EDSA-300

ISA Security Compliance Institute — Embedded Device Security Assurance –

ISASecure certification requirements

Version 2.0

June 2010

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

Revision history

version	date	author	changes
2.0	2010.06.06	C. Muehrcke	Initial version published to http://www.ISASecure.org

Contents

1 Scope 4

2 Normative references 4

3 Definitions and abbreviations 5

3.1 Definitions 5

3.2 Abbreviations 6

4 Background 6

5 Certification requirements 7

5.1 Certification level and version 7

5.2 Initial certification 8

5.3 Maintenance of certification 8

Requirement ISASecure_ED.R1 – Application for a certification level 7

Requirement ISASecure_ED.R2 – Prior certifications 7

Requirement ISASecure_ED.R3 – Publication of embedded device certification status 8

Requirement ISASecure_ED.R4 – ISASecure application requirements for an initial certification 8

Requirement ISASecure_ED.R5 – Criteria for granting an initial certification 8

Requirement ISASecure_ED.R6 – Consideration for prior SDSA 8

Foreword

NOTE This is one of a series of documents that defines ISASecure certification for embedded devices, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This specification is the overarching document in the series that describes technical requirements for certification. It references all other documents that contain these requirements and places them in context. The current list of documents related to ISASecure embedded device security assurance can be found on the web site http://www.ISASecure.org.

1 Scope

This document specifies the criteria for granting an initial ISASecure EDSA (Embedded Device Security Assurance) certification for an embedded device. A product is considered to be an embedded device if it satisfies the definition provided in 3.1.3. To specify these certification criteria, this document references other specification documents that cover detailed requirements for the three elements of certification:

- Communication robustness testing (CRT);
- Functional Security Assessment (FSA); and
- Software Development Security Assessment (SDSA).

CRT examines the capability of the device to adequately maintain essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks. 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, the SDSA examines the process under which the device was developed.

Once initial certification for a device is achieved, then under specified conditions this certification may be used as partial evidence toward a new certification for a modified device, or toward a certification of the device to a later version of the ISASecure criteria. This document provides an overview of the extent to which a previous certification can be applied in these cases, and when a new initial certification is required. The separate document [EDSA-301] provides further information on this topic.

2 Normative references

NOTE 1 The following specifications define the CRT element of the ISASecure embedded device certification. The overarching document [EDSA-310] contains references to the protocol-specific documents listed after it. These are maintained here as normative references rather than in [EDSA-310], in order to provide one place where all ISASecure technical specifications are listed.

NOTE 2 Although the following specifications include forward looking requirements for testing protocols over IPv6, neither IPv6 nor protocols running over IPv6 are tested or certified by ISASecure EDSA CRT at this time.

[EDSA-310] *ISA Security Compliance Institute Embedded Device Security Assurance – Common requirements for communication robustness testing of IP based protocol implementations,* as specified at http://www.ISASecure.org

[EDSA-401] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols,* as specified at http://www.ISASecure.org.

[EDSA-402] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4,* as specified at http://www.ISASecure.org

[EDSA-403] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-404] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-405] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org.

[EDSA-406] *ISA Security Compliance Institute Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

NOTE 3 The following specifications define the FSA and SDSA elements of the ISASecure embedded device certification, respectively.

[EDSA-311] *ISA Security Compliance Institute Embedded Device Security Assurance – Functional security assessment,* as specified at http://www.ISASecure.org

[EDSA-312] *ISA Security Compliance Institute Embedded Device Security Assurance – Software development security assessment*, as specified at http://www.ISASecure.org

NOTE 4 The following specification defines requirements for maintaining ISASecure certification of an embedded device.

[EDSA-301] *ISA Security Compliance Institute Embedded Device Security Assurance – Maintenance of ISASecure certification,* as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

3.1.1
allocatable

able to be met by other components

NOTE As used here, refers to security capabilities capable of being met by other components in a device's architectural context, although not directly provided by the device itself.

3.1.2
certifier

an accredited organization with the authority to carry out ISASecure EDSA assessments and testing, and grant ISASecure EDSA certifications

3.1.3
embedded device

special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

3.1.4
essential services

specified subset of the services provided by a device that is agreed between the applicant for certification and the test lab, at the start of certification

NOTE As specified in [EDSA-310], essential services are a subset of the following 6 services: the process control/safety loop, process view, command, process alarms, provide essential history data and peer-to-peer control communication. The first four of these are always considered essential services.

