EDSA-100

ISA Security Compliance Institute — Embedded Device Security Assurance –

ISASecure® certification scheme

Version 3.3

February 2018

Revision history

version	date	changes
1.1	2010.06.06	Initial version published to http://www.ISASecure.org
2.0	2011.10.21	Support CRT by separate organization, add EDSA-206 and EDSA-207
2.8	2014.12.10	Change from Guide 65 to 17065, doc structure revisions for VIT, incorporate ISASecure SDLA references, describe relationship to ISO/IEC 62443, terminology updates: essential services to essential functions, device vendor to device supplier, remove ISASecure-101 ISCI cert scheme operation document and ASCI 2009 document, unify all chartered lab contracts to become ISASecure-202
3.3	2018.02.13	Align with approved ANSI/ISA-62443-4-1 and IEC 62443-4-1 (EDSA 2.1.0)

Contents

1 Scope 5

2 Normative references 5

2.1 Accreditation/recognition 5

2.2 ISASecure symbol and certificates 5

2.3 Technical specifications 6

2.4 External references 7

3 Definitions and abbreviations 7

3.1 Definitions 7

3.2 Abbreviations 11

4 ISASecure EDSA certification program 11

4.1 Technical ISASecure EDSA evaluation criteria 11

4.2 Certified embedded devices 13

4.3 Relationship of the EDSA program to ISA 62443 13

4.4 Organizational roles 13

4.5 Certification program documentation 14

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 is the highest level document that describes the overall certification scheme and the scope for all other related documents. A description of the ISASecure program and the current list of documents related to ISASecure EDSA (Embedded Device Security Assurance), as well as other ISASecure certification programs, can be found on the web site http://www.ISASecure.org.

1 Scope

The ISASecure® certification 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). The ISCI ISASecure EDSA (embedded device security assurance) certification program 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. An embedded device that is certified to meet these requirements can display the ISASecure symbol.

This document provides an overview of the operation of the certification program, the roles of all organizations that participate in carrying out the program, and the documents that define these roles as well as the technical aspects of the program.

2 Normative references

NOTE Section 4.5 provides a diagrammatic and expository overview of the ISASecure EDSA documents and their relationships.

2.1 Accreditation/recognition

2.1.1 Chartered laboratory operations and accreditation

NOTE The following documents describe how to achieve chartered laboratory status and operate as an ISASecure EDSA certifier.

[EDSA-200] *ISCI Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[ISASecure-115] *ISCI ISASecure Certification Programs - Policy for transition to SDLA 2.0.0, EDSA 2.1.0 and SSA 2.1.0*

[ISASecure-202] *ISCI ISASecure Certification Programs – Application and Contract for Chartered Laboratories*, internal ISCI document

2.1.2 CRT laboratory operations and accreditation

NOTE The following documents describe how to achieve CRT laboratory status and operate as a laboratory recognized for ISASecure EDSA communication robustness testing.

[EDSA-206] *ISCI Embedded Device Security Assurance – ISASecure EDSA CRT laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[EDSA-207] *ISCI Embedded Device Security Assurance – Application and Contract for CRT Laboratories*, internal ISCI document

2.1.3 CRT tool recognition program

NOTE The following documents describe how to attain ISASecure EDSA recognition for a tool used to carry out communication robustness testing.

[EDSA-201] *ISCI Embedded Device Security Assurance –Recognition process for communication robustness testing tools,* as specified at http://www.ISASecure.org

[EDSA-203] *ISCI Embedded Device Security Assurance - Application and Contract for CRT Tool Recognition,* internal ISCI document

2.2 ISASecure symbol and certificates

NOTE The following documents describe the ISASecure symbol and certificates and how they are used.

[EDSA-204] *ISCI Embedded Device Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at http://www.ISASecure.org

[EDSA-205] *ISCI Embedded Device Security Assurance – Certificate Document Format,* as specified at http://www.ISASecure.org

2.3 Technical specifications

NOTE This section includes the specifications that define technical criteria for evaluating an embedded device for ISASecure EDSA certification.

2.3.1 General technical specifications

NOTE The following document is the overarching technical specification for ISASecure EDSA certification.

[EDSA-300] *ISCI Embedded Device Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

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

[EDSA-303] *ISASecure EDSA Sample Report*, available on request to ISCI

2.3.2 Specifications for certification elements

NOTE 1 The following document provides the technical evaluation criteria for the Embedded Device Robustness Testing (ERT) element of an EDSA evaluation. ERT includes vulnerability identification test (VIT) and communication robustness test (CRT).

