ICSA-300

ISA Security Compliance Institute – IIoT Component Security Assurance –

ISASecure® certification requirements

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

Certification requirements

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 one 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). The present specification is the overarching document in the series that describes technical requirements for certification. It references all other documents that contain these requirements and places them in context. The current list of documents related to ISASecure ICSA certification and other ISASecure certification programs can be found on the web site https://www.ISASecure.org.

1 Scope

This document specifies the criteria for granting an initial ISASecure® ICSA (IIoT Component Security Assurance) certification that is applicable to the subset of IACS (Industrial Automation and Control System) IIoT (Industrial Internet of Things) components that meet eligibility criteria defined in this specification. 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 the standard [IEC 62443-4-2] and in 3.1 of the present document. 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 as specified in Table 1 below. An IIoT integrated edge computing device (3.1.12) is a type of IIoT device, hence is within the scope of ICSA certification.

To specify ICSA certification criteria, this document references other specification documents that cover detailed requirements for the following elements of certification:

- Security Development Lifecycle Process Assessment for IIoT components (SDLPA-IC);

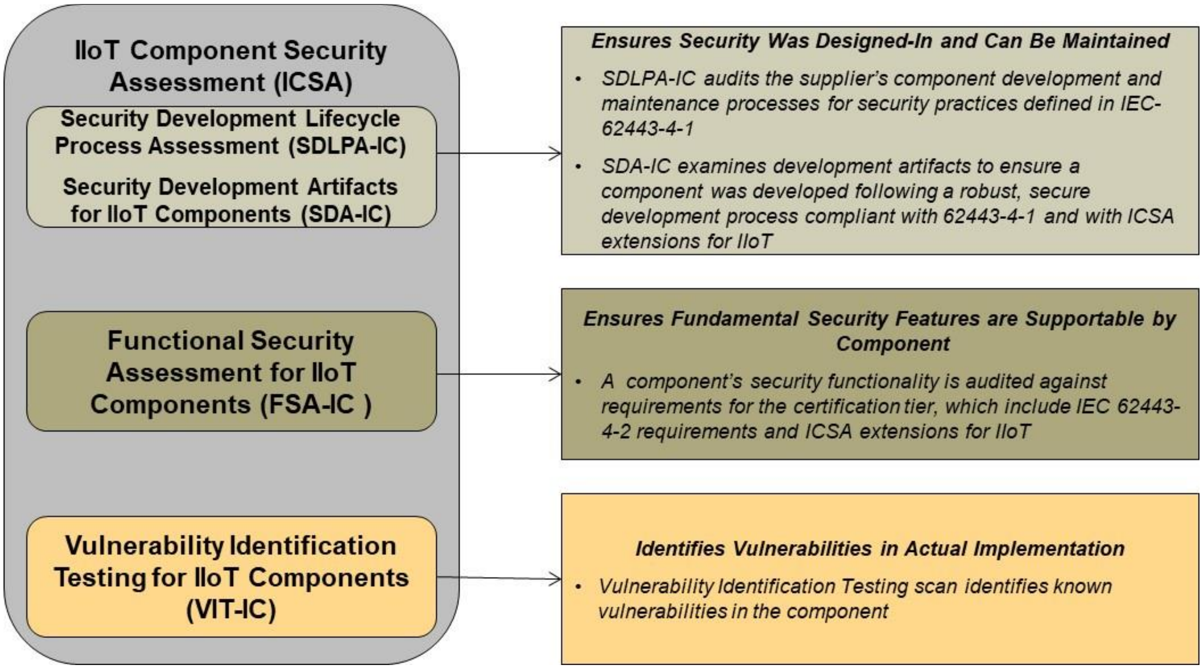
- Security Development Artifacts for IIoT components (SDA-IC);

- Functional Security Assessment for IIoT components (FSA-IC); and

- Vulnerability Identification Testing for IIoT components (VIT-IC).

