SSA-100

ISA Security Compliance Institute – System Security Assurance –

ISASecure® certification scheme

Version 3.1

August 2019

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, information, 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.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

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
2.2	2018.02.01	Align with approved ANSI/ISA 62443-4-1 (SSA 2.1.0); explicitly support scalable systems: define scalable system and layout; changes to 4.1, 4.4, 4.6.2 1st paragraph; change references to SDLA, SDLPA and SDA-S to align with incorporate erratum from SSA-102 v1.6
2.4	2018.10.02	Update for alignment with ANSI/ISA-62443-4-2: update normative references; in 4.2 modify text re FSA-E referencing other system components; in 4.2 modify text re pass/fail for VIT; add paragraph about ANSI/ISA-62443-4-2 in 4.3; changes for ISASecure-116, 4-2, CSA-311 in 4.6
3.1	2019.08.06	Systems and zones made up of components instead of devices; clarify definition of term certification level; change definition of device; remove certifier CRT and NST and related CRT labs and tool recognition; remove FSA-E; add system integrator role; change role end users to asset owners; require SDLA cert; update title and content of SSA-420; update 17025 and 17011 versions

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 of 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 standards-based, 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 components, called ISASecure CSA (Component Security Assurance) and a supplier development process certification, called ISASecure SDLA (Security Development Lifecycle Assurance). The ISASecure CSA and SDLA certification schemes and other documentation can be found on the web site http://www.ISASecure.org. The present document describes the relationship between ISASecure SSA and ISASecure SDLA.

2 Normative references

NOTE Section 4.6 provides a diagrammatic and expository overview of the ISASecure SSA documents and their relationships.

2.1 Accreditation

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-117] *ISCI ISASecure Certification Programs - Policy for transition to CSA 1.0.0 and SSA 4.0.0,* as specified at http://www.ISASecure.org

[ISASecure-202] *ISCI ISASecure Certification Programs – Application and Contract for Chartered 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

[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 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

NOTE 2 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 SDLA assessment of supplier secure product 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 3 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product 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 procedures and policy parameter values used to perform Vulnerability Identification Testing (VIT-S) for a specific system.

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Specification*, 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 1 Section 4.3 describes the relationship of ISASecure to the ANSI/ISA/IEC 62443 series of standards.

NOTE 2 The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC

[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*

[IEC 62443-1-1] IEC TS 62443-1-1:2009 *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*

[ANSI/ISA-62443-3-3] ANSI/ISA−62443−3−3 (99.03.03) - 2013, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

[IEC 62443-3-3] IEC 62443−3−3:2013 *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

[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 1 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

NOTE 2 The transition timeline to the later 2017 version of ISO/IEC 17025 below is defined by ISO/ILAC policy.

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

[ISO/IEC 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories**",*** November 2017

2.4.3 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure chartered laboratory accreditation process. The transition timeline to the later 2017 version of ISO/IEC 17011 below is defined by ISO/ILAC policy.

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

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", November 2017

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 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
asset owner
individual or company responsible for one or more IACS

NOTE 1 Used in place of the generic term end user to provide differentiation.

NOTE 2 This includes the components that are part of the IACS.

NOTE 3 In the context of this document, an asset owner also includes the operator of the IACS.

3.1.5
capability security level
security level that a component or system can provide when properly configured and integrated

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.

3.1.6
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 and chartered 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 level
capability security level for which conformance is demonstrated by a certification

NOTE An SSA certification for a particular security zone may be for capability security level 1, 2, 3, or 4. A zone certified to capability security level *n* meets requirements for capability security level *n* as defined in the standard [IEC 62443-3-3].

3.1.9
certification scheme
overall definition of and process for operating a certification program

3.1.10
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

3.1.11
certification body
third-party conformity assessment body operating certification schemes

3.1.12
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.

3.1.13
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.14
conformity assessment
demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

3.1.15
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.

3.1.16
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.17
device
asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

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

3.1.22
host device
general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

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
layout
description of a specific instance of a scalable control system, that defines quantities of zones and resident components, and internal and external interfaces

3.1.25
network device
device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

3.1.26
pass
meet the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.27
scalable control system
control system which supports replication of zones and/or components to support small and large installations

3.1.28
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.

