SSA-100

ISA Security Compliance Institute — System Security Assurance –

ISASecure® certification scheme

Version 1.7

December 2014

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SPECIFICATION.

WITHOUT LIMITING THE FOREGOING, ASCI DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THIS SPECIFICATION ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE SPECIFICATION AVAILABLE, ASCI IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS ASCI UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE. ANYONE USING THIS SPECIFICATION SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ASCI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL,PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SPECIFICATION, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SPECIFICATION OR OTHERWISE ARISING OUT OF THE USE OF THE SPECIFICATION, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SPECIFICATION, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF ASCI OR ANY SUPPLIER, AND EVEN IF ASCI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision history

version	date	changes
1.5	2014.02.09	Initial version published to http://www.ISASecure.org
1.7	2014.12.10	Change from Guide 65 to 17065, remove reference to ASCI 2009 application document, change name of EDSA-310, introduce acronym SDLPA

Contents

Table of Figures

FOREWORD

This is one of a series of documents that defines ISASecure® certification for control systems, 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 SSA (System Security Assurance), as well as other ISASecure certification programs, can be found on the web site http://www.ISASecure.org.

1 Scope

This document provides an overview of the operation of the ISASecure® SSA (System Security Assurance) 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. This document provides an overview the requirements for certification of a system; the detailed reference for that topic is the document [SSA-300] listed in Section 2.

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). ISASecure SSA supports this goal by offering a common industry-recognized set of system and development process requirements that drive system security, simplifying procurement for asset owners, and system assurance for product suppliers. A supplier can display the ISASecure symbol in association with a system that is certified to meet these requirements. In addition to ISASecure SSA, ISCI also operates a product certification program for embedded devices, called ISASecure EDSA (Embedded Device Security Assurance) and a supplier development process certification, called ISASecure SDLA (Security Development Lifecycle Assurance). The ISASecure EDSA and SDLA certification schemes and other documentation can be found on the web site http://www.ISASecure.org. The present document describes the relationships between ISASecure SSA and these other certification programs.

2 Normative references

NOTE Section 4.6 provides a diagrammatic and expository overview of the ISASecure SSA 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 SSA certification body.

[SSA-200] *ISCI System Security Assurance – ISASecure SSA Chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[ISASecure-111] *ISCI ISASecure Certification Programs - Transition to ISO/IEC 17065*, as specified at http://www.ISASecure.org

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

2.1.2 CRT tool recognition program

NOTE The following documents describe how to attain ISASecure recognition for a tool used to carry out communication robustness testing (CRT) and network stress testing (NST), which are two aspects of the system robustness testing performed for an SSA evaluation. CRT is also a requirement for ISASecure EDSA certification for an embedded device. The same tool recognition process applies for all of these applications of the tool.

[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

2.1.3 CRT laboratory operations and accreditation

NOTE The following documents describe how to achieve CRT laboratory status and operate as a laboratory recognized for performing ISASecure CRT for embedded devices. CRT is required for both ISASecure EDSA and ISASecure SSA certifications.

[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

2.2 ISASecure symbol and certificates

NOTE The following document describes the ISASecure symbol and certificates and how they are used.

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

[SSA-205] *ISCI System 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 a system for ISASecure SSA certification.

2.3.1 General technical specifications

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

[SSA-300] *ISCI System Security Assurance – ISASecure certification requirements,* as specified at http://www.ISASecure.org

[SSA-301] *ISCI System Security Assurance – Maintenance of ISASecure certification,* 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

[SSA-303] *ISASecure SSA 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 System Robustness Testing element of an SSA evaluation.

[SSA-310] *ISCI System Security Assurance – System robustness testing,* as specified at http://www.ISASecure.org

NOTE 2 The following document defines how tests are carried out for both ISASecure EDSA and for several aspects of SSA Systems Robustness Testing (SRT). It applies for ISASecure SSA to the extent described in [SSA-310].

