ICSA-100

ISA Security Compliance Institute — IIoT Component Security Assurance –

ISASecure® certification scheme

Version 1.1

December 2022

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	2022.12.04	Initial version published to https://www.isasecure.org/

Contents

1 Scope 6

2 Normative references 6

2.1 Accreditation 6

2.2 ISASecure symbol and certificates 6

2.3 Technical specifications 6

2.4 External references 7

3 Definitions and abbreviations 8

3.1 Definitions 8

3.2 Abbreviations 14

4 ISASecure ICSA certification program 14

4.1 Technical ISASecure ICSA evaluation criteria 14

4.2 Certified components 15

4.3 Relationship of the ICSA program to ANSI/ISA/IEC 62443 16

4.4 Organizational roles 16

4.5 Certification program documentation 17

FOREWORD

This is one of a series of documents that defines the ISASecure® ICSA (IIoT Component Security Assurance) certification program for IIoT (Industrial Internet of Things) devices and gateways. These product types are defined in the present specification. They are subtypes of the product types: embedded devices, host devices, and network devices, defined in the standard IEC 62443-4-2. ISASecure ICSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This is the highest level document that describes the overall ICSA certification scheme and the scope for all other related documents. A description of the program and the current list of documents related to ISASecure ICSA, as well as other ISASecure certification programs, can be found on the website https://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 ICSA (IIoT Component Security Assurance) certification program achieves this goal by offering a common standards-based, industry-recognized set of component and process requirements that drive IIoT (Industrial Internet of Things) component security, simplifying procurement for asset owners, and component assurance for product suppliers. IIoT devices and IIoT gateway devices, as defined in this document, are eligible for ICSA certification. A component that is certified to meet ICSA requirements can display the ISASecure symbol. ICSA certification is primarily based on the 62443 standard; the relationship of ICSA to 62443 is described in 4.3.

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 ICSA documents and their relationships.

2.1 Accreditation

2.1.1 Chartered laboratory operations and accreditation

NOTE 1 The following documents describe how to achieve chartered laboratory status and operate as an ISASecure ICSA certifier.

NOTE 2 Accreditation for ISASecure CSA as described in [CSA-200] is a prerequisite to accreditation for ISASecure ICSA.

[ICSA-200] *ISCI IIoT Component Security Assurance – ISASecure ICSA chartered laboratory operations and accreditation,* as specified at https://www.ISASecure.org

[CSA-200] *ISCI Component Security Assurance – ISASecure ICSA chartered laboratory operations and accreditation,* as specified at https://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.

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

[ICSA-205] *ISCI IIoT Component Security Assurance – Certificate Document Format,* as specified at https://www.ISASecure.org

2.3 Technical specifications

NOTE This section includes the specifications that define technical criteria for evaluating a component for ISASecure ICSA certification.

2.3.1 General technical specifications

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

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

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

[ICSA-303] *ISASecure ICSA 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 (FSA-IC) of an ICSA evaluation.

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

[ICSA-500] *ISCI IIoT Component Security Assurance – Selected commonly accepted security practices*, available at https://www.ISASecure.org

NOTE 2 The [SDLA-312] and [ISDLA-312] documents contain identical information that is used for SDLA certification (SDLPA-IC). They differ in that [SDLA-312] is the reference for the SDA (Security Development Artifacts) element of CSA called SDA-C, and [ISDA-312] is the reference for the SDA element of ICSA, called SDA-IC.

[ICSA-312] *ISCI IIoT Component Security Assurance – Security development artifacts for IIoT components,* as specified at https://www.ISASecure.org

[ISDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment for IIoT components*, as specified at https://www.ISASecure.org

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

2.3.3 Vulnerability identification testing specification

NOTE The following document describes the procedures and policy parameter values used to perform the VIT (vulnerability identification testing) element of an ICSA evaluation (VIT-IC).

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

2.4 External references

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

2.4.1 IACS security standards

NOTE 1 Section 4.3 describes the relationship of ISASecure ICSA 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 The following international standards apply to the ISASecure ICSA 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*"**,** November 2017

2.4.3 International standards for accreditation programs

[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 applicati on

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.