[EDSA-310] *ISCI Embedded Device Security Assurance – Requirements for embedded device robustness testing,* as specified at http://www.ISASecure.org

NOTE 2 The following documents provide the technical evaluation criteria for the Functional Security Assessment element of an EDSA evaluation.

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

NOTE 3 The following documents provide the overall technical evaluation criteria for the Security Development Artifacts element of an EDSA product evaluation. [SDLA-312] also provides the technical evaluation criteria for an ISASecure assessment of a supplier's security development lifecycle process.

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

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

NOTE 4 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier security development lifecycle processes.

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

2.3.3 Vulnerability identification testing specifications

NOTE The following document describes the policy parameter values used to perform VIT. VIT is a sub element of Embedded Device Robustness Testing.

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*, as specified at http://www.ISASecure.org

2.3.4 CRT specifications

NOTE These protocol-specific ISASecure EDSA technical CRT specifications refer to [EDSA-310] for requirements that are common across all protocols.

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

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

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

[EDSA-405] *ISCI 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] *ISCI 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

2.4 External references

External references are documents that are maintained outside of the ISASecure EDSA program and are used by the program.

2.4.1 IACS security standards

NOTE Section 4.3 describes the relationship of ISASecure EDSA to these approved standards as well as to ISA 62443 series standards under development.

[ANSI/ISA-62443-1-1] ANSI/ISA-62443-1-1 *(99.01.01)-2007 Security for industrial automation and control systems Part 1-1: Terminology, concepts and models*

[ANSI/ISA-62443-4-1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[IEC 62443-4-1] IEC 62443-4-1:*2018 Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

2.4.2 International standards for certification programs

NOTE The following international standards apply to the ISASecure EDSA certification and testing processes.

[ISO/IEC 17065] ISO/IEC 17065, "*Conformity assessment - Requirements for bodies certifying products, processes, and services*", September 15, 2012

[ISO/IEC 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories*", 15 May 2005

2.4.3 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure EDSA chartered laboratory and CRT laboratory accreditation processes.

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", 01 September 2004

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
for ISASecure certification programs, assessment and recognition process via which an organization is granted chartered laboratory or CRT laboratory status

3.1.2
accreditation body
third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment

3.1.3
artifact
tangible output from the application of a specified method that provides evidence of its application

NOTE Examples of artifacts for secure development methods are a threat model document, a security requirements document, meeting minutes, internal test results

3.1.4
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.5
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.

3.1.6
certificate
document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

NOTE For ISASecure EDSA, there are certificates for certified devices, recognized CRT tools, chartered laboratories, CRT laboratories.

3.1.7
certification
third party attestation related to products, processes, or persons that conveys assurance that specified requirements have been demonstrated

NOTE Here, this refers to either a successful authorized evaluation of a product or a process to ISASecure criteria. This outcome permits the product supplier or organization performing the process to advertise this achievement in accordance with certification program guidelines.

3.1.8
certification scheme
overall definition of and process for operating a certification program

3.1.9
certification level
number associated with a particular certification granted, where requirements to achieve that certification increase in rigor for higher levels

NOTE It is intended that a product that achieves EDSA certification level *n* will meet requirements for capability security level *n* as defined in ISA-62443-4-2 *Security for industrial automation and control systems - Part 4-2:Technical security requirements for IACS components*. Once the ISA-62443-4-2 standard is approved, EDSA program certification levels will be aligned with capability security levels in that standard.

3.1.10
certified device
well-defined version of an embedded device that has undergone an evaluation by a chartered laboratory, has met the ISASecure EDSA criteria and has been granted certified status by the chartered laboratory

3.1.11
chartered laboratory
organization chartered by ASCI to evaluate products or development processes under one or more ISASecure certification programs and to grant certifications under one or more of these programs

NOTE A chartered laboratory is the conformity assessment body for the ISASecure certification programs.

3.1.12
communication robustness testing
tests that determine the extent to which a device maintains its essential functions under adverse network traffic conditions

3.1.13
conformity assessment
demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

3.1.14
conformity assessment body
body that performs conformity assessment services and that can be the object of accreditation

NOTE This is an ISO/IEC term and concept. For ISASecure EDSA, the conformity assessment body is a chartered laboratory.