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

NOTE 3 The following documents provide the technical evaluation criteria for the Functional Security Assessment element of an SSA evaluation.

[SSA-311] *ISCI System Security Assurance – Functional security assessment for systems,* as specified at http://www.ISASecure.org

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

NOTE 4 The following document provides the overall technical evaluation criteria for the Security Development Artifacts element of an SSA product evaluation. [SDLA-312] also provides the technical evaluation criteria for an ISASecure assessment of supplier security development lifecycle processes.

[SSA-312] *ISCI System Security Assurance – Security development artifacts for systems,* 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 5 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 Vulnerability Identification Testing (VIT) for a specific system. VIT is a sub element of System 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

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 used by the ISASecure SSA program but maintained outside of the ISASecure program.

2.4.1 IACS security standards

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

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

[ISA 62443-3-3] ANSI/ISA−62443−3−3, *Security for industrial automation and control system: Part 3-3, System security requirements and security levels*

2.4.2 International standards for certification programs

NOTE The following international standards apply to the ISASecure 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 December 1999

2.4.3 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure chartered laboratory accreditation process.

[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 a 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
security level that a component or system can provide when properly configured

NOTE This type of security level states that a particular component or system is capable of meeting a target security level natively without additional compensating countermeasures when properly configured and integrated.

3.1.5
certificate
document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

NOTE For ISASecure SSA, there are certificates for certified systems, recognized CRT tools, chartered laboratories, and CRT laboratories.

3.1.6
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.

3.1.7
certification scheme
overall definition of and process for operating a certification program

3.1.8
certified embedded 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

3.1.9
certified system
well-defined version of a control system that has undergone an evaluation by a chartered laboratory, has met the ISASecure SSA criteria and has been granted certified status by the chartered laboratory

3.1.10
certification body
third-party conformity assessment body operating certification schemes

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 certification 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 certification programs, the conformity assessment body is a chartered laboratory.

3.1.15
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.16
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 EDSA or SSA certification

3.1.17
device
combination of components having a given function forming a part of a piece of equipment, apparatus or system

NOTE Examples include DCS computers, substation computers, PLCs, RTUs, sensors, etc.

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
end user
organization that purchases, uses or is impacted by the security of control systems products

3.1.20
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.

3.1.21
“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
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

3.1.24
pass
meet the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.25
provisional chartered status
interim, temporary recognition status granted by ISCI during which a chartered laboratory is authorized to perform evaluations and grant ISASecure certifications

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

3.1.26
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

3.1.27
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.

3.1.28
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.

3.1.29
security zone
grouping of logical or physical assets that share common security requirements

NOTE 1 A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

NOTE 2 This definition and NOTE 1 are from [ISA 62443-3-3]. A security zone configuration is part of the system architecture diagram submitted by applicants for ISASecure SSA certification, as required per [SSA-310].

3.1.30
supplier
organization that is responsible for compliance of a product or development process with ISASecure requirements

3.1.31
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.32
system
control system

NOTE In the ISASecure SSA documentation, this shorter term is used for convenience to refer to a control system product that may fall under the scope of ISASecure SSA certification. Per the definition above, control systems include safety systems.

3.1.33
tool supplier
provider of a test tool to support communication robustness testing

3.1.34
version (of a product)
well defined release of a system, embedded device, or other control system component product, typically identified by a release number

3.1.35
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 SSA 2.6.1

3.1.36
zone
security zone

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
DCS	distributed control system
EDSA	embedded device security assurance
FSA-E	functional security assessment for embedded devices
FSA-S	functional security assessment for systems
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
IPv6	Internet protocol version 6
ILAC	International Laboratory Accreditation Cooperation
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
OS	operating system
PLC	programmable logic controller
RTU	remote terminal unit
SDA-S	security development artifacts for systems
SDLA	security development lifecycle assurance
SDLPA	security development lifecycle process assessment
SIS	safety instrumented system
SNAP	sub network access protocol
SSA	system security assurance
SRT	system robustness testing
TCP	transmission control protocol
UDP	user datagram protocol
VIT	vulnerability identification test