While SDLPA-IC is an evaluation of the product supplier's secure product development lifecycle process for conformance to [IEC 62443-4-1], SDA-IC examines the artifacts that are the outputs of that process for the component to be certified. FSA-IC examines the security capabilities of the component. In accordance with [IEC 62443-4-2], requirements for security functionality differ based upon 62443-4-2 component type, that is, whether the component is an embedded device, host device, network device, and/or software application. FSA-IC will examine functional capabilities of a product based on its 62443-4-2 component type(s) and whether it is an IIoT device and/or an IIoT gateway. VIT-IC scans the component for the presence of known vulnerabilities.

The following figure illustrates the elements of ISASecure ICSA certification. SDA-IC and FSA-IC incorporate exceptions and extensions to the requirements in the standards [IEC 62443-4-1] and [IEC 62443-4-2], to address the IIoT environment.



IIoT Component Security Assessment (ICSA)
Security Development Lifecycle Process Assessment (SDLPA-IC)
Security Development Artifacts for IIoT Components (SDA-IC)
Functional Security Assessment for IIoT Components (FSA-IC)
Vulnerability Identification Testing for IIoT Components (VIT-IC)

Ensures Security Was Designed-In and Can Be Maintained

- *SDLPA-IC audits the supplier's component development and maintenance processes for security practices defined in IEC-62443-4-1*
- *SDA-IC examines development artifacts to ensure a component was developed following a robust, secure development process compliant with 62443-4-1 and with ICSA extensions for IIoT*

Ensures Fundamental Security Features are Supportable by Component

- *A component's security functionality is audited against requirements for the certification tier, which include IEC 62443-4-2 requirements and ICSA extensions for IIoT*

Identifies Vulnerabilities in Actual Implementation

- *Vulnerability Identification Testing scan identifies known vulnerabilities in the component*

Figure 1 - Evaluation Elements for ISASecure ICSA Certification

Once initial certification for a component is achieved as described in the present document, then modified versions of the component may maintain certification as described in the separate document [ICSA-301] *ISA Security Compliance Institute IIoT Component Security Assurance – Maintenance of ISASecure certification*. That document is summarized as follows, where the terms *update* (e.g., a bug fix) and *upgrade* (e.g., addition of a new feature set) are defined in [IEC 62443-4-2] and in 3.1 below:

- For an update of a certified product to maintain its product certification, or an upgrade to obtain a new certification, the supplier maintains a certified development process compliant with [IEC 62443-4-1], that is applied to these releases.
- The Security Maintenance Audit (described below) for the certified product, remains in good standing. This and the above criterion suffice for a product and its updates to retain certified status.
- An upgrade of the product requires additional assessment in order to maintain the product certification but may use the initial certification evidence for the product as partial evidence toward certification.

Security Maintenance Audit (SMA) is a periodic evaluation of the supplier's security maintenance practices for ICSA certified products. [ICSA-301] provides details of the SMA process.

ISASecure ICSA certification is distinct from ISASecure CSA (Component Security Assurance) certification, which verifies conformance with 62443-4-2. [ICSA-301] describes the process for a product with CSA certification to obtain ICSA certification. At a high level, an ICSA Core tier certification (as defined in 4.2) requires meeting most CSA capability level 2 certification requirements, together with some extensions to both functional and lifecycle requirements. Likewise, ICSA Advanced tier requires meeting most CSA capability security level 4 certification requirements, together with extensions to functional and lifecycle requirements. [ICSA-100] describes the relationship of ICSA with the 62443 standard; [ISASecure-119] compares ISASecure ICSA with ISASecure CSA in requirement-by-requirement detail. There is no difference between SDLPA-C for CSA and SDLPA-IC for ICSA; for both certifications these criteria require a supplier organization to hold an ISASecure SDLA process certification as a prerequisite for any product certification.