3.1.15
CRT laboratory
organization authorized by ASCI to perform communication robustness testing for embedded devices and submit results to a chartered laboratory as evidence toward ISASecure certification

3.1.16
CRT tool supplier
provider of a test tool to support communication robustness testing

3.1.17
device supplier
organization that is responsible for compliance of an embedded device with ISASecure requirements

3.1.18
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.

3.1.19
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.

3.1.20
end user
organization that purchases, uses or is impacted by the security of embedded devices

3.1.21
“Ethernet”
IEEE802.3 as Ethernet II or IEEE 802.3 Type 1 plus IEEE 802 SNAP

3.1.22
functional security assessment
assessment of a defined list of security features for a control system, embedded device or other control system component

3.1.23
pass
meet the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.24
provisional chartered status
interim, temporary recognition status during which a chartered laboratory is authorized to perform evaluations and grant ISASecure certifications

NOTE ISCI grants provisional chartered status for ISASecure EDSA when an EDSA accreditation body has assessed all requirements as passing, but has not yet formalized the accreditation of the chartered laboratory.

3.1.25
recognized CRT tool
test tool that has been evaluated by ISCI and determined to meet applicable requirements for carrying out ISASecure communication robustness testing as required for the EDSA and SSA certification programs

3.1.26
security development artifacts
assessment of artifacts that demonstrates that secure development and maintenance methods have been applied to a particular product

NOTE In some cases these artifacts will be created during an organization's transition to a secure development process, for products which predate that process, but will be maintained under it going forward.

3.1.27
security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

NOTE Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.28
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is "mark."

3.1.29
version (of embedded device)
well defined release of an embedded device, typically identified by a release number

3.1.30
version (of ISASecure certification)
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 2.1.0

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
ARP	address resolution protocol
CRT	communication robustness testing
ERT	embedded device robustness testing
EDSA	embedded device security assurance
FSA-E	functional security assessment for embedded devices
IACS	industrial automation and control system(s)
IETF	Internet engineering task force
IAF	International Accreditation Forum
ICMPv4	internet control message protocol version 4
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IPv4	internet protocol version 4
ILAC	International Laboratory Accreditation Cooperation
ISA99	ISA committee developing the S99 standard for IACS security
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
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 ISASecure EDSA certification program

4.1 Technical ISASecure EDSA evaluation criteria

ISASecure EDSA is a certification program for embedded devices, where a product is considered to be an embedded device if it satisfies the definition provided in 3.1.18. The elements of an EDSA certification are illustrated in Figure 1 below.

In order to obtain ISASecure EDSA certification, a supplier must pass a security development lifecycle process assessment (SDLPA). This evaluation may be performed as part of the EDSA evaluation, or may have been completed previously if the supplier holds an ISASecure SDLA process certification, as described in [SDLA-100]. A supplier may at their option apply for EDSA and SDLA certification in parallel. ISASecure certification of embedded devices has three additional elements:

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

SDLPA and SDA-E both assess development process, hence are grouped under "Security Development Assessment" in Figure 1 below. SDA-E examines the artifacts that are the outputs of the supplier's security development processes as they apply to 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 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 above. The SDLPA and SDA-S assessments are the same for all certification levels with the exception of allowable residual risk for known security issues. FSA-E and VIT increase in rigor for levels greater than 1; pass/fail criteria for VIT reference applicable FSA-E requirements. CRT criteria are the same regardless of certification level. Figure 1 illustrates this concept.