[SOURCE IEC 62443-4-2]

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

[SOURCE text in 62443-3-3 A.2.2]

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 ICSA, 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 certified component

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

3.1.11
chartered laboratory

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

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

3.1.12
conformity assessment

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

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

[SOURCE IEC 62443-4-2]

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 ICSA, the conformity assessment body is a chartered laboratory.

3.1.15
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.

[SOURCE IEC 62443-4-2]

3.1.16
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.

[SOURCE IEC 62443-4-2]

3.1.17
end user
organization that purchases, uses, or is impacted by the security of IACS products

3.1.18
functional security assessment
assessment of a defined list of security features for a control system, or for a component of a control system

3.1.19
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.).

[SOURCE IEC 62443-4-2]

3.1.20
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

[SOURCE IEC 62443-4-2]

3.1.21
IIoT (Industrial Internet of Things)
system that connects and integrates industrial control systems with enterprise systems, business processes and analytics

[SOURCE IIC The Industrial Internet of Things G8: Vocabulary V2.1]

3.1.22
IIoT device
entity that is a sensor or actuator for a physical process, or communicates with sensors or actuators for a physical process, that directly connects to an untrusted network to support and/or use data collection and analytic functions accessible via that network

NOTE 1 This definition adds detail for the purposes of the present document, to the definition from ISO/IEC FDIS 20924, 3.2.4 for IoT, which reads “entity of an IoT system that interacts and communicates with the physical world through sensing or actuating.” The 20924 definition does not specify connection to an untrusted network.

NOTE 2 Examples of IIoT devices that communicate with sensors or actuators are a PLC with an internet connection, and an IIoT integrated edge computing device (see 3.1.24).

3.1.23
IIoT gateway
entity of an IIoT system that connects one or more proximity networks and the IIoT devices on those networks to each other and directly connects to one or more untrusted access networks

NOTE 1 This definition is from ISO/IEC FDIS 20924, except that IoT is replaced by IIoT, and the qualifications “directly” and “untrusted” have been added for the purposes of this document.

NOTE 2 From [IICRA]: “The proximity network connects the sensors, actuators, devices, control systems and assets, collectively called edge nodes.”

NOTE 3 An IIoT gateway device is a type of network device (see 3.1.26).

NOTE 4 Functions hosted on an IIoT gateway device may also include data translation, processing and control.

3.1.24
IIoT integrated edge computing device
IIoT device that communicates with other IIoT devices and includes either or both of: environment for hosting application software or pre-defined application software

NOTE 1 The reader is advised that terminology usage in the IoT arena is not standardized at this time, so that other sources may use other terms for this concept.

NOTE 2 Examples of application software are analytics and data filtering. Device may include IIoT gateway functionality to transmit sensor information or derivative information to the cloud, may provide instructions to sensors, actuators, controllers, or other IIoT integrated edge computing devices, application environment may consist of virtual machines and/or a container environment, may use wired communication, or cellular or other wireless communication.

NOTE 3 An example IIoT integrated edge computing device might include sensor connections providing data for a “local” processing capability on the device, and a connection to the cloud for “remote” processing of some version of that data. In this example, the IIoT integrated edge computing device would meet 62443 definitions for network device and host (if it includes an environment for hosting application software) or software application (if it includes pre-defined applications).

3.1.25
IIoT system
system providing functionalities of Industrial Internet of Things

NOTE IIoT system is inclusive of IIoT devices, IIoT gateways, sensors, actuators, analytics and processing software together with its hardware/software environment, and related human interfaces.

[SOURCE ISO/IEC FDIS 20924, 3.2.7 (for IoT, incorporating additions to NOTE)]

3.1.26
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.

[SOURCE IEC 62443-4-2]

3.1.27
pass
meet the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.28
product supplier
organization that is responsible for compliance of a product with ISASecure requirements

3.1.29
proximity network
network that connects the sensors, actuators, devices, control systems and assets

NOTE 1 The proximity network typically connects these nodes, as one or more clusters related to a gateway that bridges to other networks.