3.1.29
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.

3.1.30
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 [IEC 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-300].

3.1.31
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1 Software applications typically execute on host devices or embedded devices.

NOTE 2 Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

3.1.32
supplier
organization that is responsible for compliance of a product or development process with ISASecure requirements

3.1.33
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is "mark."

3.1.34
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.

3.1.35
system integrator
service provider that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

NOTE This may also include other system supplier designations such as General Automation Contractor, Main Automation Contractor, Main Instrument Vendor, and similar.

3.1.36
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

3.1.37
upgrade
incremental hardware or software change in order to add new features

3.1.38
version (of a product)
well defined release of a system, embedded device, or other control system component product, typically identified by a release number

3.1.39
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 4.0.0

3.1.40
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CSA	Component Security Assurance
DCS	distributed control system
FSA-S	functional security assessment for systems
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission
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
SIS	safety instrumented system
SSA	system security assurance
VIT-S	vulnerability identification test for systems

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 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 component.
- 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 control system may have a fixed component and zone layout, or may be scalable, that is, may support replication of components and of zones in order to scale for small and large installations.
- The system product is under configuration control and version management.

[SSA-300] further specifies the architectural similarity required between layouts that are to be certified under a single SSA certificate. [SSA-300] also 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 hold an ISASecure SDLA development process certification, as described in [SDLA-100], such that the system to be evaluated is in the scope of that process. A supplier may at their option apply for SSA and SDLA certification in parallel. ISASecure SSA certification of systems has three additional elements:

- Security Development Artifacts for systems (SDA-S);
- Functional Security Assessment for systems (FSA-S); and
- Vulnerability identification testing for systems (VIT-S).

Both the SDLA certification evaluation and SDA-S assess development process. SDLA certification demonstrates that the supplier has a documented secure product development lifecycle process, that it is compliant with [IEC 62443-4-1], and that there is evidence the process is followed. SDA-S examines the artifacts that are the outputs of the supplier's development lifecycle process as it applies to the system to be certified. FSA-S examines the security capabilities of the system. VIT-S scans all components of the system for the presence of known vulnerabilities.

A system submitted for certification is comprised of one or more security zones together with desired capability security levels for each zone to be demonstrated by the certification. The notions of security zone, security level and capability security level are introduced in [IEC 62443-1-1]. SDLA certification does not have an associated level. SDA-S and VIT-S assessments are the same for all capability security levels with the exception of allowable residual risk for known security issues. FSA-S incorporates more requirements at higher levels, aligned with the requirements assigned to each capability security level in [IEC 62443-4-2].

NOTE In SDLA-312 v5.5, the treatment of residual risk related to known security issues is found in SDLA requirement SDLA-DM-4.

For scalable systems, tests performed by the certifier as part of FSA-S will be performed on a reference system, whose layout meets criteria specified in [SSA-300]. Analyses performed by the certifier will take into account all layouts to be evaluated under the certification.

4.3 Relationship of the SSA program to ANSI/ISA/IEC 62443

A goal for the SSA certification program is to offer a compliance program for the ANSI/ISA/IEC 62443 series of standards, which address security for IACS. ISASecure SSA certification incorporates requirements that apply to a control system, which is the hardware and software for an IACS.

It is the intent that the ISASecure program align terminology, concepts and reference architectures with those used by the ANSI/ISA/IEC 62443 effort, in particular as presented in [IEC 62443-1-1]. Definitions for terms 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 [IEC 62443-1-1], to be discussed further in the planned ANSI/ISA/IEC standard 62443-3-2 "Security for industrial automation and control systems Part 3-2: Risk assessment and design," which is currently under development.

The SSA FSA-S requirements for certification include all requirements in IEC 62443-3-3 "Security for industrial automation and control systems Part 3-3: System security requirements and security levels." The capability security levels for the FSA-S evaluation of a security zone within a system, align with the IEC-62443-3-3 capability security levels and associated requirements. ANSI/ISA has published this standard as [ANSI/ISA-62443-3-3].

The ISASecure evaluation requirements for SDLA certification and SDA-S artifact assessment performed for SSA certification, align with the requirements in the standard IEC 62443-4-1 "Security for industrial

automation and control systems Part 4-1: Secure product development lifecycle requirements." ANSI/ISA has published this standard as [ANSI/ISA- 62443-4-1].