4 ISASecure SSA certification program

4.1 Scope of the SSA certification program

ISASecure SSA is a certification program for a particular subset of control systems. A control system product that meets all of the following criteria may be certified under the SSA program:

- The control system consists of an integrated set of components and includes more than one device.
- The control system is available from and supported as a whole by a single supplier, although it may include hardware and software components from several manufacturers.
- The supplier has assigned a unique product identifier to the control system which the supplier uses in the marketplace to refer to the integrated set of components as a whole.
- The system product is under configuration control and version management.

[SSA-300] provides examples and additional discussion of the types of systems that may be certified under the SSA program.

4.2 Technical ISASecure SSA evaluation criteria

In order to obtain ISASecure SSA certification, a supplier must pass a security development lifecycle process assessment (SDLPA). This evaluation may be performed as part of the SSA 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 SSA and SDLA certification in parallel. ISASecure SSA certification of systems has four additional elements:

- Security Development Artifacts for systems (SDA-S);
- Functional Security Assessment for systems (FSA-S);
- Functional Security Assessment for embedded devices (FSA-E); and
- System robustness testing (SRT).

SDA-S examines the artifacts that are the outputs of the supplier's security development processes as they apply to the system to be certified. FSA-S examines the security capabilities of the system. FSA-E examines the security capabilities of any embedded devices that are components of the system, recognizing that in some cases security functionality is provided by other system components. SRT has three major elements - Vulnerability Identification Testing (VIT), Communication Robustness Testing (CRT), and Network Stress Testing (NST). VIT scans all components of a system for the presence of known vulnerabilities. CRT and NST verify that the system adequately maintains essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions) at its network interfaces.

The following figure illustrates the elements of ISASecure SSA certification.