2 Normative references

2.1 Technical specifications

[ICSA-100] *ISCI IIoT Component Security Assurance – ISASecure certification scheme*, as specified at https://www.ISASecure.org

NOTE 1 The following specifications define the SDLPA-IC and SDA-IC elements of the ISASecure IIoT component certification.

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 [ISDLA-312] is the reference for the SDA element of ICSA, called SDA-IC.

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure certification scheme*, as specified at https://www.ISASecure.org

[ISDLA-312] *ISCI IIoT Security Development Lifecycle Assurance – Security development lifecycle assessment for ICSA, 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

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

NOTE 3 The following specification defines the FSA-IC element of the ISASecure IIoT component certification.

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

NOTE 4 The following specification defines the VIT-IC element of the ISASecure IIoT component certification.

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

2.2 IACS security standards

NOTE 1 [ICSA-100] describes the relationship of ISASecure ICSA to these 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*

3 Definitions and abbreviations

3.1 Definitions

Those terms defined in sources external to ISASecure specifications, indicate the source for their definitions.

3.1.1
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]

3.1.2
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.

3.1.3
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]

3.1.4
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]

3.1.5
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]

3.1.6
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]

3.1.7
independent test

form of requirements verification that requires the certifier’s direct exercise of the entity under evaluation, or exercise of a development tool used by the supplier of that entity

NOTE In contrast, some requirements may be validated by an examination of documents alone.

3.1.8
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]

3.1.9
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]

3.1.10
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 3.1.12).

3.1.11
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 3.1.16).

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

3.1.12
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).

3.1.13
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)]

3.1.14
initial certification

certification where the ISASecure certification process does not take into account any prior ISASecure certifications of the entity under evaluation or of any prior versions of the entity

3.1.15
ISASecure version

identifier for the 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

3.1.16
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]

3.1.17
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]]

3.1.18
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]

3.1.19
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.

3.1.20
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]

3.1.21
untrusted

not meeting predefined requirements to be trusted

NOTE 1 An entity may simply be declared as untrusted.

NOTE 2 For ICSA, a common use of this term 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 declared as untrusted may also include, but are not limited to, internal enterprise networks that are not 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 IEC 62443-4-2, Note 2 added]

3.1.22
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

[SOURCE IEC 62443-4-2]

3.1.23
upgrade
incremental hardware or software change in order to add new features

[SOURCE IEC 62443-4-2]

3.2 Abbreviations

The following abbreviations are used in this document

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CSA	component security assurance
DCS	distributed control system
FSA-IC	functional security assessment for IIoT components
HMI	human machine interface
IACS	industrial automation and control system
ICSA	IIoT component security assurance
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
OS	operating system
PLC	programmable logic controller
SDA-IC	security development artifacts for IIoT components
SDLA	security development lifecycle assurance
SDLPA-C	security development lifecycle process assessment for components
SDLPA-IC	security development lifecycle process assessment for IIoT components
SIF	safety instrumented function
SIS	safety instrumented system
TR	technical report
VIT-C	vulnerability identification test for components
VIT-IC	vulnerability identification test for IIoT components

4 Background

4.1 Program implementation

The ISASecure 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. ISASecure ICSA certification achieves this goal by offering a common industry-recognized set of component and process requirements that drive component security, simplifying procurement for asset owners, and component assurance for product suppliers.

ASCI (Automation Standards Compliance Institute) will accredit private organizations to perform ISASecure certification evaluations as “certifiers”.

NOTE ISCI is organized under the umbrella structure provided by ASCI.

ASCI grants accredited certifiers the right to grant ISASecure ICSA certifications for IIoT components based upon the certifier’s tests and assessments conforming to ISASecure specifications listed in Clause 2. ISCI will publish a list of certified products on its website.

4.2 Certification tiers

The ICSA program defines two certification tiers for a component, offering two grades of security assurance. The tiers offered are Core and Advanced. The corresponding certifications are called ISASecure ICSA Core tier and ISASecure ICSA Advanced tier. An ICSA certification earned by a particular product will indicate the applicable component type(s) and tier, and thus be expressed for example, as ISASecure ICSA Core tier (IIoT Gateway). The document [ICSA-100] further describes the relationship between tiers for ICSA certification, and capability security levels in [IEC 62443-4-2].

