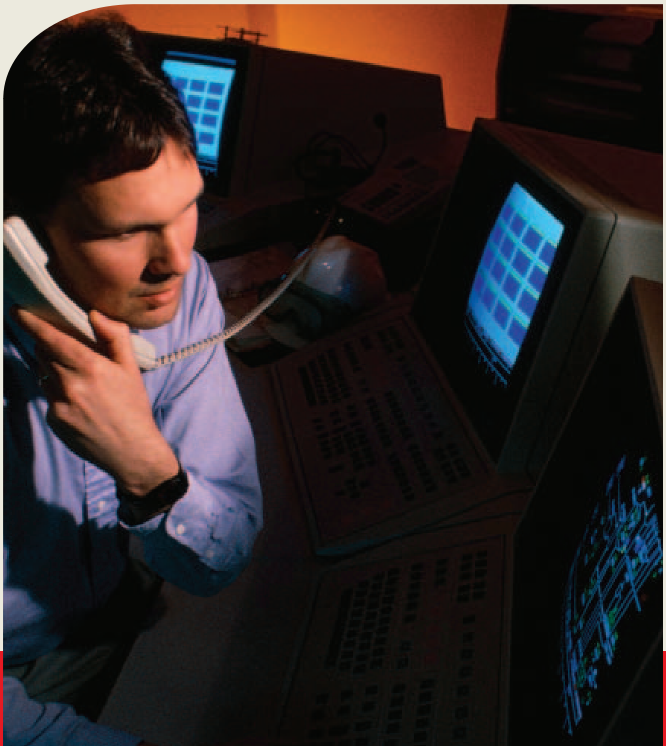
ISASecure Embedded Device Security Assurance Certification

Introduction

The ISASecure program has been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry-wide improvement of cyber security for Industrial Automation and Control Systems (IACS). It achieves this goal by offering a common industry-recognized set of device and process requirements that drive device security, simplifying procurement for asset owners and device assurance for equipment vendors.

This document provides an overview of the first ISASecure certification, which focuses on security of embedded devices and addresses device characteristics and supplier development practices for those devices. This certification is the ISASecure Embedded Device Security Assurance Certification, or ISASecure EDSA certification. An embedded device that meets the requirements of the ISASecure specifications receives the ISASecure EDSA certification—a trademarked designation that provides instant recognition of product security characteristics and capabilities and provides an independent industry stamp of approval similar to a "Safety Integrity Level" Certification (ISO/IEC 61508).

An embedded device is a special purpose device running embedded software designed to directly monitor, control, or actuate an industrial process (as defined by a work product of the ISA99 standards committee). Common examples are programmable logic controllers (PLCs), distributed control system (DCS) controllers, and remote terminal units (RTUs).



The ISASecure EDSA certification program offers three certification levels for a device, offering increasing levels of device security assurance. These certifications are called ISASecure Level 1 for Devices, ISASecure Level 2 for Devices, and ISASecure Level 3 for Devices. All levels of certification granted under this program contain the following technical elements:

- Software Development Security Assessment (SDSA)
- Functional Security Assessment (FSA)
- Communication Robustness Testing (CRT)

SDSA and FSA requirements increase in rigor for levels 2 and 3, while CRT criteria are the same regardless of the certification level. Figure 1 illustrates this concept.

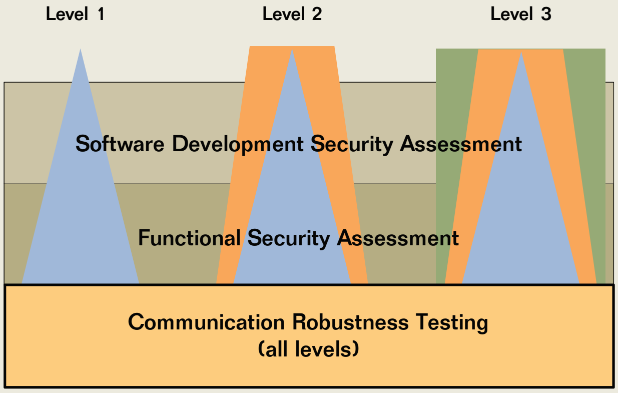

Level 1
Level 2
Level 3
Software Development Security Assessment
Functional Security Assessment
Communication Robustness Testing
(all levels)

Figure 1 - Structure of ISASecure EDSA Certification

The remainder of this document further describes the three technical elements of certification, the certification levels, and the certification program.

This effort has leveraged communication robustness testing best practices available today in the marketplace to create a common industry-recognized standard for this kind of testing. It also followed and leveraged the parallel ISA99 standards efforts underway for embedded device cyber security requirements. When the *ISA-99.04.01* standard is completed, the ISASecure EDSA certification will be updated to serve as a compliance program for that standard.