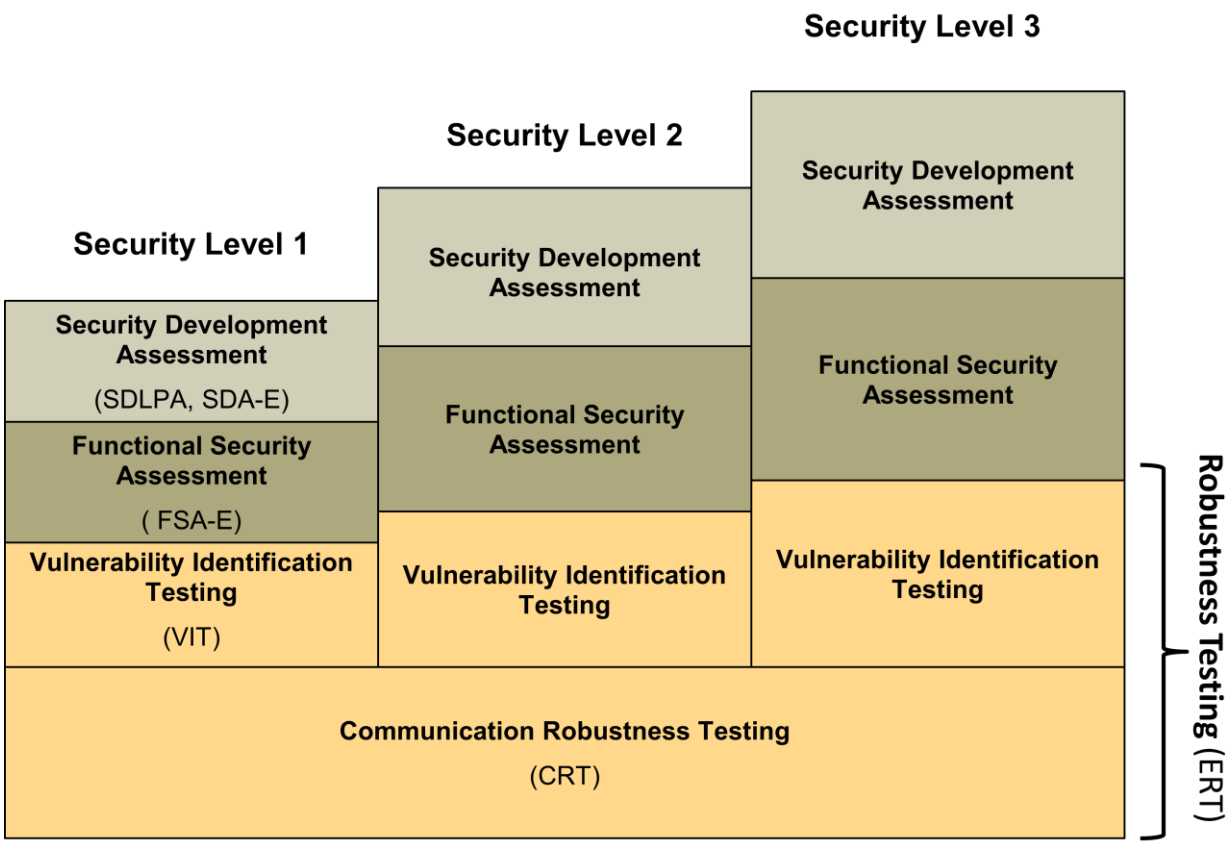

Figure 1 - Structure of EDSA Certification

NOTE 1 In SDLA-312 v4.52, the treatment of residual risk related to known security issues is found in SDLA requirement SDLA-DM-4.

NOTE 2 Currently the ISASecure SSA certification has four levels, while EDSA has only three possible certification levels defined at this time. As noted in Section 4.3, EDSA requirements and certification levels for FSA-E will be aligned with ISA-62443-4-2

requirements and capability security levels, once that standard is approved. Thus since it is expected that the approved ISA-62443-4-2 will have four levels, EDSA certification will be modified to offer four corresponding certification levels.

4.2 Certified embedded devices

The supplier for an embedded device that has been evaluated under the ISASecure EDSA certification program and shown to meet these technical criteria may display the ISASecure symbol and a certificate granting certification, in accordance with program procedures. Certification applies to a particular version of an embedded device, and references a 3-digit certification version that identifies the set of ISASecure specifications used for the certification. For example, device model 234, version 1.9 might be certified to ISASecure EDSA 2.1.0 Level 1. The program defines procedures to maintain certification for the next version of the device, to later versions of the ISASecure EDSA evaluation program and to higher certification levels.

Subject to permission of each device supplier, ISCI will post the names of certified devices on its web site http://www.ISASecure.org.

4.3 Relationship of the EDSA program to ISA 62443

A goal for the EDSA certification program is to offer a compliance program for the ISA 62443 series of standards. ISA 62443 standards address security for IACS. ISASecure EDSA certification incorporates requirements that apply to an embedded device, which is one type of component of an IACS.

It is the intent that the ISASecure program align terminology, concepts and reference architectures with those used by the ISA 62443 effort, in particular as presented in [ANSI/ISA-62443-1-1]. Definitions for terms are found on the ISA 99 wiki at http://isa99.isa.org/ISA99%20Wiki/Master-Glossary.aspx and will be published in the technical report currently under development: “ISA TR 62443-1-2 Security for industrial automation and control systems - Master glossary of terms and abbreviations."