NOTE 2 Variant of term “proximity defined network,” in ISO/IEC TR 29181-9:2017 *Information technology — Future Network — Problem statement and requirements — Part 9: Networking of everything*, which reads “network configured among devices in close proximity, using conventional LAN or WAN technologies: which are in not only physically close proximity, but also closely related, or logically close proximity.”

[SOURCE text in [IICRA]]

3.1.30
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.

3.1.31
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.

[SOURCE IEC 62443-3-3]

3.1.32
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.

[SOURCE IEC 62443-4-2]

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 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.

[SOURCE IEC 62443-4-1]

3.1.35
tier
designation to identify a set of certification criteria, where any two tiers are comparable under some ordering scheme

NOTE ISASecure ICSA offers certification to Core tier or Advanced tier. Advanced is the higher tier, as it encompasses more requirements than Core tier.

3.1.36
trust
confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

NOTE 1: An entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.

NOTE 2: Trust may apply only for some specific function.

[SOURCE IEC 62443-4-2]

3.1.37
untrusted
not meeting predefined requirements to be trusted

NOTE 1 An entity may simply be declared as untrusted.

NOTE 2 A common use of this term for ICSA is in the phase “untrusted network” or “untrusted connection,” which defines the security posture assumed for networks to which a component is designed to connect, as declared by the product supplier. ([ICSA-300] requirement ICASecure_IC.R4 requires such a declaration.) Networks accessible to the public, such as the internet or cell networks to which a component connects, are expected to be declared as untrusted. Networks to which a component connects that are identified as untrusted may also include, but are not limited to, internal enterprise networks that may not be under the full control of the asset owner responsible for the cybersecurity impact of the IIoT component. These enterprise networks may be controlled by the asset owner's overall enterprise or by another enterprise such as a partner or vendor. Some ICSA functional security requirements only apply to component interfaces declared to support direct connections to untrusted networks.

[SOURCE 62443-4-2 NOTE 2 added]

3.1.38
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

[SOURCE IEC 62443-4-2]

3.1.39
upgrade
incremental hardware or software change in order to add new features

[SOURCE IEC 62443-4-2]

3.1.40
version (of component)
well defined release of a component, typically identified by a release number

3.1.41
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 ICSA 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
FDIS	final draft international standard
FSA-IC	functional security assessment for IIoT components
HMI	human-machine interface
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
ICSA	IIoT Component Security Assurance
IEC	International Electrotechnical Commission
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
ILAC	International Laboratory Accreditation Cooperation
IoT	Internet of Things
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
SDA-IC	security development artifacts for IIoT components
SDLA	security development lifecycle assurance
SDLPA-IC	security development lifecycle process assessment for IIoT components
SIF	safety instrumented function
SIS	safety instrumented system
SMA	security maintenance audit
SSA	system security assurance
TR	technical report
TS	technical specification
VIT-IC	vulnerability identification test for IIoT components

4 ISASecure ICSA certification program

4.1 Technical ISASecure ICSA evaluation criteria

ISASecure ICSA is a certification program for IIoT devices and IIoT gateways. ICSA certification applies to IACS components that:

- meet the [IEC 62443-4-2] definition for at least one of *embedded device*, *host device*, or *network device*; and

- meet the definition in 3.1 of this document for at least one of *IIoT device* or *IIoT gateway*.

In accordance with the definitions in 3.1, IIoT devices and IIoT gateways are intended to support direct connection to an untrusted network.

ICSA applies to physical devices only. However, if a physical device eligible for ICSA certification also includes a software application, then 62443-4-2 requirements for software applications will be part of the ICSA certification. An IIoT integrated edge computing device (3.1.24) is a type of IIoT device, hence is within the scope of ICSA certification.

In order to obtain an ISASecure ICSA 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. This criterion is called SDLPA-IC (Security Development Lifecycle Process Assessment for IIoT components). A supplier may at their option apply for ICSA and SDLA certifications in parallel. ISASecure ICSA certification of components has three additional elements:

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

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

An ICSA certification has an associated certification tier, which may be Core tier or Advanced tier. Both tiers of ICSA certification include the certification elements above. The required underlying SDLA certification does not have an associated tier. SDA-IC and VIT-IC assessments are the same for both ICSA tiers with the exception of allowable residual risk for known security issues. FSA-IC incorporates more requirements for Advanced tier than for Core tier.