Both certification tiers include the certification elements defined in Clause 1. SDLPA-IC is the same regardless of tier. SDA-IC and VIT-IC assessments are the same for both 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, certifier validation for requirement SDLA-DM-4-ICSA1 which applies for SDA-IC, differs by tier. SDLA-DM-4-ICSA1 states that products certified to Advanced tier require lower residual risk than those certified to Core tier, in particular where this risk is affected by the severities of unmitigated vulnerabilities identified in the product.

5 Certification requirements

5.1 Certification tier and version

Requirement ISASecure_IC.R1 – Application for a certification tier

When a supplier applies for certification of a component, the certification applicant SHALL specify the highest tier for which they would like to achieve component certification. The tiers possible are Core or Advanced. The certifier SHALL award certification to a component at the highest tier for which the component qualifies.

Requirement ISASecure_IC.R2 – Prior certifications

When applying for ISASecure certification of a component, the applicant SHALL specify one of:

- this is an initial certification
- this component or an earlier version has achieved an ISASecure CSA or ICSA certification, which is offered as evidence toward this certification.

NOTE 1 As discussed in Clause 1, the separate document [ICSA-301] defines certification criteria for the second case.

Requirement ISASecure_IC.R3 – Publication of component certification status

If ISCI, the certifier, or the component supplier publishes certification status information for certified components in a public venue, information provided SHALL specify the version(s) of the component to which the ISASecure ICSA certification applies, and the version of the certification achieved, such as ISASecure ICSA 1.0.0.

NOTE 2 It is not necessary to list all certified product versions, but rather to indicate the versions in scope for the certification in some manner, such as 3.1.x.

5.2 Initial certification

Requirement ISASecure_IC.R4 – ISASecure application requirements for an initial certification

Items specified as follows SHALL be submitted to the ISASecure ICSA certification process by an applicant for an initial certification:

a) List of essential functions of the component, in accordance with the definition in 3.1.5, including (optionally) a list of events where associated event record data is considered to be essential history data

b) Component product hardware and/or software, that is or will be unambiguously identifiable and specifiable by an end customer for procurement, in a hardware/software configuration that enables all of the procured software functionality of the product (for certifier testing under FSA-IC and VIT-IC)

c) End user documentation for the component, (printed, on-line or otherwise) that is delivered along with, or made available to, an end customer who purchases the product submitted for certification

d) List of end user accessible interfaces and implemented IP protocols, which should include all interfaces such that:

- the supplier recommends the interface to customers as suitable for use during operation or maintenance; and
- the interface supports any IP protocol, for operation or instrumentation; and
- connection to the interface can occur without physical reconfiguration of the normal operational configuration.

e) Those end user accessible interfaces identified as supported for direct connection to an untrusted network

f) Description of any intended component defensive behavior, which is information for each IP protocol supported by the component, that indicates one of:

- traffic received under that protocol is not subject to rate limiting, in other words the design of the component does not distinguish between rates of incoming traffic
- traffic received by the component is subject to rate limiting.

g) Other technical items as required by the specifications listed in Clause 2; and

h) Administrative and potentially additional technical items defined by the certifier.

NOTE: The effect of identifying an interface to an untrusted network is that this interface will be in scope for certification criteria that explicitly refer to untrusted network connections.

The certifier SHALL in the course of certification activities, review the supplier submissions upon which these activities depend. The review SHALL verify completeness and consistency of these submissions with definitions in the ICSA specifications and with the product as presented for certification. The supplier SHALL make revisions to these submissions if found necessary in this review.