The ISASecure SDLPA and SDA-E security development requirements for ISASecure EDSA align with the requirements in the approved standard “ANSI/ISA-62443-4-1 Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements.” The IEC has separately approved this standard as [IEC 62443-4-1].

In the future, the ISASecure EDSA FSA-E requirements and certification levels will be aligned with the requirements and capability security levels in the approved standard "ISA-62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components.”

4.4 Organizational roles

The following organizations participate in the ISASecure EDSA program. A term in parentheses following a description indicates the term used for this role in [ISO/IEC 17065].

- **End users** define procurement criteria for embedded devices, and may require an ISASecure certification for a device, to a particular level
- **Device suppliers** apply for certification of their embedded devices (supplier)
- **Chartered laboratories** for the EDSA program accept applications from device suppliers for device certification, evaluate devices, and are authorized to grant device certifications to device suppliers (conformity assessment body)
- **CRT laboratories** may test embedded devices to the CRT requirements and submit results to chartered laboratories as evidence toward an ISASecure EDSA certification
- **CRT tool suppliers** provide test tools that allow chartered laboratories or CRT laboratories to carry out CRT, and allow device suppliers to test their devices in advance of formal evaluation for certification
- **ISCI** defines, maintains and manages the ISASecure certification programs, including ISASecure EDSA, grants recognition to qualified CRT tools, interprets the ISASecure specifications and maintains a web

site for publishing program documentation, as well as lists of chartered ISASecure laboratories, CRT laboratories, recognized CRT tools, ISASecure certified products and ISASecure certified supplier development processes

- **ASCI**, as the legal entity representing ISCI, grants chartered laboratory status or CRT laboratory status to applicant organizations based on successful accreditation to criteria defined by ISCI

- **EDSA accreditation bodies** evaluate candidates for chartered laboratory status or CRT laboratory status and determine if they meet program accreditation criteria (accreditation body)

Note that either a chartered laboratory or a CRT laboratory may perform CRT for an embedded device evaluation. In either case, a chartered laboratory is the entity that grants an ISASecure EDSA certification. An organization may perform either one or both of the roles CRT tool supplier and CRT laboratory.

ISCI is organized as an interest area within ASCI (Automation Standards Compliance Institute), a not-for-profit 503 (c) (6) corporation owned by ISA. Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: http://www.ISASecure.org.

An EDSA accreditation body will be an organization recognized by IAF/ILAC.

Information related to device evaluations is private to chartered laboratories or CRT laboratories performing these evaluations, and is not disclosed to ASCI/ISCI, except as explicitly permitted by the device supplier or for cause in ASCI/ISCI's role as manager of the certification program.

4.5 Certification program documentation

4.5.1 Overview of documentation

Figure 2 shows the documents that define the ISASecure EDSA certification program. An arrow represents a referential dependency of a document on the contents of another document. Refer to Section 2 for the detailed bibliographic listing of these documents.

NOTE 1 [EDSA-200], [EDSA-201] and [EDSA-206] contain references to all related technical specifications. To retain readability, these references are not shown as arrows in the figure.

NOTE 2 The figure depicts all documents in Section 2 with the exception of the application forms [ISASecure-202], [EDSA-203] and [EDSA-207] , the certificate format document [EDSA-205], and the policy document [ISASecure-115] regarding transition from the prior SDLPA and SDA-E assessment requirements for EDSA, to the assessment aligned with [ANSI/ISA-62443-4-1] in [SLDA-312].