NOTE In ISDLA-312 v6.3, the treatment of residual risk related to known security issues is found in SDLA requirement SDLA-DM-4-ICSA1.

4.2 Certified components

The supplier for a component that has been evaluated under the ISASecure ICSA 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 ICSA 1.0.0 Core tier.

The program defines procedures in [ICSA-301] to maintain certification for later versions of the component that incorporate component updates (3.1.38) and upgrades (3.1.39). To maintain validity of a certification for a component and its upgrades, the supplier undergoes a periodic surveillance evaluation of the supplier's security maintenance practices as applied to products holding ICSA certification, called Security Maintenance Audit (SMA). A supplier must maintain their SDLA certification and maintain good standing under SMA for a product, in order for that product and its upgrades to maintain ICSA certification.

[ICSA-301] also defines procedures to obtain certification to later versions of the ISASecure ICSA evaluation program and to obtain Advanced tier certification, based upon a prior Core tier certification. A streamlined procedure is also defined for a product that holds a CSA certification, to obtain an ICSA certification.

ISCI will post the names of certified components on its website https://www.ISASecure.org.

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

ICSA is primarily based upon the standard "IEC 62443-4-2 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components," also published by ANSI/ISA as [ANSI/ISA-62443-4-2]. ICSA incorporates a relatively small number of exceptions and extensions to this standard to address the IIoT component environment. These modifications were identified as part of a joint study carried out by ISCI and the ISA Global Cybersecurity Alliance. The goal for the study is to determine the applicability of 62443 standards and certifications to IIoT components and systems. Quoting from the executive summary of the phase 1 study report, which addressed IIoT devices and gateways [IIoTCert2021]:

"The study concluded that a certification that addresses such IIoT devices and gateways could be constructed based upon existing 62443-4-2 certification programs, by incorporating a manageable number of program enhancements. The delta defined in this paper to existing 62443 certification programs is offered to contribute to the dialog regarding application and revision of 62443 for IIoT, looking forward to future IIoT product certifications based solely on that standard. In the near term, it provides a proposal for standardization and therefore the possibility of comparison across IIoT certification offerings, where such certifications may be offered prior to availability of 62443 updates for IIoT."

The ICSA certification program structure of two tiers as compared to the four security levels of 62443-4-2, is driven by the known risks for IIoT devices and gateways directly connected to untrusted networks. FSA-IC requirements and associated tiers are documented in [ICSA-311]. FSA-IC for ICSA Core tier requires conformance to all capability security level 2 requirements in 62443-4-2, with one exception for IIoT gateways, and two for IIoT devices. Core tier also adds a few requirements from levels 3 and 4 in acknowledgment of the threat posed by the component's connection to the Internet or other untrusted network. Advanced tier requires conformance to all capability security level 4 requirements with four exceptions. Overall, all 62443-4-2 requirements with the exception of 5 are incorporated in ICSA. The ISCI/ISAGCA study also recommended sixteen requirements that were not found among the (126) requirements in 62443-4-2. These additions are refined and incorporated in ICSA. Study methodology and rationale for resulting recommendations is provided in [IIoTCert2021].

ICSA is modeled after the ISASecure CSA certification program (Component Security Assurance), which certifies conformance to 62443-4-2 for software applications, embedded devices, host devices, and network devices. Much of the CSA program has been reapplied for ICSA, as the two programs have the majority of their requirements in common. The document [ISASecure-119] provides a detailed comparison of these two programs and summarizes the ICSA exceptions and extensions to 62443-4-2.

In particular, supplier certification of secure product development lifecycle practices to 62443-4-1 is a prerequisite for CSA certification, and remains so for ICSA. The ISASecure SDLA certification requirements fully 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]. Although ICSA SDA-IC evaluates a small number of lifecycle practices not required by 62443-4-1, these apply for ICSA product certification only, and do not affect SDLA certification.

4.4 Organizational roles

The following organizations participate in the ISASecure ICSA 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 tier. 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 ICSA program, the ICSA conformance 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 ICSA, interprets the ISASecure specifications and maintains a website for publishing program documentation, as well as lists of ISASecure chartered laboratories, ISASecure certified products and ISASecure certified supplier development processes (scheme owner)

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

- **ICSA 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: https://www.ISASecure.org.

