CSA-100

ISA Security Compliance Institute — Component Security Assurance –

ISASecure® certification scheme

Version 4.3

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
1.1	2010.06.06	Initial version published to http://www.ISASecure.org
2.0	2011.10.21	Support CRT by separate organization, add EDSA-206 and EDSA-207
2.8	2014.12.10	Change from Guide 65 to 17065, doc structure revisions for VIT, incorporate ISASecure SDLA references, describe relationship to ISO/IEC 62443, terminology updates: essential services to essential functions, device vendor to device supplier, remove ISASecure-101 ISCI cert scheme operation document and ASCI 2009 document, unify all chartered lab contracts to become ISASecure-202
3.3	2018.02.13	Align with approved ANSI/ISA-62443-4-1 and IEC 62443-4-1 (EDSA 2.1.0)
3.7	2018.10.01	Align with approved ANSI/ISA-62443-4-2: replace EDSA-311 by CSA-311, change verbiage about permitting allocation to environment – to *met by integration into system*, change to four levels from three, remove statement that VIT depends upon FSA-E (EDSA 3.0.0)
4.3	2019.08.02	Change title of document from EDSA-100 to CSA-100, updating from scheme for embedded devices to scheme for all 62443-4-2 component types; clarify definition of term certification level; remove CRT-related aspects of program; revise overview of maintenance of certification; add system integrator to roles in 4.4, change end user to asset owner and clarify role; add latest version of 17011

Contents

FOREWORD

This is one of a series of documents that defines the ISASecure® CSA (Component Security Assurance) certification program for software applications, embedded devices, host devices, and network devices. These are the component types defined by the standard IEC 62443-4-2, that are used to build control systems. ISASecure CSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This is the highest level document that describes the overall CSA certification scheme and the scope for all other related documents. A description of the program and the current list of documents related to ISASecure CSA, as well as other ISASecure certification programs, can be found on the web site http://www.ISASecure.org.

1 Scope

The ISASecure® certification program has been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for Industrial Automation and Control Systems (IACS). The ISCI ISASecure CSA (Component Security Assurance) certification program achieves this goal by offering a common standards-based, industry-recognized set of component and process requirements that drive IACS component security, simplifying procurement for asset owners, and component assurance for product suppliers. A component that is certified to meet these requirements can display the ISASecure symbol.

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

2 Normative references

NOTE Section 4.5 provides a diagrammatic and expository overview of the ISASecure CSA 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 CSA certifier.

[CSA-200] *ISCI Component Security Assurance – ISASecure CSA 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 documents describe the ISASecure symbol and certificates and how they are used.

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

[CSA-205] *ISCI Component 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 component for ISASecure CSA certification.

2.3.1 General technical specifications

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

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

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

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

2.3.2 Specifications for certification elements

NOTE 1 The following documents provide the technical evaluation criteria for the Functional Security Assessment element of a CSA evaluation.

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

NOTE 2 The following documents provide the overall technical evaluation criteria for the Security Development Artifacts element of a CSA evaluation. [SDLA-312] also provides the technical evaluation criteria for the ISASecure SDLA certification of a supplier's secure product development lifecycle process.

[CSA-312] *ISCI Component Security Assurance – Security development artifacts for components,* 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 the VIT (vulnerability identification testing) element of a CSA evaluation.

[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 maintained outside of the ISASecure CSA program and are used by the program.

2.4.1 IACS security standards

NOTE 1 Section 4.3 describes the relationship of ISASecure CSA 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-62443-4-1] 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*

[ANSI/ISA-62443-4-2] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[IEC 62443-4-2] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

2.4.2 International standards for certification programs

NOTE 1 The following international standards apply to the ISASecure CSA 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 CSA 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 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 product 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
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.6
certifier
chartered laboratory, which is an organization that is qualified to certify products or supplier development processes as ISASecure

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

3.1.7
certificate

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

NOTE For ISASecure CSA, there are certificates for certified components and chartered laboratories.

3.1.8
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.