3.1.5
independent test

for the FSA and SDSA, requirement items whose validation requires the certifier's exercise of the embedded device itself, or exercise of a software development tool used by the device vendor

NOTE In contrast, some items may be validated by an examination of documents alone. This is true for most items in the SDSA.

initial certification
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of the embedded device or of any prior versions of the device

3.1.6
ISASecure version
identifier for the ISASecure certification criteria in force at a particular point in time, denoted using a year, followed by a period and a release number

NOTE An example is ISASecure EDSA 2010.2. An ISASecure version will map to document versions of the ISASecure technical specifications that define the technical criteria for certification.

3.1.7
supported
security functionality provided by the embedded device itself (vs. functionality allocated to entities in the device's environment)

NOTE This is in contrast to *allocatable* as defined above.

3.2 Abbreviations

The following abbreviations are used in this document

ASCI	Automation Standards Compliance Institute
ARP	address resolution protocol
CRT	communication robustness testing
ED	embedded device
EDSA	embedded device security assurance
FSA	functional security assessment
IACS	industrial automation and control system
IETF	Internet engineering task force
ICMP	Internet control message protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet (network layer) protocol
IPv4	IP version 4 (uses 32-bit network layer addresses)
IPv6	IP version 6 (uses 128-bit network layer addresses)
MAC	media access control sub-layer of the data link layer
ISCI	ISA Security Compliance Institute
SDSA	software development security assessment
TCP	transmission control protocol
UDP	user datagram protocol

4 Background

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). ISASecure EDSA certification 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 EDSA Level 1, ISASecure EDSA Level 2 and ISASecure EDSA Level 3.

All levels of certification include the three certification elements defined in Clause 1. 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.

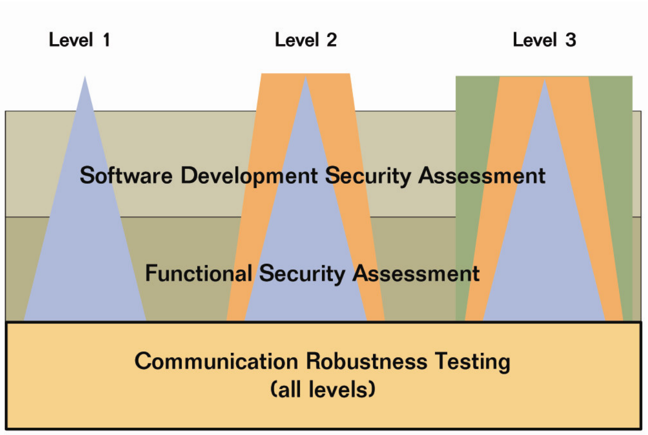
Level 1
Level 2
Level 3
Software Development Security Assessment
Functional Security Assessment
Communication Robustness Testing
(all levels)

Figure 1 - Structure of ISASecure Embedded Device Certifications

ASCI (Automation Standards Compliance Institute) will accredit private organizations to perform ISASecure certification evaluations as “certifiers”. ASCI will also recognize test tools designed to perform communication robustness testing for use by these organizations for CRT and by device vendors in preparation for certification.

NOTE ISCI is organized under the umbrella structure provided by ASCI.

ASCI grants accredited certifiers the right to grant ISASecure certifications for devices based upon the certifier’s tests and assessments conforming to ISASecure specifications listed in Clause 2. ISCI will publish a list of certified products on its website.

5 Certification requirements

5.1 Certification level and version

Requirement ISASecure_ED.R1 – Application for a certification level

When a device vendor applies for certification of an embedded device, the certification applicant SHALL specify the maximum level for which they would like to achieve device certification. The levels possible are 1, 2, or 3. The certifier SHALL award certification to a device at the highest level less than or equal to this maximum level for which the device qualifies, without requiring the device vendor to reapply for certification.

Requirement ISASecure_ED.R2 – Prior certifications

When applying for ISASecure certification of an embedded device, the applicant SHALL specify one of:

- this is an initial certification
- this device or an earlier version has achieved an ISASecure certification, which is offered as evidence toward this certification.

NOTE As discussed in 5.3, if the certifier agrees that evidence from the earlier certification may be applicable to the new certification, an assessment is performed to determine the extent to which this evidence is applicable.