An ICSA 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 ICSA 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 [ICSA-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 document [CSA-200] covering CSA accreditation, the editable certificate template [ICSA-205], and [SDLA-312], which is equivalent to [ISDLA-312] as used for SDLPA-IC.

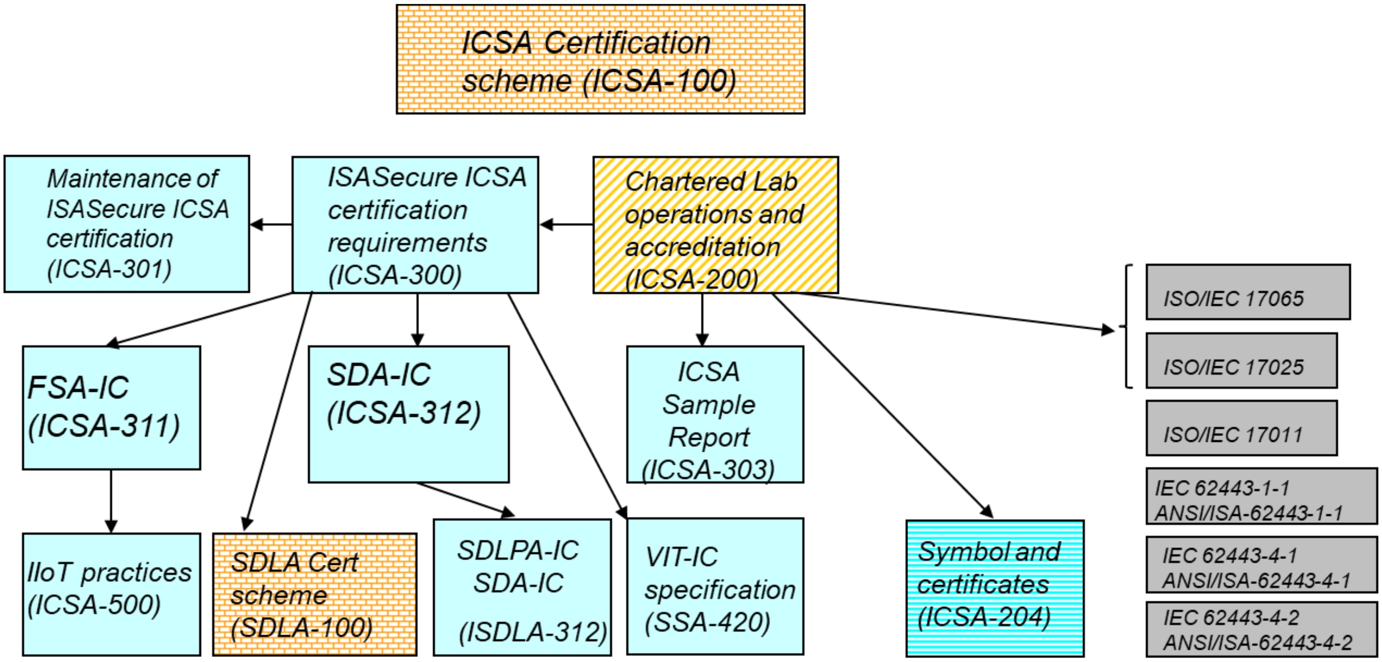
ICSA Certification scheme (ICSA-100)
Maintenance of ISASecure ICSA certification (ICSA-301)
ISASecure ICSA certification requirements (ICSA-300)
Chartered Lab operations and accreditation (ICSA-200)
ISO/IEC 17065
ISO/IEC 17025
ISO/IEC 17011
IEC 62443-1-1 ANSI/ISA-62443-1-1
IEC 62443-4-1 ANSI/ISA-62443-4-1
IEC 62443-4-2 ANSI/ISA-62443-4-2
FSA-IC (ICSA-311)
SDA-IC (ICSA-312)
ICSA Sample Report (ICSA-303)
IIoT practices (ICSA-500)
SDLA Cert scheme (SDLA-100)
SDLPA-IC SDA-IC (ISDLA-312)
VIT-IC specification (SSA-420)
Symbol and certificates (ICSA-204)

Figure 1 - ISASecure ICSA Documents

There are five major categories of ISASecure ICSA 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 ICSA program. The following sections describe the documents in each category in further detail.