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. An initial certification is granted for a particular version of a system, and a specific layout or (for a scalable system) a set of layouts, 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 with layouts as described in a named reference document, might be certified to ISASecure SSA 4.0.0. The ISASecure SSA certificate for a system will name its security zones and the capability security levels to which they have been certified.

The SSA program defines procedures to maintain certification for later versions of the system that incorporate updates (3.1.36) and upgrades (3.1.37) which may include further scalability options, to later versions of the ISASecure evaluation program, and to higher capability security 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].

- **Asset owners** define procurement criteria and risk tolerance for IACS, and may require an ISASecure certification for a system for which particular zones have been certified to particular capability security levels. Asset owners approve the system integrator's IACS protection concept and rationale. An entity may act both as an asset owner and a system integrator.

- **System integrators** bring together component subsystems into a whole that meets asset owner criteria

- **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, the SSA compliance authorities, accept applications from system suppliers for system certification, evaluate systems, and are authorized to grant system certifications to system suppliers (certification body)

- **ISCI** defines, maintains and manages the overall ISASecure SSA and SDLA certification programs, interprets the ISASecure specifications, and maintains a web site for publishing program documentation, as well as lists of chartered SSA and SDLA laboratories, 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 1 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] contains 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 form [ISASecure-202], the certificate form [SSA-205], and the policy document [ISASecure-117] regarding the ISASecure transition to SSA 4.0.0.