The ISASecure EDSA certification program is similar in structure to functional safety certification—IEC 61508—which is a mature and broadly accepted program.

The ISCI webpage, **www.ISASecure.org**, describes how to participate in ISCI and this ongoing effort.

Technical Certification Elements

For all levels of ISASecure EDSA certification, a device undergoes a software development security assessment (SDSA), a functional security assessment (FSA), and communication robustness testing (CRT).

The SDSA examines the process under which the device was developed. The FSA examines the security capabilities of the device, while recognizing that in some cases security functionality may be allocated to other components of the device's overall system environment. CRT examines the capability of the device to adequately maintain essential services while being subjected to normal and malformed network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks.

The following sections further describe these technical certification elements.

Software Development Security Assessment

At all levels, the SDSA covers requirements for the following development lifecycle phases:

- Security Management Process
- Security Requirements Specification
- Software Architecture Design
- Security Risk Assessment and Threat Modeling
- Detailed Software Design
- Document Security Guidelines
- Software Module Implementation and Verification
- Security Integration Testing
- Security Process Verification
- Security Response Planning
- Security Validation Testing
- Security Response Execution

An ISASecure auditor performs a SDSA audit based upon both document evidence submitted for the certification and a site visit, including interviews of development personnel and managers.

Basic criteria for passing a SDSA apply at all certification levels and become more rigorous at higher certification levels. For example, ISASecure devices at all certification levels will have documented security requirements with a specified content scope. A second example is that a change management process is required for all certification levels; however, additional requirements may apply to this process for certification levels 2 and 3.

Functional Security Assessment

The FSA examines the device from the point of view of required security capability and correct implementation. Security capabilities may be supported directly by the device itself or may be explicitly allocated to higher level components that support the device in its intended system environment. For example, in some cases a firewall with particular settings is required to be deployed along with the device to achieve adequate security.

The FSA is organized using the accepted ISA99 Foundation Requirements found in *ISA-99.03.03 System Security Requirements and Security Assurance Levels.* The FSA covers the following areas, which are addressed by *ISA-99.03.03:*

- Access Control
- Use Control
- Data Integrity
- Data Confidentiality
- Restricted Data Flow
- Timely Response to Event
- Network Resource Availability

An ISASecure auditor performs the FSA based upon user and design documentation, documentation submitted specifically for the audit, and testing of the device itself.

Basic criteria for passing an FSA apply at all levels of certification with additional criteria being introduced at higher certification levels. For example, ISASecure devices at all certification levels must support automated enforcement of access control based on authentication of users, unless this functionality is allocated explicitly to a higher level component of the system architecture; while support for role-based access control is required for higher level certifications.

Communication Robustness Testing

Communication robustness measures the extent to which network protocol implementations on an embedded device defend themselves and other device functions against unusual or intentionally malicious traffic received from the network. Under the general concept called "protocol fuzzing," invalid messages and sequences of messages are generated and sent to the device at varying traffic rates. In addition, susceptibility to known attacks against each protocol will be tested as part of the certification.

Inappropriate message responses or failure of the device to continue to adequately maintain essential services demonstrate potential security vulnerabilities within the device. Note that CRT does not examine the correctness of implementations or conformance to mandatory provisions of the controlling protocol standards.

A key definition in ISASecure CRT is "adequately maintain essential services." The following are **always** considered essential services: *the process control/safety loop, process view, command* (meaning change parameters of process control, such as setpoints), and *process alarms.* To pass the ISASecure communication robustness tests, the process control/safety loop must be maintained under all network traffic conditions. Conversely, it is acceptable that other essential services may be lost due to interference from flooding on their own network interface, but not due to any other network traffic conditions. Examples of other services that may be considered as essential services are those that "*provide critical process history information*" and *peer-to-peer control communication.* A certification applicant may explicitly opt-out of testing for the behavior of these services if they are not relevant to their marketplace or architecture.

ISCI will develop CRT specifications for the protocols in the table below, where the groups of protocols are arranged by priority with Group 1 being the highest priority. Tests for Group 1 protocols will be available for certifications at the rollout of this certification program and tests for Groups 2–5 will be available in future releases of the ISASecure EDSA certification program.

Group 1	Group 2	Group 3	Group 4	Group 5
• IEEE 802.3 (Ethernet) • ARP • IPv4 • ICMPv4 • TCP • UDP	• BOOTP • DHCP • DNS • NTP, SNTP • FTP, TFTP • HTTP • SNMPv1-2 • Telnet	• HTTPS • TLS • Modbus/TCP	• IPv6 • OPC • Ethernet/IP/CIP • PROFINET • FFHSE • Selected wireless protocols/stacks with elements such as: - IEEE 802.11 - *ISA100.11a* - WirelessHART	• SNMPv3 • SSH Server • OPC-UA • MMS • IEC 61850 • SMTP

Table 1 - Protocols for ISASecure Communications Robustness Testing

Any given embedded device will not support all of these certifiable protocols. A vendor will submit a configuration for testing that enables all of their available software functionality. All protocols with ISCI test specifications, available at the time of the certification and that are active in this configuration, will be tested for all ISASecure EDSA certification levels.

