EDSA-300

ISA Security Compliance Institute — Embedded Device Security Assurance –

ISASecure® certification requirements

Version 2.8

December 2014

Revision history

version	date	changes
2.0	2010.06.06	Initial version published to http://www.ISASecure.org
2.8	2014.12.10	Add VIT, add ISASecure SDLA and SDA-E references, add figure for elements of certification and revise figure illustrating levels, remove 5.3 about maintenance of certification (redundant with EDSA-301), ERT.R3 revised, terminology updates: essential services to essential functions, device vendor to device supplier

Contents

Certification requirements

FOREWORD

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 elements of certification:

- Security Development Lifecycle Process Assessment (SDLPA);
- Security Development Artifacts for embedded devices (SDA-E);
- Functional Security Assessment for embedded devices (FSA-E); and
- Embedded device robustness testing (ERT).

While SDLPA is an evaluation of the embedded device supplier's security development lifecycle process, SDA-E examines the artifacts that are the outputs of that process for the embedded device to be certified. FSA-E 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.

ERT has two major elements - Vulnerability Identification Testing (VIT) and Communication Robustness Testing (CRT). VIT scans the device for the presence of known vulnerabilities. CRT examines the capability of the device to adequately maintain essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions).

The following figure illustrates the elements of ISASecure EDSA certification.

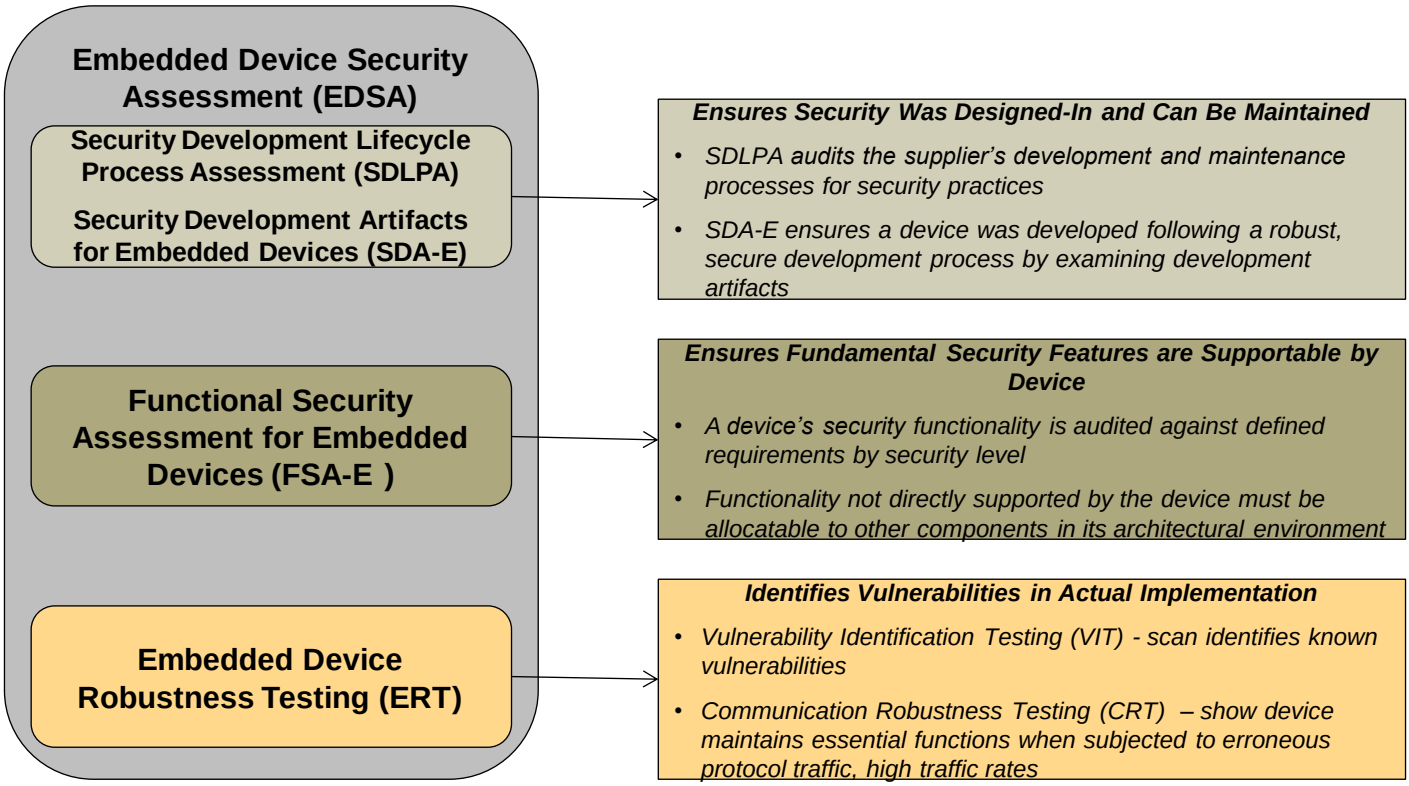

Figure 1 - Evaluation Elements for ISASecure EDSA Certification

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. The separate document [EDSA-301] *ISA Security Compliance Institute Embedded Device Security Assurance – Maintenance of ISASecure certification* addresses this topic.