Requirement ISASecure_ED.R3 – Publication of embedded device certification status

ISCI, the certifier, and the device vendor SHALL publish certification status information for certified devices in a public venue. Information provided SHALL include the most granular version identifier of the device to which the ISASecure EDSA certification applies, and the version of the certification achieved, designated by the year and release, such as ISASecure EDSA 2010.2.

5.2 Initial certification

Requirement ISASecure_ED.R4 – ISASecure application requirements for an initial certification

Items specified as follows SHALL be submitted to the ISASecure EDSA certification process by an applicant for an initial certification:

a) technical items as required by the specifications listed in Clause 2; and

b) administrative and potentially additional technical items defined by the certifier.

[EDSA-310] defines requirements on a certifier for carrying out CRT, and criteria for passing this element of the certification. [EDSA-311] and [EDSA-312] contain lists of requirements on an embedded device and device development process that a certifier must assess for the FSA and SDSA, respectively. Validation activities for compliance with these requirements include documentation review and in some cases, independent test.

Requirement ISASecure_ED.R5 – Criteria for granting an initial certification

An initial ISASecure EDSA certification for level *n* SHALL be granted for an embedded device if:

- for all levels, the CRT pass criteria are met as defined in [EDSA-310];
- all FSA criteria in [EDSA-311] applicable to level *n* are assessed as either supported or allocatable; and
- all SDSA criteria in [EDSA-312] applicable to level *n* are assessed as pass.

Requirement ISASecure_ED.R6 – Consideration for prior SDSA

A certifier SHALL consider the applicability of SDSA evaluation evidence and results for a certified device, to certifications for any later devices from the same organization.

5.3 Maintenance of certification

5.3.1 Relevant scenarios

As an illustrative example, consider the scenario in which a vendor has achieved ISASecure EDSA 2010.1 Level 1 certification on device version 136.1.3. That device version retains that certification indefinitely. However, once the device is upgraded to version 136.1.4, this new device is not certified unless the vendor takes specific action to maintain the certification. Further, when ISASecure upgrades its certification program in 2011, neither device will be certified under the new ISASecure EDSA 2011.1 program, without action by the vendor.

A device vendor is not *required* to obtain an embedded device certification for every field patch and new release of a device, to every new version of ISASecure EDSA. The decision to obtain a particular certification is ultimately an optimization made by the vendor, considering end customer requirements and certification cost to the vendor. However, the device vendor is required to clearly communicate to the marketplace which version of their device meets the ISASecure criteria, and which version of the criteria it meets, per Requirement ISASecure_ED.R3.

5.3.2 Device modification

In the above scenario, if the vendor decides to certify device version 136.1.4 to ISASecure EDSA 2010.1 Level 1, this requires at a minimum an analysis by the vendor of the changes in this release, which is reviewed by the certifier that provided the initial certification of version 136.1.3. If it is agreed there is no impact on the prior certification evaluation, then the new device version is registered as certified at the conclusion of this analysis. If the changes in 136.1.4 could have had an impact on the prior certification evaluation, then some portion or all of the certification evaluation will need to be carried out on version 136.1.4 in order for that version to be certified. The form of this analysis of changes and the criteria for determining what portions of the evaluation will need to be carried out on the new device are specified in [EDSA-301]. For significant changes to the device, a new initial certification will be required. Minor bug fixes will typically be found not to impact the prior certification evaluation. Note that Requirement ISASecure_ED.R6 permits reuse of a portion of the SDSA results from the prior certification.

5.3.3 Modified ISASecure EDSA criteria

The vendor might decide to certify device version 136.1.3 to ISASecure 2011.1 Level 1, because for example this version of ISASecure contains CRT tests for additional protocols supported by the device which the vendor's end customers would like to see certified. In this case, to obtain this certification, it will be sufficient for the certifier to carry out those tests and assessments in ISASecure 2011.1 Level 1 that are changed or new over 2010.1 Level 1. The specific definition for this incremental certification evaluation is found in [EDSA-301].

5.3.4 Device and certification criteria modified

If the vendor would like to certify device version 136.1.4 to ISASecure 2011.1 Level 1, then both the device and the certification criteria have changed. [EDSA-301] specifies that a combination of analysis of device changes and an incremental certification evaluation be applied in this case. A similar case described in that document is the certification of a previously certified device to a higher level than the certification previously obtained.