Frequently Asked Questions

1. *What is the ISA Security Compliance Institute (ISCI)?*

Founded in 2007, the ISA Security Compliance Institute's mission is to provide the highest level of assurance possible for the cyber security of industrial automation control systems (IACS). ISCI is a non-profit organization established by thought leaders from major organizations in the industrial automation controls community seeking to improve the cyber security posture of Critical Infrastructure for generations to come.

ISCI's goals are realized through industry standards compliance programs, education, technical support, and improvements in suppliers' development processes and users' lifecycle management practices. ISCI membership is open to all interested organizations and individuals. For more information, visit **www.ISASecure.org**.

2. *Who will perform ISASecure EDSA certification assessment and testing?*

ISCI will accredit organizations (called "certifiers") to perform these certification evaluations. ISCI will also accredit test platforms designed to perform communication robustness testing for use by these organizations and by device vendors in preparation for certification.

3. *Who will grant ISASecure EDSA certifications?*

ISCI grants accredited certifiers the right to grant ISASecure EDSA certifications for devices based upon the certifier's tests and assessments conforming to ISASecure specifications. ISCI will publish a list of certified products on its website (www.ISASecure.org).

4. *Which ISASecure EDSA certification will be available in 2010?*

Accredited certifiers will be prepared to accept applications for ISASecure for Devices 2009 certification, which will include all three certification elements: software development security assessment (SDSA), functional security assessment (FSA), and communication robustness testing (CRT). CRT will include testing for the Group 1 protocols as shown in Table 1 (see previous page).

5. *How were the ISASecure EDSA certification criteria developed?*

The ISASecure effort has leveraged the substantial existing work in general cyber security and process control system cyber security. The SDSA and FSA criteria are aligned, wherever possible, with draft work products of the ISA99 Standards committee. The SDSA requirements are ultimately traceable to requirements in the following source documents:

Reference Sources for Software Development Security Assessment	
ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
IEC 61508 Part 3	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software Development
RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certifications
ISBN-13: 978-0735622142	*The Security Development Lifecycle*, M. Howard, S. Lipner, Microsoft Press (June 28, 2006)
OWASP CLASP	OWASP CLASP (Comprehensive, Lightweight Application Security Process)

The FSA requirements are ultimately traceable to requirements in the following source documents:

Reference Sources for Functional Security Assessment	
ISA-99.03.03 Draft	System Security Requirements and Security Assurance Levels
NERC Standards CIP-001-1 through CIP-001-9	North American Electric Reliability Council Cyber Security Standards
NIST 800-53	Recommended Security Controls for Federal Information Systems
ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
	Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers

Achieving an ISASecure EDSA certification will not ensure compliance with the above standards. ISASecure EDSA certification criteria were selected from these sources and refined by working groups of experts based upon application and importance to embedded device security.

The CRT criteria were first developed from principles based on relevant protocol standards by subject matter experts with assistance from existing organizations that perform this kind of testing.

All ISASecure EDSA certification criteria were reviewed and approved by both the ISCI membership and an external technical subject matter expert.

6. *How does the ISASecure EDSA certification address proprietary protocols?*

ISCI will not directly address proprietary protocols as part of the CRT portion of the ISASecure EDSA certification. CRT will focus on open-standards protocols that are used in IACS; conversely, the FSA and SDSA will provide assessments of the functional security of the IACS as well as the software development processes used to develop the IACS. The SDSA will assure that secure development processes are followed as part of protocol development, thus reducing the probability that a certified embedded device contains common software errors which would lead to security and robustness issues.

7. *How does the ISASecure EDSA certification address wireless capabilities?*

The initial ISASecure EDSA certification will not apply to the wireless capabilities of embedded devices; however, ISCI plans to develop robustness test specifications for selected wireless protocols/stacks with elements such as IEEE 802.11, *ISA100.11a*, and WirelessHART. When these tests are available, they will become part of the communication robustness element of the ISASecure EDSA certification.

8. *How does the ISASecure EDSA certification address IPv6?*

The initial ISASecure EDSA certification will address IPv4 and will not apply to the IPv6 capability of an embedded device; however, ISCI will develop communication robustness test specifications for IPv6 as IPv6 becomes a protocol used by IACS.