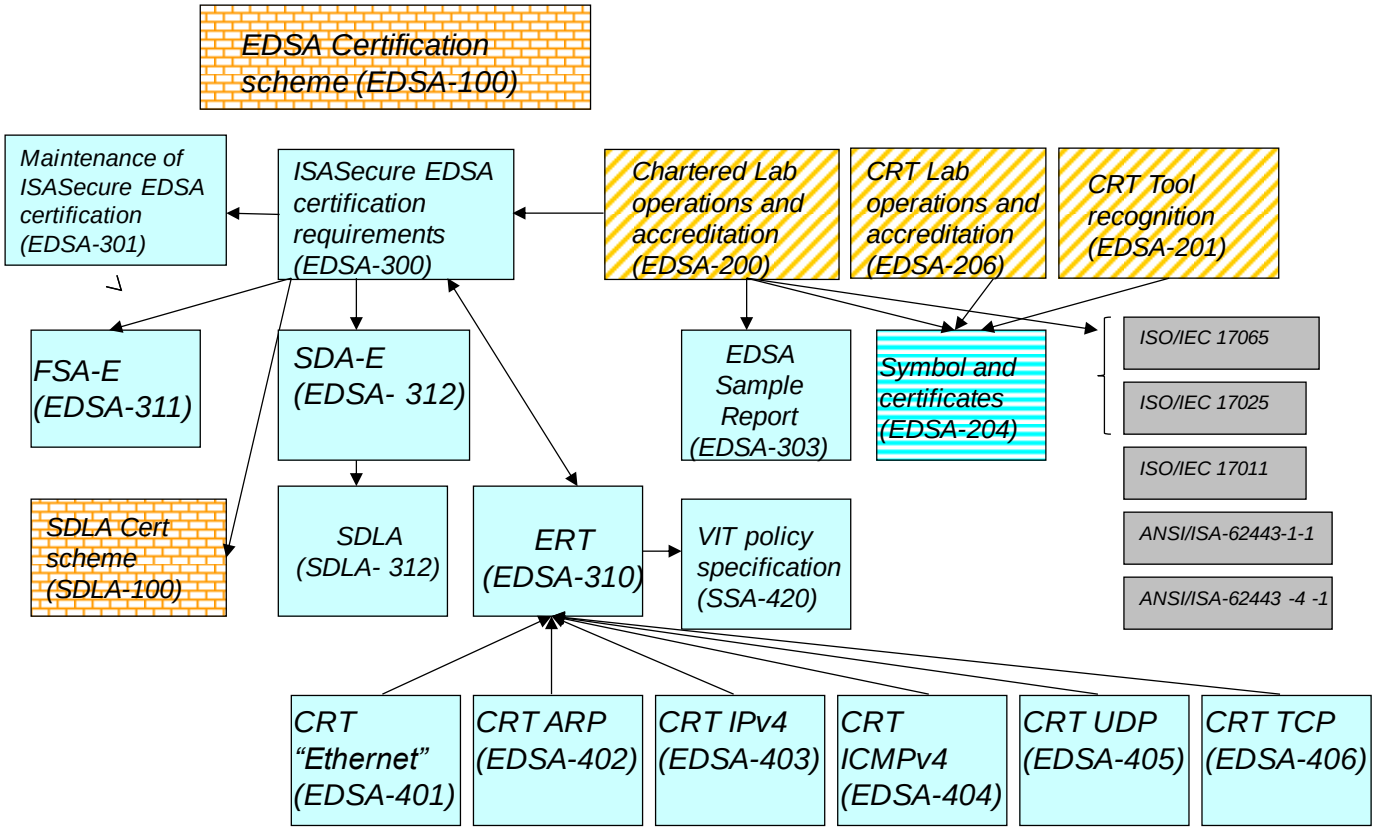

Figure 2 - ISASecure EDSA Documents

There are five major categories of ISASecure EDSA program documents:

- **Technical specifications**, shown with no pattern in light blue, that describe the technical criteria applied to determine whether a device will be certified
- **Accreditation/recognition**, shown in gold diagonal stripe, that describe how an organization can become a chartered or CRT laboratory, and how a tool supplier can obtain recognition for a CRT tool
- **Symbol and certificates**, shown in blue horizontal stripe, covers the topic of proper usage of the ISASecure symbol and certificates
- **Structure,** shown in an orange brick pattern, used to describe and operate the overall program. The present document falls in this category.
- **External references**, shown with no pattern in dark grey, are documents that apply to the ISASecure program but are maintained outside of the program.

The documents with prefixes "SSA" and "SDLA" are used both by those certification programs, respectively, as well as the EDSA program. The following sections describe the documents in each category in further detail.

4.5.2 Technical specifications

The brief document [EDSA-300] *ISCI EDSA - ISASecure Certification Requirements,* defines at a high level the criteria for embedded device certification, which simply stated, are for the device supplier's development

organization to pass an ISASecure SDLPA evaluation, and for the product to pass SDA-E, FSA-E, and ERT. [EDSA-300] points to the detailed documents on these topics as shown in Figure 2.