3.1.9
certification scheme

overall definition of and process for operating a certification program

3.1.10
certification level

capability security level for which conformance is demonstrated by a certification

NOTE It is intended that a component that achieves certification to CSA capability security level *n* will meet requirements for capability security level *n* as defined in IEC 62443-4-2 "Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components."

3.1.11 certified component

component that has undergone an evaluation by a chartered laboratory, has met the ISASecure CSA criteria and has been granted certified status by the chartered laboratory

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 conformity assessment body for the ISASecure certification programs.

3.1.13
conformity assessment

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

3.1.14
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

3.1.15
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 CSA, the conformity assessment body is a chartered laboratory.

3.1.16
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.

3.1.17
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.

3.1.18
end user
organization that purchases, uses, or is impacted by the security of IACS products

3.1.19
functional security assessment
assessment of a defined list of security features for a control system, or for a component of a control system

3.1.20
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.).

3.1.21
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

3.1.22
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.

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

3.1.24
product supplier
organization that is responsible for compliance of a product with ISASecure requirements

3.1.25
secure development artifacts
assessment of artifacts that demonstrates that secure product 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 product development process, for products which predate that process, but will be maintained under it going forward.

3.1.26
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.

3.1.27
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.

3.1.28
symbol

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

NOTE An earlier term for symbol is “mark.”

3.1.29
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.

3.1.30
update

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

3.1.31
upgrade

incremental hardware or software change in order to add new features

3.1.32
version (of component)

well defined release of a component, typically identified by a release number

3.1.33
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 CSA 1.0.0

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
EDSA	embedded device security assurance
FSA-C	functional security assessment for components
HMI	human-machine interface
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
SDA-C	security development artifacts for components
SDLA	security development lifecycle assurance
SIF	safety instrumented function
SIS	safety instrumented system
SSA	system security assurance
TS	technical specification
VIT-C	vulnerability identification test for components

4 ISASecure CSA certification program

4.1 Technical ISASecure CSA evaluation criteria

ISASecure CSA is a certification program for IACS components. An IACS component is an entity that is used to build control systems and that exhibits the characteristics of one or more of a software application, embedded device, host device, or network device. These component types are defined in [IEC 62443-4-2] and in 3.1 of the present document.

In order to obtain an ISASecure CSA certification, a supplier must hold an ISASecure SDLA (Security Development Lifecycle Assurance) development process certification such that the component to be evaluated is in the scope of that process. A supplier may at their option apply for CSA and SDLA certifications in parallel. ISASecure certification of components has three additional elements:

- Security Development Artifacts for components (SDA-C);
- Functional Security Assessment for components (FSA-C); and
- Vulnerability Identification Testing for components (VIT-C).

Both the SDLA certification evaluation and SDA-C 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-C examines the artifacts that are the outputs of the supplier's development processes as they apply specifically to the component to be CSA certified. FSA-C examines component security capabilities, incorporating requirements for all component types applicable to the product. VIT-C scans the component for the presence of known vulnerabilities.

The program defines four certification levels for a component, offering increasing levels of component security assurance. Levels offered are capability security levels 1, 2, 3, and 4. The corresponding certifications are called ISASecure CSA Capability Security Level 1, ISASecure CSA Capability Security Level 2, ISASecure CSA Capability Security Level 3, and ISASecure CSA Capability Security Level 4. A component that achieves CSA Capability Security Level *n* is certified to meet requirements for capability security level *n* as defined in [IEC 62443-4-2].

All levels of CSA certification include the certification elements above. SDLA certification does not have an associated level. SDA-C and VIT-C assessments are the same for all CSA certification levels with the exception of allowable residual risk for known security issues. FSA-C 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.

4.2 Certified components

The supplier for a component that has been evaluated under the ISASecure CSA 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 component, and references a 3-digit certification version that identifies the set of ISASecure specifications used for the certification. For example, component model 234, version 1.9 might be certified to ISASecure CSA 1.0.0 Capability Security Level 2. The program defines procedures to maintain certification for later versions of the component that incorporate component updates (3.1.30) and upgrades (3.1.31). The program also defines procedures to obtain certification to later versions of the ISASecure CSA evaluation program and to higher certification levels, based upon a prior certification.

