



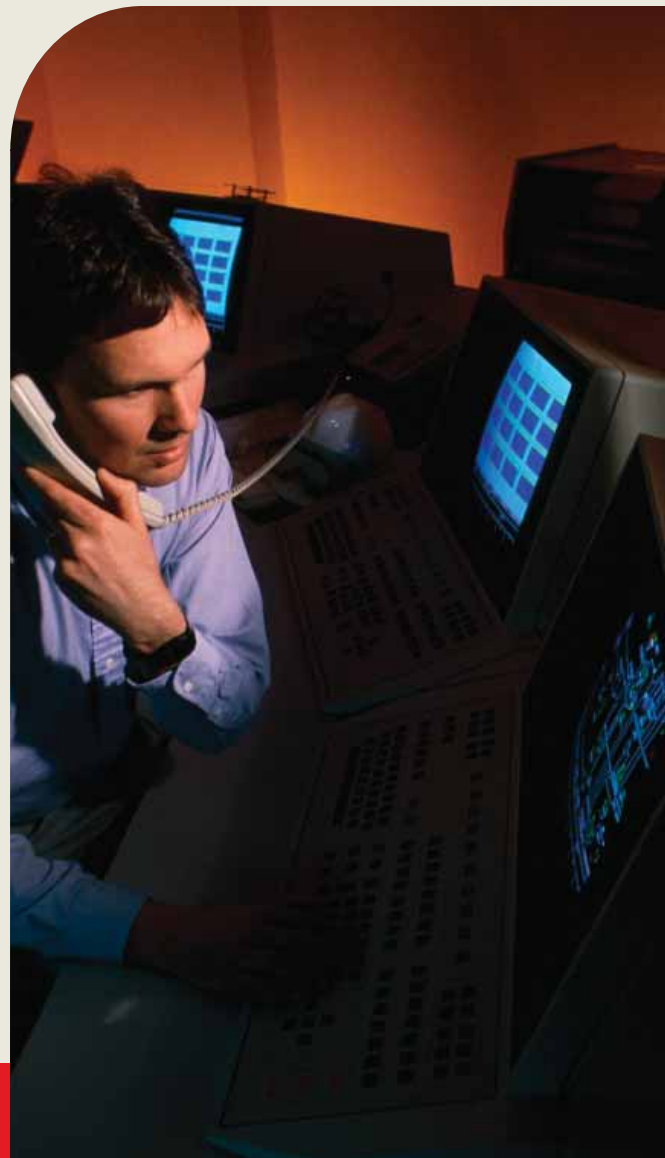
**ISA Security
Compliance Institute**

**ISASecure Embedded Device
Security Assurance Certification**

Introduction

This document provides an overview of the ISASecure certification program for embedded devices. 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, DCS controllers, and remote terminal units.

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.



The 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 certification level. Figure 1 illustrates this concept. The remainder of this document further describes the three technical elements of certification, certification levels, and the certification program.

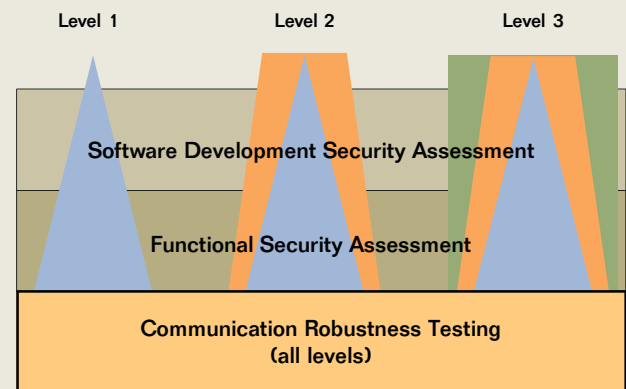


Figure 1 - Structure of ISASecure Embedded Device Certifications

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 effort underway for embedded device cyber security requirements. When the ISA-99.04.01 standard is completed, the ISASecure Embedded Device certification will be updated to serve as a compliance program for that standard.

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

The ISCI web page www.isa.org/isasecure describes how to participate in this organization and ongoing effort.

Technical Certification Elements

For all levels of ISASecure 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. Finally, 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 the 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 an 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 an SDSA apply at all certification levels and become more rigorous at higher certification levels. For example, ISASecure embedded devices at all certification levels will have documented security requirements with a specified content scope. As a second example, 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. 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 response(s), or failure of the device to continue to adequately maintain essential services, demonstrates potential security vulnerabilities within the device. Communication robustness testing does not examine the correctness of implementations or conformance to mandatory provisions of the controlling protocol standard(s).