The SDLA specification [SDLA-312] provides requirements both on a supplier's security development lifecycle process and on the artifacts generated by these methods for a specific product. [SDLA-312] is used for SDLA certification and within an EDSA evaluation for SDLPA and SDA-E. The SDA-E specification [EDSA-312] is a brief document that points to the artifact requirements in [SDLA-312] which comprise the SDA-E criteria for EDSA certification. The document [EDSA-311] defines the technical evaluation criteria for a device to pass FSA-E for each certification level.

The ERT specification [EDSA-310] provides test requirements for embedded device robustness testing, which includes VIT and CRT. VIT requirements in [EDSA-310] point to [SSA-420], which defines the parameters for the vulnerability scanning policy to be used with the VIT tool to perform VIT.

[EDSA-310] contains test requirements that apply in common to CRT for all protocols. Hence individual protocol-specific test specifications all refer to this document. It should be pointed out that the approach taken for these specifications was to write each protocol-specific specification such that it could be understood as a stand alone document. Hence there is conceptual material that is similar across all of these specifications. However, details of common requirements are not repeated in each protocol-specific document, but rather presented in the common specification [EDSA-310] and referenced in the individual specifications.

The reference section of [EDSA-300] maintains the current list of protocol-specific CRT specifications, which defines the set of protocols that will be tested under CRT. As of this ISASecure version, there are six such specifications, for "Ethernet", ARP, IPv4, ICMPv4, UDP and TCP. These are documents numbered EDSA 401-406, shown at the bottom of the figure. An example is [EDSA-404] *ISCI EDSA – Testing the robustness of implementations of the IETF ICMPv4 network protocol*.

[EDSA-310] refers to [EDSA-300] for the list of required protocols to be tested, in order to define the pass criteria for CRT. This structure was chosen so that all ISASecure EDSA technical specifications could be listed in one technical document, which is [EDSA-300].

The document [EDSA-301] *ISCI EDSA – Maintenance of ISASecure Certification*, describes the certification criteria and process for a modified device, where a previous version has already achieved certification. It also covers the process for upgrading a certification to a later ISASecure version (for example 2.1.0 Level 1 to 3.0.0 Level 1), or to a higher level.

These documents are used by:

- End users, to understand the meaning of various levels of ISASecure certification
- Device suppliers, to understand the criteria against which their devices will be evaluated
- Chartered and CRT laboratories, to define evaluation processes and criteria
- Tool suppliers and ISCI, as the end reference for technical requirements for achieving CRT tool recognition
- EDSA accreditation bodies, as the end reference for technical readiness assessment requirements when evaluating candidate organizations for chartered or CRT laboratory status.

The embedded device evaluation report template/example [EDSA-303] will be followed by chartered laboratories. It provides end users and device suppliers with an understanding of the type of information that will be provided to device suppliers following all device evaluations.

4.5.3 Accreditation/Recognition

ISASecure EDSA chartered laboratories, CRT laboratories and CRT tool suppliers implement the technical aspects of the certification program. The accreditation/recognition documents define how they obtain this role.

[EDSA-200] *ISCI EDSA – ISASecure EDSA chartered laboratory operations and accreditation* describes the accreditation criteria and process that an organization will follow to become a chartered laboratory. A candidate organization initially attains provisional chartered status which allows it full rights to evaluate devices and grant ISASecure EDSA certifications. To be granted full status as a chartered laboratory for the ISASecure EDSA program, a laboratory shall attain within a specified time frame the following internationally recognized accreditations, performed by an EDSA accreditation body:

- accredited to IAF ISO/IEC 17065, with technology scope of accreditation covering ISASecure EDSA certification, and
- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure EDSA ERT specifications.

[EDSA-200] details the requirements for chartered laboratory status, including interpretations of the above international standards for the ISASecure EDSA program, and the process for technical readiness assessment. This document is used by:

- organizations that are candidate chartered laboratories, to understand the accreditation requirements and process
- EDSA accreditation bodies, as the source for program specific requirements for the ISO/IEC 17065 and ISO/IEC 17025 accreditations listed above.

[EDSA-206] *ISCI EDSA – ISASecure EDSA CRT laboratory operations and accreditation* describes the accreditation criteria and process that an organization will follow to become a CRT laboratory. To be granted status as a CRT laboratory for the ISASecure EDSA program, a laboratory shall attain the following internationally recognized accreditation, performed by the EDSA accreditation body:

- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure EDSA CRT specifications.

This document is used by:

- organizations that are candidate CRT laboratories, to understand the accreditation requirements and process
- EDSA accreditation bodies, as the source for program specific requirements and interpretations for the ISO/IEC 17025 accreditation listed above.