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

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

A goal for the CSA certification program is to offer a compliance program for the ANSI/ISA/IEC 62443 series of standards, which address security for IACS. ISASecure CSA certification applies to software applications, embedded devices, host devices, and network devices, which are the four types of IACS components defined in those standards. Some certification requirements are common to all component types, and some are unique to particular component types, in accordance with the standards.

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 ISASecure SDLA certification requirements and SDA-C secure product development requirements for ISASecure CSA 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].

The ISASecure CSA FSA-C requirements and certification levels align with the requirements and capability security levels in the standard "IEC 62443-4-2 Security for industrial automation and control systems Part 4-

2: Technical security requirements for IACS components." ANSI/ISA has published this standard as [ANSI/ISA-62443-4-2].

4.4 Organizational roles

The following organizations participate in the ISASecure CSA 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 approve the system integrator's IACS protection concept and rationale, which may rely upon components certified to a specific security level. An entity may act both as an asset owner and a system integrator.
- **System integrators** use component certification information as a method for identifying components to be procured as part of an IACS solution, that provide necessary security capabilities to meet system requirements
- **Product suppliers** apply for certification of their components (supplier)
- **Chartered laboratories** for the CSA program, the CSA compliance authorities, which accept applications from product suppliers for certification, evaluate components, and are authorized to grant component certifications to product suppliers (conformity assessment body)
- **ISCI** defines, maintains, and manages the ISASecure certification programs, including ISASecure CSA, interprets the ISASecure specifications and maintains a web site for publishing program documentation, as well as lists of ISASecure chartered laboratories, ISASecure certified products and ISASecure certified supplier development processes
- **ASCI**, as the legal entity representing ISCI, grants chartered laboratory status to applicant organizations based on successful accreditation to criteria defined by ISCI
- **CSA accreditation bodies** evaluate candidates for chartered laboratory status and determine if they meet program accreditation criteria (accreditation body)

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

A CSA accreditation body will be an organization recognized by IAF/ILAC.

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

4.5 Certification program documentation

4.5.1 Overview of documentation

Figure 1 shows the documents that define the ISASecure CSA certification program. An arrow represents a referential dependency of a document on the contents of another document. Refer to Section 2 for the detailed bibliographic listing of these documents.

NOTE 1 [CSA-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 editable certificate template [CSA-205], and the policy document [ISASecure-117] which describes the transition from the prior ISASecure EDSA program to CSA.