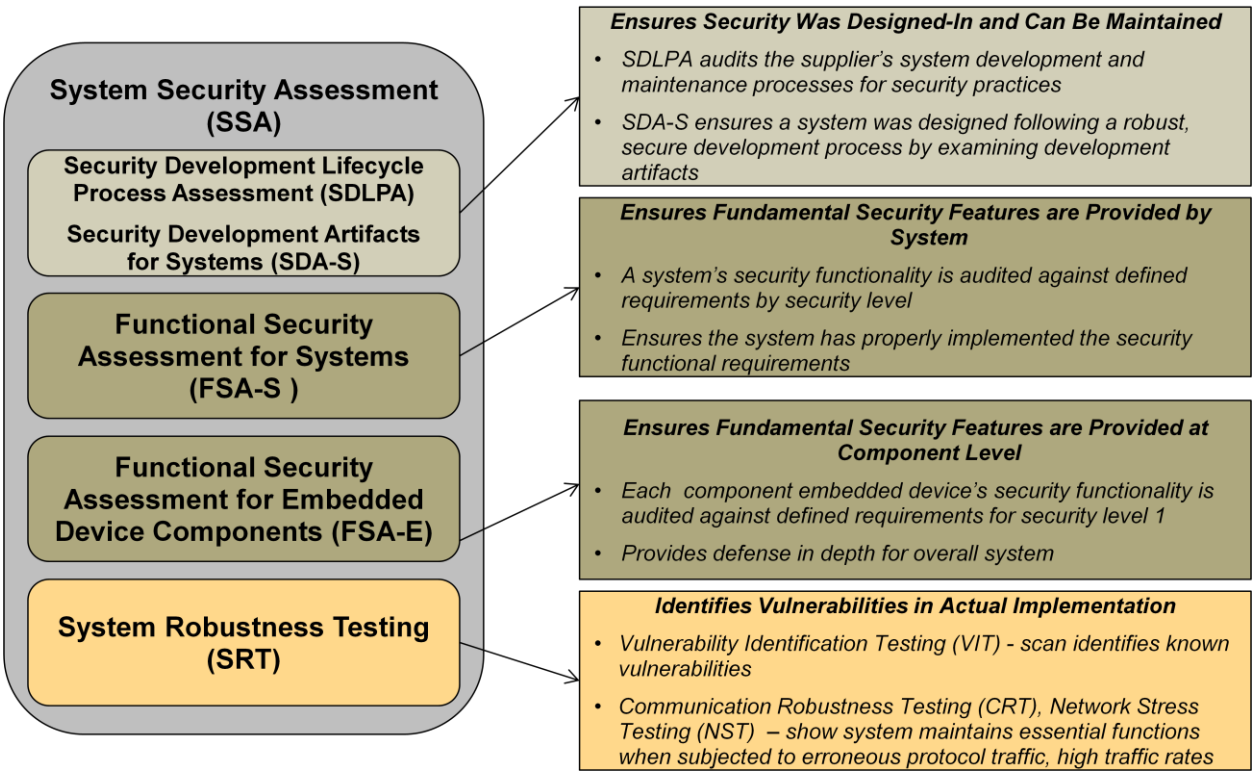

Figure 1 - Evaluation Elements for ISASecure SSA Certification

The SSA certification process for a system may leverage prior ISASecure EDSA certifications for embedded devices that are components of that system. In particular, if a component of a system is a certified ISASecure EDSA embedded device, then FSA-E and the CRT aspect of SRT need not be performed on that device as part of the SSA certification process. This is due to the fact that these assessments will have been performed previously under the ISASecure EDSA certification process.

A system submitted for certification is comprised of one or more security zones together with desired capability security levels for each zone. The notions of security zone, security level and capability security level are introduced in [ISA 62443-1-1]. Evaluation criteria for SDA-S, FSA-S, and VIT increase in rigor for higher security levels.

4.3 Relationship of the SSA program to ISA 62443

A goal for the SSA certification program is to offer a compliance program for the ISA 62443 series of standards. ISA 62443 standards address security for IACS. ISASecure SSA certification incorporates requirements that apply to control systems, which are the hardware and software components of 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 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 SSA specifications define and use the notions of security zone, conduit and security level introduced in ISA 62443-1-1, to be discussed further in ISA 62443-3-2 “Security for industrial automation and control systems – Risk assessment and design,” which is currently under development.

The SSA FSA-S requirements for certification include all requirements in ISA 62443-3-3 “Security for industrial automation and control systems – System security requirements and security levels.” The security

levels for the FSA-S evaluation of a security zone within a system, align with the ISA 62443-3-3 security levels.

In the future, the ISASecure process evaluation requirements and levels for SDLA certification (and SDLPA when performed within a product certification evaluation), will be revised as necessary to align with the requirements and levels in the planned standard ISA 62443-4-1 “Security for industrial automation and control systems – Product development requirements.” This standard is under development.

4.4 Certified systems

The supplier for a system that has been evaluated under the ISASecure SSA 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 a system, and references a 3-digit certification version that identifies the set of ISASecure specifications used for the certification. . For example, system model 234, version 1.9 might be certified to ISASecure SSA 2.6.1. The ISASecure SSA certificate for a system will name its security zones and the security levels to which they have been certified.

The SSA program defines procedures to maintain certification for updated versions of the system, to later versions of the ISASecure evaluation program, and to higher certification levels.