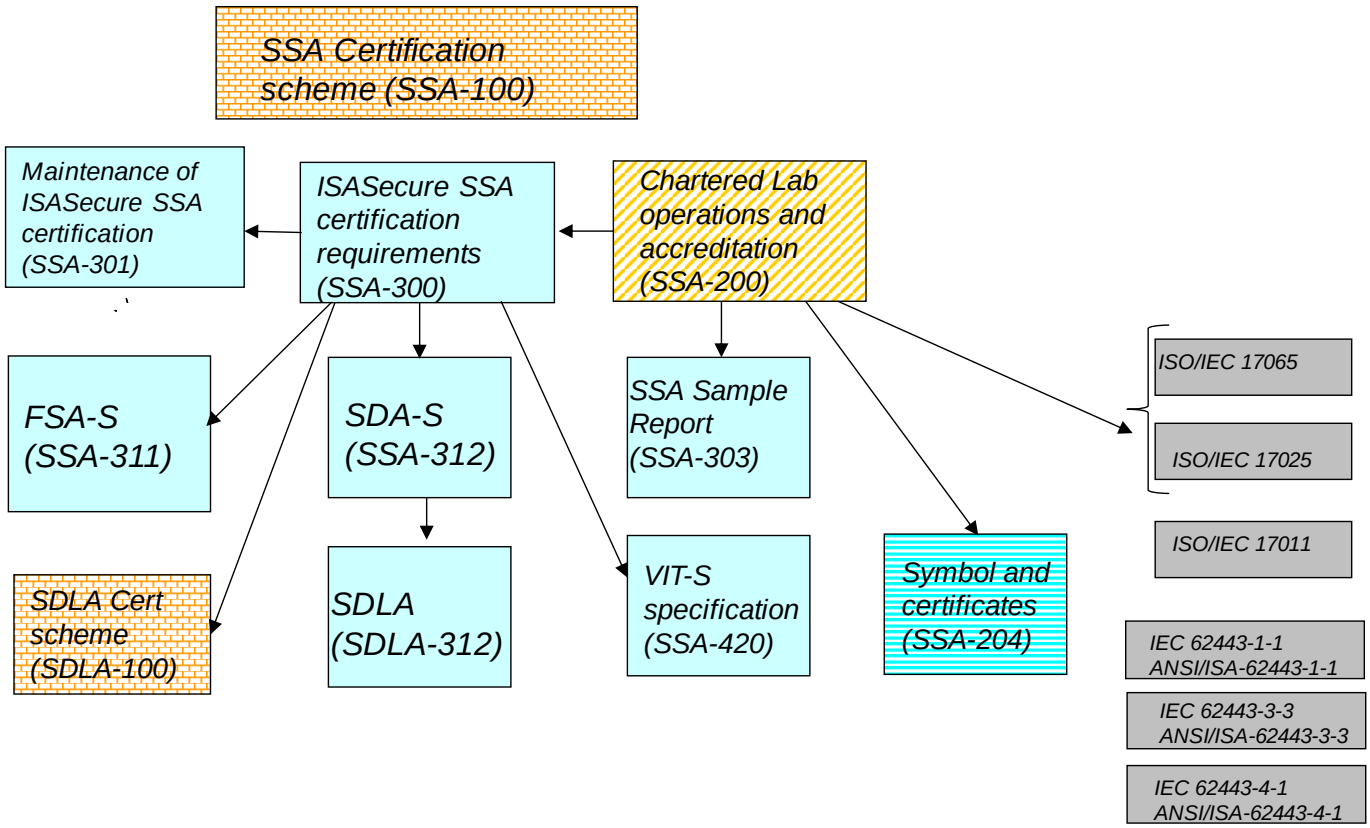

Figure 1 - ISASecure SSA Documents

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**, shown in gold diagonal stripe, that describe how an organization can become a chartered SSA laboratory

- **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 prefix “SDLA” are used both by the SDLA certification program, 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’s development organization to hold an SDLA certification for the development process used for the system, and for the system to pass SDA-S, FSA-S and VIT-S. [SSA-300] points to the detailed documents on these topics as shown in Figure 1. It specifies the scalable system concept and 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. [SSA-300] also provides an example of how a supplier testing effort could define whether the control function is adequately maintained during testing. The SDLA specification [SDLA-312] provides requirements both on supplier secure product development lifecycle (used for SDLA certification) 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 the capability security level to which the zone will be certified.

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

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 system version has already achieved certification. It also covers the process to obtain certification of a certified system to a later ISASecure version (for example SSA 2.0.0 to SSA 4.0.0), or of a particular security zone to a higher capability security level.

These documents are used by:

- Asset owners and system integrators, to understand the meaning of various levels of ISASecure SSA certification

- System suppliers, to understand the criteria against which their systems will be evaluated

- Chartered laboratories, to define evaluation processes and criteria

- 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 asset owners, system integrators, 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

ISASecure SSA chartered laboratories implement the technical aspects of the certification program. The accreditation document defines how they obtain and carry out 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 FSA-S and VIT-S specifications.

[SSA-200] details the requirements for 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.

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 to indicate their authorized participation in the ISASecure program.

Two types of ISASecure certificates are issued related to the SSA program: for certified systems and chartered SSA laboratories.

[SSA-204] as it applies to certified systems is used by:

- system suppliers, to understand requirements for symbol and certificate usage
- asset owners and system integrators, 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 is used by:

- chartered laboratories, to understand requirements for symbol and certificate usage

- system suppliers, to understand the meaning of the symbol or certificate displayed by a chartered laboratory
- ASCI/ISCI, to create certificates for chartered laboratories
- ISCI, to monitor for correct use of the symbol and certificates for chartered laboratories.

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 secure product development lifecycle process. [SDLA-100] provides references and descriptions for all detailed documents that define the SDLA certification program, in a manner similar to the present document. SDLA certification is a part of the SSA certification requirements, as described in [SSA-300].

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 FSA-S and VIT-S elements 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.

[ISO/IEC 17011] is an international standard that applies to the accreditation process itself. This document is used by SSA 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 the ANSI/ISA/IEC 62443 standards, as described in 4.3. The same technical standards used in the SSA program are published by both ANSI/ISA and IEC using the same standard numbers 62443-m-n. Figure 1 refers to three standards from the 62443 series. [IEC 62443-1-1] covers terminology and concepts. [IEC 62443-3-3] covers system security requirements and security levels. [IEC 62443-4-1] covers requirements for the secure product development lifecycle for suppliers developing industrial automation and control system products. The ISASecure specifications are closely related to these standards as follows. [IEC 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 capability security levels used by the SSA specifications. The FSA-S evaluation criteria in [SSA-311] are directly derived from [IEC 62443-3-3]. The SDLA certification requirements and SDA-S evaluation criteria are directly derived from [IEC 62443-4-1].