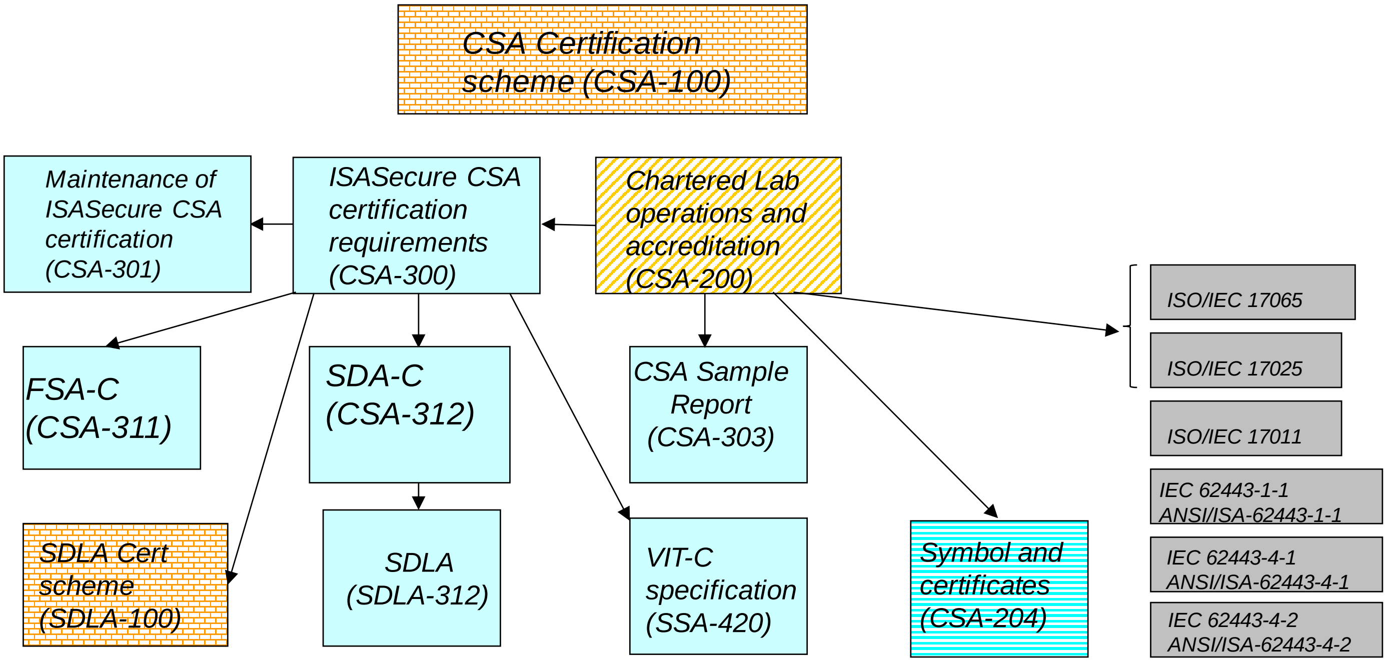
CSA Certification scheme (CSA-100)
Maintenance of ISASecure CSA certification (CSA-301)
ISASecure CSA certification requirements (CSA-300)
Chartered Lab operations and accreditation (CSA-200)
FSA-C (CSA-311)
SDA-C (CSA-312)
CSA Sample Report (CSA-303)
ISO/IEC 17065
ISO/IEC 17025
ISO/IEC 17011
IEC 62443-1-1 ANSI/ISA-62443-1-1
SDLA Cert scheme (SDLA-100)
SDLA (SDLA-312)
VIT-C specification (SSA-420)
Symbol and certificates (CSA-204)
IEC 62443-4-1 ANSI/ISA-62443-4-1
IEC 62443-4-2 ANSI/ISA-62443-4-2

Figure 1 - ISASecure CSA Documents

There are five major categories of ISASecure CSA program documents:

- **Technical specifications**, shown with no pattern in light blue, that describe the technical criteria applied to determine whether a component will be certified
- **Accreditation**, shown in gold diagonal stripe, that describe how an organization can become a chartered 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 and operate 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 prefixes “SSA” and “SDLA” are used both by those certification programs, respectively, as well as the CSA program. The following sections describe the documents in each category in further detail.

4.5.2 Technical specifications

The brief document [CSA-300] ISCI CSA - ISASecure Certification Requirements, defines at a high level the criteria for component certification, which simply stated, are for the product supplier's development organization to hold an SDLA certification for the development process used for the component, and for the component to pass SDA-C, FSA-C, and VIT-C. [CSA-300] points to the detailed documents on these topics as shown in Figure 1.

The SDLA specification [SDLA-312] provides requirements both on a supplier's secure product development lifecycle process and on the artifacts generated by these methods for a specific product. [SDLA-312] is used for SDLA certification and within a CSA evaluation for SDA-C. The SDA-C specification [CSA-312] is a brief document that points to the artifact requirements in [SDLA-312] which comprise the SDA-C criteria for CSA certification.

The document [CSA-311] defines the technical evaluation criteria for a component to pass FSA-C for each certification level. [SSA-420] defines the VIT test procedure and parameters for the vulnerability scanning policy to be used with the specified VIT tool to perform VIT-C.