4.5.2 Technical specifications

The brief document [ICSA-300] *ISCI ICSA - 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 (this criterion is called SDLPA-IC), and for the component to pass SDA-IC, FSA-IC, and VIT-IC. [ICSA-300] points to the detailed documents on these topics as shown in Figure 1.

The SDLA specification [ISDLA-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. [ISDLA-312] is used for SDLA certification and within an ICSA evaluation for SDA-IC. The [SDLA-312] document used for the CSA certification program and the [ISDLA-312] document contain identical information that is used for SDLA certification (SDLPA-IC). The SDA-IC specification [ICSA-312] is a brief document that identifies the artifact requirements in [ISDLA-312] which comprise the SDA-IC criteria for ICSA certification.

The document [ICSA-311] defines the technical evaluation criteria for a component to pass FSA-IC for each tier. For some requirements in [ICSA-311], evaluation criteria refer to [ICSA-500] which provides examples of commonly accepted IIoT security practices. [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-IC.

The document [ICSA-301] *ISCI ICSA – 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 ICSA 1.0.0 Core tier to ICSA 2.0.0 Core tier), or from ICSA Core tier to Advanced tier. [ICSA-301] also describes the process for a product with CSA certification to obtain ICSA certification.

These documents are used by:

- System integrators, to understand the meaning of ISASecure ICSA certification tiers and therefore the impact of a certified component on overall IACS security

- Asset owners need the general understanding that ICSA certification provides assurance that a component meets, at a minimum, all IEC 62443-4-2 requirements at level 2 with two exceptions for IIoT devices and one for IIoT gateways, and meets additional requirements tailored for IIoT components, as stated in 4.3 of the present document. Certified components may in turn be relied upon by the system integrator to meet the asset owner’s IIoT solution requirements. An asset owner wishing to go deeper into component level requirements and how they are assured by ICSA certification may review the ICSA technical specifications.

- Product suppliers, to understand the criteria against which their products will be evaluated

- Chartered laboratories, to define evaluation processes and criteria

- ICSA 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 [ICSA-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 ICSA chartered laboratories implement the technical aspects of the certification program.

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

- accredited to IAF ISO/IEC 17065, with technology scope of accreditation covering ISASecure ICSA certification, and

- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure ICSA FSA-IC and VIT-IC specifications.

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

- ICSA 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 [ICSA-204] *ISCI ICSA – 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 ICSA program: for certified components and chartered laboratories.

The supporting document [ICSA-205] *ISCI ICSA – 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 [ICSA-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 [ICSA-100] and [SDLA-100] *ISCI SDLA – ISASecure certification scheme*. [ICSA-100] is a publicly available reference to the structure of the overall ISASecure ICSA 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 ICSA certification requirements, as described in [ICSA-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] is an international standard that presents requirements for product testing programs. The requirements in this document apply to the FSA-IC and VIT-IC elements of ISASecure ICSA. 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 ICSA accreditation bodies and ASCI to define their accreditation operations for the ISASecure ICSA certification program.

Figure 1 refers to the standards from the 62443 series which are the source for the majority of ICSA certification requirements. 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-IC evaluation, and defines the concept of essential functions, as well as the concept of security levels that forms the basis for ICSA tier definitions.

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 [ISDLA-312] used for SDLA certification, and the majority of requirements used for SDA-IC, 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 majority of requirements in [ICSA-311] used for FSA-IC are derived from this standard.

Bibliography

[IICRA] Industrial Internet Consortium Reference Architecture, available at https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[IIoTCert2021] IIoT Component Certification Based on the 62443 Standard, ISA Security Compliance Institute and ISA Global Security Alliance, available at https://gca.isa.org/iiot-component-certification-based-on-62443

[ISASecure-119] ISA Security Compliance Institute – Comparison of IIoT Component Security Assurance and Component Security Assurance Certifications, available at https://www.ISASecure.org