2 Normative references

NOTE 1 The following specifications define the SDLPA and SDA-E elements of the ISASecure embedded device certification.

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment, as specified at* http://www.ISASecure.org

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme*, as specified at http://www.ISASecure.org

[EDSA-312] *ISA Security Compliance Institute Embedded Device Security Assurance – Security development artifacts for embedded devices*, as specified at http://www.ISASecure.org

NOTE 2 The following specification defines the FSA-E element of the ISASecure embedded device certification.

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

NOTE 3 The following specifications define the ERT element of the ISASecure embedded device certification. The overarching document [EDSA-310] contains references to the protocol-specific CRT documents and to the document describing VIT scanning policy, which are listed after it. The protocol-specific CRT documents 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 4 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 – Requirements for embedded device robustness testing,* 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

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*, 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
chartered laboratory, which is an organization that is qualified to certify products or supplier development processes as ISASecure

NOTE This term is used when a simpler term that indicates the role of a "chartered laboratory" is clearer in a particular context.

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 function
function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.

3.1.5
independent test
form of requirements validation that requires the certifier's exercise of the entity under evaluation itself, or exercise of a development tool used by the supplier of that entity

NOTE In contrast, some requirements may be validated by an examination of documents alone.

3.1.6
initial certification
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of a product under evaluation or of any of its prior versions

3.1.7
ISASecure version
identifier for the ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a three-place number, such as ISASecure EDSA 2.0.1

3.1.8
supported
provided by the entity under evaluation itself

NOTE This term is used when referring to security functionality. In particular, supported functionality need not be allocatable to external entities that exist in the environment of the entity under evaluation.

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
ERT	embedded device robustness testing
FSA-E	functional security assessment for embedded devices
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
SDA-E	security development artifacts for embedded devices
SDLA	security development lifecycle assurance
SDLPA	security development lifecycle process assessment
TCP	transmission control protocol
UDP	user datagram protocol
VIT	Vulnerability identification test

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 suppliers.

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 certification elements defined in Clause 1. The security development process assessment requirements for SDLPA and SDA-E increase in rigor for levels 2 and 3. This is also true for FSA-E and for VIT, since pass/fail criteria for VIT reference applicable FSA-E requirements. CRT criteria are the same regardless of certification level. Figure 2 illustrates this concept.