The document [CSA-301] *ISCI CSA – Maintenance of ISASecure Certification*, describes the certification criteria and process for a modified component, where a previous version has already achieved certification. It also covers the process for upgrading a certification to a later ISASecure version (for example CSA 1.0.0 Capability Security Level 1 to CSA 2.0.0 Capability Security Level 1), or to a higher level (for example CSA 1.0.0 Capability Security Level 2).

These documents are used by:

- System integrators, to understand the meaning of various levels of ISASecure CSA certification and therefore the impact of a certified component on overall IACS security
- Asset owners need the general understanding that CSA certification provides assurance that a component meets IEC 62443-4-2 requirements, as stated in 4.1 of the present document. Certified components may in turn be relied upon by the system integrator to meet the asset owner's IACS requirements. An asset owner wishing to go deeper into component level requirements and how they are assured by CSA certification may review the CSA technical specifications.
- Product suppliers, to understand the criteria against which their products will be evaluated
- Chartered laboratories, to define evaluation processes and criteria
- CSA accreditation bodies, as the end reference for technical readiness assessment requirements when evaluating candidate organizations for chartered laboratory status.

The component evaluation report template/example [CSA-303] will be followed by chartered laboratories. It provides asset owners and product suppliers with an understanding of the type of information that will be provided to product suppliers following all component evaluations.

4.5.3 Accreditation

ISASecure CSA chartered laboratories implement the technical aspects of the certification program.

[CSA-200] *ISCI CSA – ISASecure CSA 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 CSA program, a laboratory shall attain the following internationally recognized accreditations, performed by a CSA accreditation body:

- accredited to IAF ISO/IEC 17065, with technology scope of accreditation covering ISASecure CSA certification, and
- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure CSA FSA-C and VIT-C specifications.

[CSA-200] details the requirements for chartered laboratory status, including interpretations of the above international standards for the ISASecure CSA 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

- CSA accreditation bodies, as the source for program specific requirements for the ISO/IEC 17065 and ISO/IEC 17025 accreditations listed above.

4.5.4 Symbol and certificates

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

Two types of ISASecure certificates are issued under the CSA program: for certified components and chartered laboratories.

The supporting document [CSA-205] *ISCI CSA – Certificate Document Format* is a convenient shorter document that contains an editable component certificate format template only.

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

- product 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 components
- chartered laboratories, to monitor for correct use of the symbol and component certificates by client product suppliers as required by [CSA-200].

These documents as they apply to chartered laboratories are used by:

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

4.5.5 Structure

Documents in the Structure category are the present document [CSA-100] and [SDLA-100] *ISCI SDLA – ISASecure certification scheme*. [CSA-100] is a publicly available reference to the structure of the overall ISASecure CSA program. [SDLA-100] is a publicly available reference to the structure of the overall SDLA certification program for supplier development processes. SDLA certification is a part of the CSA certification requirements, as described in [CSA-300].

4.5.6 External references

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

[ISO/IEC 17025] (which updates [ISO/IEC 17025 2005]) is an international standard that presents requirements for product testing programs. The requirements in this document apply to the FSA-C and VIT-C elements of ISASecure CSA. To obtain chartered status, chartered laboratories will demonstrate adherence to the requirements in these standards as part of the accreditation process.

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

Figure 1 refers to the standards from the 62443 series with which CSA certification aligns. The same technical standards are published by both IEC and ANSI/ISA using the same standard numbers 62443-m-n.

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

The technical standard published as [IEC 62443-4-1] and [ANSI/ISA-62443-4-1] covers requirements for the secure product development lifecycle for suppliers developing industrial control system products. The requirements in [SDLA-312] used for SDLA certification and SDA-C are derived from this standard.

The technical standard published as [IEC 62443-4-2] and [ANSI/ISA-62443-4-2] covers technical security requirements that apply for IACS components. Components are categorized as software applications, embedded devices, host devices, or network devices, and may belong to more than one category. The requirements in [CSA-311] used for FSA-C are derived from this standard.