The ISASecure EDSA certification program requires the use of test tools for CRT. In particular a chartered laboratory must use a CRT tool recognized by ISCI. [EDSA-201] *ISCI EDSA – Recognition process for communication robustness testing tools* details how a tool supplier applies for and maintains recognition of their CRT test tool for use within the program. Specifically, this document details which aspects of the test requirements in [EDSA-310] and [EDSA-401] through [EDSA-406] must be addressed by a CRT tool, and how a tool supplier will demonstrate these capabilities to ISCI in order to become a recognized ISASecure CRT tool. Thus this document is used by:

- CRT tool suppliers, to understand tool recognition requirements
- ISCI, as the technical and process guide for its CRT tool recognition program

- Chartered and CRT laboratories, to understand the requirements that will be met by all recognized CRT tools, since a laboratory potentially must meet the balance of ISASecure EDSA CRT requirements by other means.

4.5.4 Symbol and certificates

The document [EDSA-204] *ISCI EDSA – Instructions and Policies for Use of the ISASecure Symbol and Certificates* describes the format and correct usage for the ISASecure symbol and certificates. The ISASecure symbol is used by device suppliers to indicate a certified embedded device. It is also used by chartered laboratories, CRT laboratories and suppliers of recognized CRT tools to indicate their authorized participation in the ISASecure program.

Four types of ISASecure certificates are issued under the EDSA program: for certified devices, chartered laboratories, CRT laboratories and recognized CRT tools.

The supporting document [EDSA-205] *ISCI EDSA – Certificate Document Format* is a convenient shorter document that contains certificate format templates only.

The documents in this category as they apply to certified devices are used by:

- embedded device suppliers, to understand requirements for symbol and certificate usage
- end users, to understand the meaning of a symbol or certificate displayed by a supplier
- chartered laboratories, to create certificates for certified devices
- chartered laboratories, to monitor for correct use of the symbol and device certificates by client device suppliers as required by [EDSA-200].

These documents as they apply to chartered laboratories, CRT laboratories and CRT tools are used by:

- chartered laboratories, CRT laboratories and CRT tool suppliers, to understand requirements for symbol and certificate usage
- embedded device suppliers, to understand the meaning of the symbol or certificate displayed by a chartered laboratory or CRT laboratory
- chartered laboratories and embedded device suppliers, to understand the meaning of the symbol or certificate as displayed by a CRT laboratory or CRT tool supplier
- ASCI/ISCI, to create certificates for chartered laboratories, CRT laboratories and CRT tools
- ISCI, to monitor for correct use of the symbol and certificates for chartered laboratories, CRT laboratories and recognized CRT tools.

4.5.5 Structure

Documents in the Structure category are the present document [EDSA-100] and [SDLA-100] *ISCI SDLA – ISASecure certification scheme.* [EDSA-100] is a publicly available reference to the structure of the overall ISASecure EDSA program. [SDLA-100] is a publicly available reference to the structure of the overall SDLA certification program for supplier development processes, which may be leveraged for partial fulfillment of EDSA certification requirements.

4.5.6 External references

[ISO/IEC 17065] is an international standard that contains requirements for operating a product, process, or service certification program.

[ISO/IEC 17025] is an international standard that presents requirements for product testing programs. The requirements in this document apply to the ERT element of ISASecure EDSA. To obtain chartered status, chartered laboratories will demonstrate adherence to the requirements in these standards as part of the accreditation process. To obtain CRT laboratory status, a laboratory will demonstrate adherence to ISO/IEC 17025.

[ISO/IEC 17011] is an international standard that applies to the accreditation process itself. Thus this document is used by EDSA accreditation bodies and ASCI to define their accreditation operations for the ISASecure EDSA certification program.

Although the ISASecure specifications are self-contained, the ISASecure program intent is to provide a conformance program for ISA 62443, as described in 4.3. Figure 2 refers to the approved standards from the ISA 62443 series with which EDSA certification aligns.

[ANSI/ISA-62443-1-1] covers terminology and concepts. In particular that standard lists the foundational high level requirements used to derive and organize the detailed requirements for the FSA-E evaluation, and defines the concepts of essential functions and security levels used by the EDSA specifications.

[ANSI/ISA-62443-4-1] covers requirements for the security development lifecycle for suppliers developing industrial control system products.