9. *How are ISASecure EDSA certification levels related to ISA99 security assurance levels?*

ISASecure is based on published and draft standards from ISA99 in addition to other applicable standards. There is no formal relationship at this time between ISASecure EDSA certification levels and ISA99 security assurance levels, but an effort has been made to align ISASecure EDSA levels with current ISA99 thinking. As the definitions for ISA99 security assurance levels are further developed, ISCI will examine more fully how these concepts are best coordinated.

To achieve this coordination, ISCI and ISA99 have established a joint working group and a representative of the ISA99 committee holds a seat on the ISCI governing board. When the *ISA-99.04.01* standard is completed, ISASecure will be updated to become the compliance program for that standard.

10. Will a vendor that has already obtained a certification for a device be allowed to submit those results for the ISASecure EDSA certification?

Yes. ISCI has identified specific certifications from which pre-existing artifacts may be offered as evidence for meeting specific certification requirements in the ISASecure EDSA specification.

For example, an organization who has already received an IEC61508 certification for a device may submit artifacts on their software development practices to satisfy specific requirements in the SDSA specification section of the ISASecure EDSA certification.

11. What is the process for recertification when a device is modified?

A vendor that releases a modified device may apply for recertification of the modified product. The applicant for recertification will describe the changes in the new product in an ISCI-specified format as well as provide an impact analysis of the change on FSA, SDSA, and CRT topic areas.

For the FSA and SDSA, a similar discussion would determine which elements of these assessments would need to be revisited to support recertification.

In a simple CRT example, if a new product incorporated an enhanced control algorithm in the device but did not change any protocol stack, then no retesting would be needed.

Modifications to be considered by the recertification process include patches released to the field.

12. What is the process for recertification as ISCI changes the ISASecure EDSA certification criteria, such as adding new protocols to the communication robustness tests?

A device retains its certification named for a designated year, even as ISASecure EDSA certification requirements are subsequently updated. For example, even though ISASecure for Devices 2010 is updated to ISASecure for Devices 2011, the earlier certification may still be displayed for a product. Whenever appropriate, ISCI will make available a set of delta test and assessment specifications to update a certification to a later version of the same certification; otherwise, a device would undergo the full certification process required for the later certification. Major changes from one year to the next that would require a full recertification would be rare.

Infrequently, the ISASecure EDSA certification program will undergo significant modification at interim points within a year. For example, throughout 2010, as part of the ramp-up of the certification program, CRT for a number of protocols will come on line, which means a device would be certified with a designation such as ISASecure for Devices 2010.1, 2010.2, and so on.

The certification process will include determination by ISCI of the yearly and interim certification updates for which a vendor certification refresh is recommended. For example, consider the situation that in mid-2011 wireless protocols are added to communication robustness testing. Devices that have ISASecure for Devices 2010 certification still retain that certification. At their option, and based on marketplace demand, a vendor may opt to upgrade its certification to test its wireless capability as required to obtain ISASecure for Devices 2011 certification.

13. How will ISCI protect proprietary information required for the certification assessments?

Part of the ISCI accreditation process for certifiers will examine their process for protecting proprietary information of certification applicants. This information will be available only to the certifier and only on a need-to-know basis to those personnel involved in certification activities. The ISCI organization itself will not have access to the proprietary information of certification applicants.

About ASCI and the ISA Security Compliance Institute

The Automation Standards Compliance Institute (ASCI) is a non-profit organization incorporated by the International Society of Automation (ISA) in 2006 to provide a home for certification, conformance, and compliance assessment activities in the automation arena. ASCI extends the work that ISA has conducted for over 50 years in standards development by facilitating the effective implementation of automation industry standards. ISA provides professional management services to ASCI, drawing on an experienced staffing, financial, and administrative infrastructure.

The ISA Security Compliance Institute (ISCI) functions as an operational group within ASCI. ASCI bylaws share the open constructs of ISA while accounting for compliance organization requirements. Operating the ISCI within ASCI allows the organization to efficiently leverage the organizational infrastructure of ASCI.

For more information about the ISA Security Compliance Institute, visit **www.ISASecure.org**.

How to Join the ISA Security Compliance Institute
Interested organizations and individuals may join at any time. Please feel free to contact us for more details using the contact information below.

Membership application forms, including member fees and mailing instructions, are available for download at **www.ISASecure.org**.

Contact Information
Andre Ristaino
Managing Director, Automation Standards Compliance Institute

Direct 919-990-9222
Fax 919-549-8288
Email aristaino@isa.org
www.ISASecure.org

ISA **Security Compliance Institute**

67 Alexander Drive
PO Box 12277
Research Triangle Park, NC 27709

Copyright © 2010
ASCI - Automation Standards Compliance Institute
All rights reserved.