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

4.5 Organizational roles

The following organizations participate in the ISASecure SSA 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 systems, and may require an ISASecure certification for a system for which particular zones have been certified to particular levels
- **System suppliers** apply for certification of their systems. A system assembled for a particular customer by a system integrator or by the customer themselves, is not addressed by this certification program unless it meets the requirements listed in 4.1 (client)
- **Chartered laboratories** for the SSA program accept applications from system suppliers for system certification, evaluate systems, and are authorized to grant system certifications to system suppliers (certification body)
- **CRT laboratories** may test embedded devices to the CRT requirements and submit results to chartered laboratories as evidence toward an SSA (and/or ISASecure EDSA) certification. Note that a chartered laboratory may also perform CRT for embedded devices, and will perform CRT for all other types of devices in a system undergoing SSA certification
- **CRT tool suppliers** provide test tools that allow chartered laboratories and CRT laboratories to carry out CRT, chartered laboratories to carry out NST, and system suppliers to test their systems in advance of formal evaluation for certification
- **ISCI** defines, maintains and manages the overall ISASecure SSA, EDSA and SDLA certification programs, 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 SSA, EDSA and SDLA laboratories, recognized CRT tools, ISASecure certified products and ISASecure certified supplier development processes (scheme owner)
- **ASCI** (Automation Standards Compliance Institute), as the legal entity representing ISCI, grants chartered SSA laboratory status to applicant organizations based on successful accreditation to criteria defined by ISCI

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

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

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

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

4.6 Certification program documentation

4.6.1 Overview of documentation

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

NOTE 1 [SSA-200] and [EDSA-201] 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 form [SSA-205], and the policy regarding transition from ISO/IEC Guide 65 to ISO/IEC 17065 [ISASecure-111].

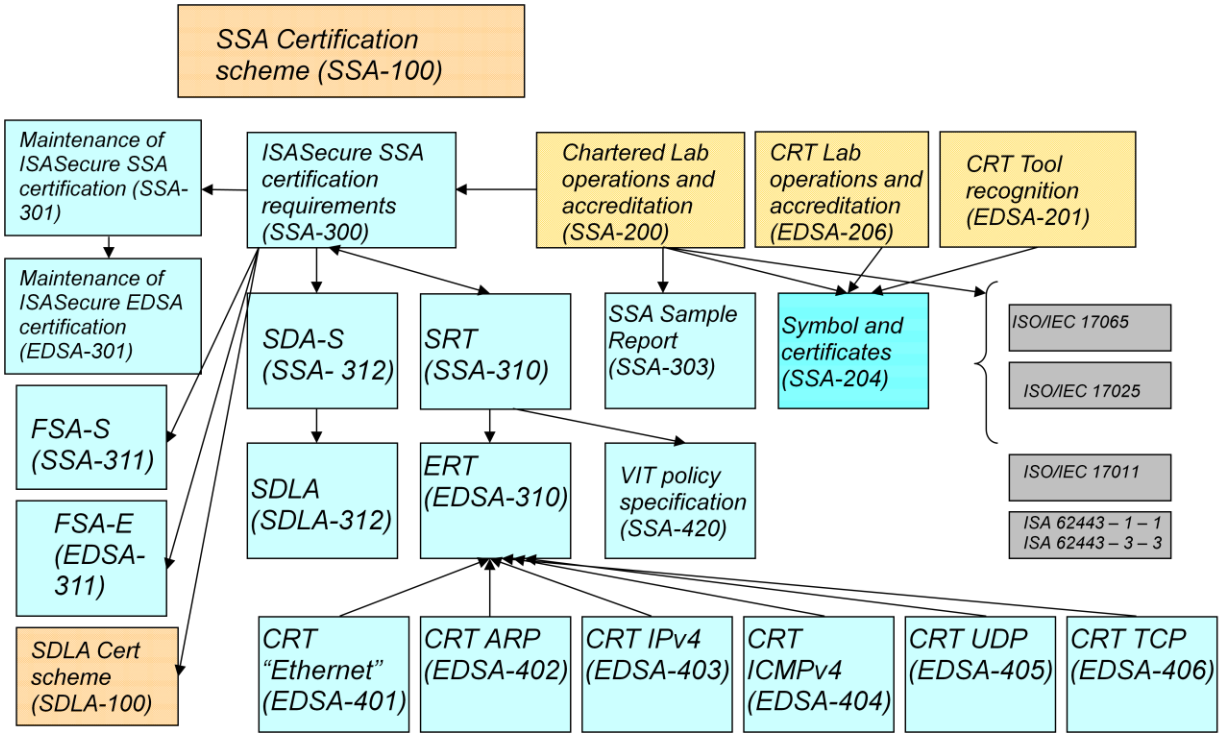

Figure 2 - ISASecure SSA Documents

There are five major categories of ISASecure SSA program documents:

- **Technical specifications**, shown with no pattern in light blue, that describe the technical criteria applied to determine whether a system will be certified

- **Accreditation/recognition**, shown in gold diagonal stripe, that describe how an organization can become a chartered SSA laboratory or a 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 an overall certification 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 prefix “SSA” are unique to the ISASecure SSA certification program. The documents with prefixes “EDSA” and “SDLA” are used both by those certification programs, respectively, as well as the SSA program. The following sections describe all documents in each category in further detail.

4.6.2 Technical specifications

The brief document [SSA-300] *ISCI SSA - ISASecure Certification Requirements,* defines at a high level the criteria for system certification, which simply stated, are for the supplier to pass an ISASecure SDLPA evaluation, and for the product to pass SDA-S, FSA-S, FSA-E (applicable if the system has embedded device components), and SRT. [SSA-300] points to the detailed documents on these four topics as shown in Figure 2. It also contains further discussion and examples of types of systems that would fall under the SSA certification program and how the evaluation elements of the program would be applied to an example system. The SDLA specification [SDLA-312] provides requirements both on supplier security development lifecycle process (used for SDLA certification or for SDLPA within an SSA evaluation) and on the artifacts generated by these methods for a specific product. The SDA-S specification [SSA-312] is a brief document that points to the artifact requirements in [SDLA-312] which comprise the SDA-S criteria for SSA certification. The FSA-S document [SSA-311] defines the technical evaluation criteria for a security zone within a system to pass FSA-S, based upon its security level. The document [EDSA-311] defines the technical evaluation criteria for an embedded device to pass functional security assessment for ISASecure EDSA certification; the level 1 criteria in this document also comprise the FSA-E element of SSA certification. The SRT specification [SSA-310] provides test requirements for system robustness testing, which includes VIT, CRT, and NST.

The detailed specifications for CRT (in EDSA-310, and EDSA-401 through 406) were developed for testing embedded devices under the ISASecure EDSA certification program. However, the methodology they describe is applicable as well for other types of component devices of systems, such as workstations and historian servers. [SSA-310] defines the scope of CRT testing required for components of a system in order to achieve SSA certification. Specified requirements in these EDSA documents also apply for NST.

The reference section of [SSA-300] maintains the current list of protocol-specific CRT specifications, which defines the set of protocols that will be tested under the CRT and NST elements of SRT. At launch of the program, there are six such specifications, for “Ethernet”, ARP, IPv4, ICMPv4, UDP and TCP. These are documents numbered EDSA-401 through 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.*

The ERT specification [EDSA-310], *ISCI EDSA – Embedded device robustness testing*, 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 standalone 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 [EDSA-310] and referenced in the individual specifications. Other CRT requirements in [EDSA-

310] apply for CRT and NST performed under SSA SRT, to the extent specified in the SRT specification [SSA-310].

[EDSA-310] also contains requirements for VIT for embedded devices. [SSA-310] includes a self-contained set of VIT requirements for SSA certification and therefore does not reference VIT requirements in [EDSA-310]. (However, VIT requirements as they apply to embedded devices are consistent in [EDSA-310] and SSA-310].)

[SSA-420] defines the parameters for the vulnerability scanning policy to be used with the VIT tool to perform VIT.

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

The document [SSA-301] *ISCI System Security Assurance – Maintenance of ISASecure Certification*, describes the certification criteria and process for a modified system, 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 to 3.1.0), or a particular security zone to a higher security level. [SSA-301] refers to specific requirements in [EDSA-301] *ISCI EDSA - Maintenance of ISASecure Certification*, which covers these same topics for embedded devices under the ISASecure EDSA certification program.