[ISDLA-312] contains the list of requirements on component development process that a certifier assesses for SDLPA-IC and SDA-IC. [ICSA-311] contains the security functions list that is assessed based upon component type(s), for FSA-IC. [SSA-420] defines requirements on a certifier for carrying out VIT-IC. Validation activities for compliance with these requirements include documentation review and independent test. The following requirement states the full set of criteria for ICSA certification, which relies upon these detailed specifications.

Requirement ISASecure_IC.R5 – Criteria for granting an initial certification

An initial ISASecure ICSA certification for one of Core tier or Advanced tier SHALL be granted for a component if the following requirements are met, as defined in Table 1 and the reference documents shown.

Table 1 - Requirements for initial ICSA certification

Topic	Element	Requirement	Reference Document
Secure Development Processes Implemented by Supplier	SDLPA-IC	The supplier holds an ISASecure SDLA certification at the time of issuance of the ICSA certificate. The component is within the stated scope of the certified process, for development going forward.	[SDLA-100] [SDLA-300] [ISDLA-312] or [SDLA-312]*
Secure Development Processes Applied to Component	SDA-IC	The component passes SDA-IC, which consists of (1) a review of 62443-4-1 compliant secure product development artifacts and (2) a review of five additional documented SDL processes and associated artifacts required under ICSA.	[ICSA-312] [ISDLA-312]
Security Functions of Component	FSA-IC	The certifier determines which 62443 component type(s) (software application, embedded device, host device, network device) apply to the product submitted for certification. The certifier further determines if the product is an IIoT device, an IIoT gateway, or both. These determinations are made in accordance with the definitions for these component types found in 3.1 of the present document. The subset of requirements in [ICSA-311] that meet either of the criteria below, are assessed as either *Met, Met by component, Met by integration into system, or Not Relevant,* per the criteria specified in the validation activity.** • 62443-4-2 requirements applicable to some 62443 component type of the product, where the requirement is also applicable to some IIoT component type of the product, as well as to the tier of the ICSA certification • Requirements in the “ICSA additions” section of [ICSA-311] that are applicable to some IIoT component type of the product, as well as to the tier of the ICSA certification.	[ICSA-311]

Topic	Element	Requirement	Reference Document
Vulnerability Identification	VIT-IC	The certifier carries out testing as defined for VIT-C. The component passes VIT-IC, based on applying the following criteria for issues identified during that testing: • Core tier: All "critical" and "high" issues identified are either corrected or the reason for them not being relevant has been documented. • Advanced tier: All "critical", "high", and "medium" issues identified are either corrected or the reason for them not being relevant has been documented. The above criteria for passing VIT-IC replace those for passing VIT-C found in requirement VIT-C.R5 in [SSA-420].	[SSA-420]

* The content of [ISDLA-312] and [SDLA-312] that applies for SDLA certification, is identical, after consideration of published errata. These documents differ in their content that applies for product certification, which defines SDA.

** As an example, for a device that is an embedded device and an IIoT device, certification to Core tier would include all 62443-4-2 requirements that apply to embedded devices and that also apply to Core tier IIoT devices. While this would include most 62443-4-2 requirements for embedded devices at capability security level 2 and some at level 3, this would not include for example the 62443-4-2 requirement CR 2.1 RE(2) *Permission mapping to roles*. This requirement applies to embedded devices for capability security levels greater than 1, but does not apply to Core tier IIoT devices. It would apply to Advanced tier IIoT devices (and Core or Advanced tier IIoT gateways).

Requirement ISASecure_IC.R6 – Validation by independent test

If a validation activity for a requirement in [ICSA-311] specifies that validation by independent test is required (identified by a “Yes” in the column titled “Validation by Independent Test Required (Yes/No) ICSA”) this means that the assessor SHALL BE fully responsible for the testing described. In particular this SHALL include responsibility for the appropriateness and quality of the test, and witnessing the execution of the test. The assessor MAY at their discretion use tools created by the supplier and assistance from supplier personnel in carrying out the test.

Bibliography

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

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

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