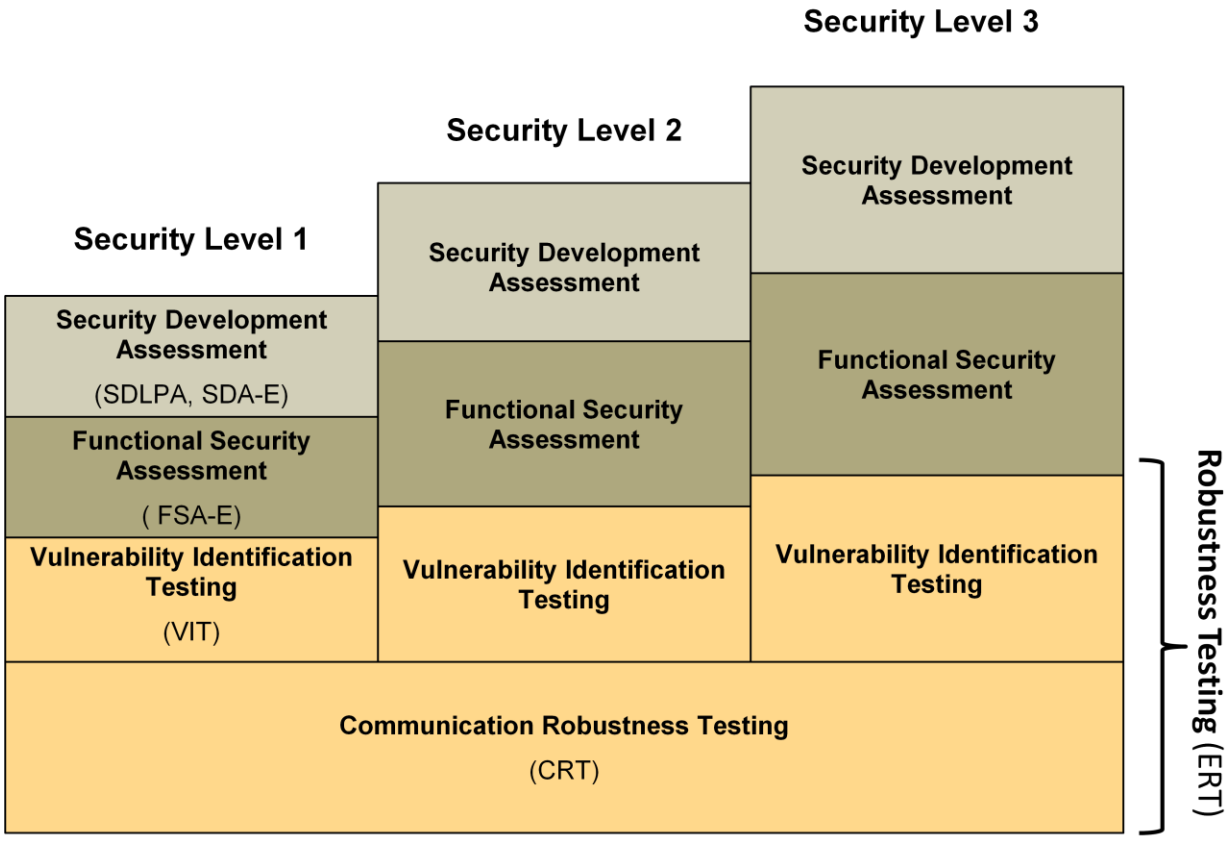

Figure 2 - Structure of ISASecure Embedded Device Certifications

NOTE 1 Currently other ISASecure certifications have four levels, while EDSA has only three possible certification levels defined at this time. Therefore SDLPA level 4 requirements as defined in [SDLA-312] are not currently applicable within the EDSA program. EDSA certification levels and criteria per level for FSA-E will be aligned with ISA 62443-4-2, once that standard is approved. Thus for example if the approved ISA-62443-4-2 defines four levels, EDSA certification will be modified to offer four levels.

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 suppliers in preparation for certification.

NOTE 2 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 supplier 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 for which the device qualifies, up to this maximum level.

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 Clause 1, the separate document [EDSA-301] defines certification criteria for the second case.

Requirement ISASecure_ED.R3 – Publication of embedded device certification status

If ISCI, the certifier, or the device supplier publishes 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, such as ISASecure EDSA 2.0.1.

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-312] contains lists of requirements on an embedded device development process that a certifier assesses for the SDLPA and SDA-E. [EDSA-311] contains the security functions list that is assessed for FSA-E. [EDSA-310] defines requirements on a certifier for carrying out ERT, and criteria for passing this element of the certification. Validation activities for compliance with these requirements include documentation review and independent test. The following requirement states the full set of criteria for EDSA certification, which relies upon these detailed specifications.

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 the following requirements are met, as defined in the reference documents shown:

Topic	Element	Requirement	Reference Document
Secure Development Processes Implemented by Supplier	SDLPA	The supplier holds an ISASecure SDLA certification, with SDLA certification level at or above level *n*. The embedded device is within the stated scope of the certified process, for development going forward. -OR- An SDLPA process evaluation is done as part of the EDSA evaluation and passes. In particular, all SDLPA criteria applicable for an SDLPA certification level at level *n*, are assessed as pass. The validation criteria are enumerated in the column labeled "Development Organization and SDL Validation Activity" in [SDLA-312].	[SDLA-100] [SDLA-300] [SDLA-312]
Secure Development Processes Applied to Embedded Device	SDA-E	The embedded device passes SDA-E, a review of security development artifacts, for level *n*.	[EDSA-312]
Security Functions of Embedded Device	FSA-E	All FSA-E criteria applicable to level *n* are assessed as either *supported* or *allocatable.*	[EDSA-311]
Embedded Device Robustness in Networked Environment	ERT	The system passes ERT, per the pass/fail criteria for level *n*.	[EDSA-310]

NOTE Regarding the second alternative for SDLPA, it is acceptable to apply for both SDLA and EDSA certifications at the same time. In effect, in this case, the supplier achieves, along with their embedded device product certification, a process certification that applies toward certifications for other products going forward.

Requirement ISASecure_ED.R6 – Consideration for prior SDLPA

A certifier SHALL consider evidence from prior ISASecure audits of a supplier's security development process, toward the SDLPA element of an EDSA certification.

NOTE For example, evidence from the SDLPA evaluation performed as part of an EDSA evaluation of an embedded device, is considered when a modified version of that device, or a completely different device model, is presented for certification.