These documents are used by:

- End users, to understand the meaning of various levels of ISASecure certification
- System suppliers, to understand the criteria against which their systems 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
- SSA accreditation bodies, as the end reference for technical readiness assessment requirements when evaluating candidate organizations for chartered laboratory status.

The evaluation report requirements embodied in the sample evaluation report [SSA-303] will be followed by chartered laboratories. This document provides end users and system suppliers with an understanding of the type of information that will be provided to system suppliers following all system evaluations.

4.6.3 Accreditation/Recognition

ISASecure SSA 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.

[SSA-200] *ISCI SSA – ISASecure SSA chartered laboratory operations and accreditation* describes the accreditation criteria and process that an organization will follow to become a chartered laboratory. To be granted full status as a chartered laboratory for the ISASecure SSA program, a laboratory shall attain the following internationally recognized accreditations, performed by an SSA accreditation body:

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

ACSI grants provisional recognition to a chartered laboratory when an SSA accreditation body informally reports to ISCI that the candidate organization has met all requirements for accreditation. Full chartered laboratory status is granted when an SSA accreditation body formally grants the above accreditations to the candidate organization.

[SSA-200] details the requirements for both provisional recognition and full chartered laboratory status, including compliance with the above international standards for the ISASecure SSA 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, as well as ongoing requirements on their operations

- SSA 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. This accreditation allows an organization to submit evidence for CRT to a chartered laboratory toward either an EDSA certification of an embedded device, or an SSA certification of a system for which an embedded device is a component. To be granted status as a CRT laboratory for the ISASecure program, a laboratory shall attain the following internationally recognized accreditation, performed by an 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 SSA certification program requires the use of test tools for CRT, which are also used for NST. 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 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:

- a tool supplier, 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 CRT requirements by other means.

4.6.4 Symbol and certificates

The document [SSA-204] *ISCI SSA – Instructions and Policies for Use of the ISASecure Symbol and Certificates* describes the format and correct usage for the ISASecure symbol and certificates within the SSA certification program. The ISASecure symbol is used by system suppliers to indicate a certified system. 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 related to the SSA program: for certified systems, chartered SSA laboratories, CRT laboratories, and recognized CRT tools.

The document in this category as it applies to certified systems is used by:

- system 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 systems
- chartered laboratories, to monitor for correct use of the symbol and system certificates by client system suppliers as required by [SSA-200].

This document as it applies to chartered laboratories, CRT laboratories, and CRT tools is used by:

- chartered laboratories, CRT laboratories and CRT tool suppliers, to understand requirements for symbol and certificate usage
- system suppliers, to understand the meaning of the symbol or certificate displayed by a chartered laboratory or CRT laboratory
- chartered laboratories and system suppliers, to understand the meaning of the symbol or certificate as displayed by a CRT laboratory or 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.

4.6.5 Structure

Two documents are in the Structure category. The first is the present document [SSA-100]. [SSA-100] is a publicly available reference to the structure of the overall ISASecure SSA certification program. The second is the scheme document [SDLA-100], which is a publicly available reference to the structure of the ISASecure SDLA certification program for supplier security development lifecycle processes. [SDLA-100] provides references and descriptions for all detailed documents that define the SDLA certification program, in a manner similar to the present document. Although not shown in the above figure, all of those documents are applicable to a supplier interested in obtaining both an ISASecure SDLA certification for their security development process and an ISASecure SSA certification for a system product.

4.6.6 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 SRT element of ISASecure SSA. To obtain chartered status, chartered laboratories will demonstrate adherence to the requirements in these two 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 SSA 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 two approved standards from the ISA 62443 series. ISA 62443-1-1 covers terminology and concepts. ISA 62443-3-3 covers system security requirements and security levels. The ISASecure specifications are closely related to these standards as follows. ISA 62443-1-1 lists the foundational high level requirements used to derive and organize the detailed requirements for the FSA-S evaluation, and defines the concepts of security zones, essential functions and security levels used by the SSA specifications. The FSA-S evaluation criteria in [SSA-311] are directly derived from ISA 62443-3-3.