Thus a key definition in ISASecure communication robustness

testing 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 set points), *and process alarms*. To pass the ISASecure communication robustness tests, the process control/safety loop must be maintained under all network traffic conditions. However, 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: *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 communication robustness test specifications for the protocols in the table below, where the groups of protocols are arranged by priority, with Group 1 being highest priority. Tests for Group 1 protocols will be available for certifications in Q1 2010 at rollout of the certification program.

Group 1 (1Q 2010)	Group 2 (3Q 2010)	Group 3 (4Q 2010)	Group 4 (Future)	Group 5 (Future)
<ul style="list-style-type: none"> • IEEE 802.3 (Ethernet) • ARP • IPv4 • ICMPv4 • TCP • UDP 	<ul style="list-style-type: none"> • BOOTP • DHCP • DNS • NTP, SNTP • FTP, TFTP • HTTP • SNMPv1-2 • Telnet 	<ul style="list-style-type: none"> • HTTPS • TLS • Modbus/TCP 	<ul style="list-style-type: none"> • IPv6 • OPC • Ethernet/IP/CIP • PROFINET • FFHSE • Selected wireless protocols/stacks with elements such as: IEEE 802.11 ISA100.11a WirelessHART 	<ul style="list-style-type: none"> • 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 certification levels.

Frequently Asked Questions

1. *Who 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. The Institute 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.

The Institute's goals are realized through industry standards compliance programs, education, technical support, and improvements in suppliers' development processes and users' life cycle management practices. ISCI membership is open to all interested organizations and individuals. For more information, visit www.isa.org/isasecure.

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

ISCI will accredit private organizations (called "certifiers") to perform ISASecure 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 certifications?*

ISCI grants accredited certifiers the right to grant ISASecure 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.

4. *Describe the ISASecure certifications that will be available in 1Q 2010.*

In the fourth quarter of 2009, accredited certifiers will be prepared to accept applications for ISASecure for Devices 2010 certification. The certification will include all three certification elements: software development security assessment, functional security assessment, and communication robustness testing. Communication robustness testing will include testing for the Group 1 protocols as shown in Table 1.

5. *How were the ISASecure 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 SFA criteria are aligned wherever possible with draft work products of the ISA99 committee. The Software Development Security Assessment requirements are ultimately traceable to requirements in the following source documents:

Reference Sources for Software Development Security Assessment	
ISO/IEC 15408-1 through 15408-3	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 Functional Security Assessment 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 15408-3	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 certification will not ensure compliance with the above standards. ISASecure certification criteria were selected from these sources and refined by working groups of experts based upon application and importance to embedded device security.

The communication robustness test 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 certification criteria were reviewed and approved by both the ISCI membership and an external technical subject matter expert.

6. How does the ISASecure program address proprietary protocols?

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

7. How does the ISASecure program address wireless capabilities?

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 certification. The initial ISASecure certification will not apply to the wireless capabilities of embedded devices.

8. How does the ISASecure program address IPv6?

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

9. How are ISASecure 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 certification levels and ISA99 security assurance levels, although an effort has been made to align ISASecure levels with current ISA99 thinking. As the definitions for ISA99 security assurance levels are further developed, we 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 is 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 need to repeat these tests under the ISASecure program?

No. ISCI will be working with interested existing certification vendors to create “delta” certification programs. Such a program would include those tests and assessments required to meet ISASecure requirements for communication robustness, functional security and software development that are not already covered by the existing certification program.

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 and SDSA topic areas.

For the CRT, recertification will be based on discussion with the certifier using well defined criteria to establish whether:

- All tests must be rerun on the new device to certify it
- No retesting is needed in order to support recertification

For the SFA 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 ISASecure changes the 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 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 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. Thus 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 those yearly and interim updates for certifications for which a vendor certification refresh is recommended. For example, consider the situation that in mid 2011 wireless protocols are added communication robustness testing. Devices that have ISASecure for Devices 2010 certification still retain that certification. At their option, and based on marketplace demand, they may opt to upgrade their certification to test their wireless capability as required to obtain ISASecure for Devices 2011 certification.

13. How will the program 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 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 done for 50 years in standards development by facilitating the effective implementation of automation industry standards. ISA provides professional management services to ASCI drawing on the extensive staffing, financial, and administrative infrastructure.

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

For more information about ISCI, including key staff engaged in this initiative, visit: <http://www.isa.org/isasecure>.

How to Join

Contact us for more information on this prospectus. Interested organizations may join at any time.

Membership application forms, showing member fees and mailing instructions, are available for download at <http://www.isa.org/ISASecure/join>.

Contact Information

Andre Ristaino

Managing Director, Automation Standards Compliance Institute



67 Alexander Drive
PO Box 12277

Research Triangle Park, NC 27709

Direct (919)-990-9222

Fax (919)-549-8288

Email aristaino@isa.org

www.isa.org/isasecure

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