# ICSA-312

# ISA Security Compliance Institute – IIoT Component Security Assurance –

**Security development artifacts for IIoT components**

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

# 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 one document in the series that specifies the technical requirements for certification. The current list of documents related to ISASecure ICSA and other ISASecure certification programs can be found on the web site https://www.ISASecure.org.

# 1 Scope

In order for a component to pass an ISASecure® ICSA (IIoT Component Security Assurance) certification as defined in [ICSA-100] per the technical pass criteria in [ICSA-300], it must pass several evaluation elements. One of these elements is the Security Development Artifact assessment for IIoT components (SDA-IC). The purpose of this document is to state the criterion for passing the SDA-IC element of an ICSA certification evaluation. This element applies to all ICSA certifications.

In order to define the criteria for passing SDA-IC, this brief document refers to the separate document [ISDLA-312] that includes an enumeration of the detailed technical requirements for SDA-IC.

# 2 Normative references

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

[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

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

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

NOTE 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-62443-4-1] 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

### 3.1.1
**artifact**
tangible output from the application of a specified method that provides evidence of its application

NOTE Examples of artifacts for secure development methods are a threat model document, a security requirements document, meeting minutes, internal test results.

### 3.1.2
**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

**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.

**3.1.5**
**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.).

**3.1.6**
**industrial automation and control system**
collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process

**3.1.7**
**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]

**3.1.8**
**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 20924, 3.2.6 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 3.1.10).

**3.1.9**
**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 3.1.12).

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

**3.1.10**
**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).

### 3.1.11
### IIoT system
system providing functionalities of Industrial Internet of Things

NOTE An IIoT system can include, but not be limited to, IIoT devices, IIoT gateways, sensors, actuators, analytics and processing software together with its hardware/software environment, and related human interfaces.

[SOURCE ISO/IEC 20924, 3.2.9 (for IoT, incorporating additions to NOTE)]

### 3.1.12
### 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.

### 3.1.13
### proximity network
network that connects 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 main definition and NOTE 1 from text in [IICRA]]

### 3.1.14
### 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.

### 3.1.15
### 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.

### 3.1.16
### 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]

**3.1.17**
**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 IEC 62443-4-2 NOTE 2 added]

### 3.2 Abbreviations

The following abbreviations are used in this document

| | |
|---|---|
| ANSI | American National Standards Institute |
| DCS | distributed control system |
| CSA | component security assurance |
| HMI | human machine interface |
| IACS | industrial automation and control system |
| ICSA | IIoT component security assurance |
| IEC | International Electrotechnical Commission |
| IIC | Industrial Internet Consortium |
| IoT | Internet of Things |
| IIoT | Industrial Internet of Things |
| ISA | International Society of Automation |
| ISCI | ISA Security Compliance Institute |
| ISO | International Organization for Standardization |
| ISDLA | Software Development Lifecycle Assurance for ICSA |
| LAN | local area network |
| OS | operating system |
| PLC | programmable logic controller |
| SDA-IC | security development artifacts for IIoT components |
| SDLA | security development lifecycle assurance |
| SDLPA-IC | security development lifecycle process assessment for IIoT components |
| SIS | safety instrumented system |
| SMA | Security Maintenance Audit |
| TR | technical report |
| WAN | wide area network |

## 4 Background

The document [ICSA-100] provides general background on the ISASecure programs, the ISASecure ICSA component certification program, and their relationship to the ANSI/ISA/IEC 62443 standards. This clause discusses the rationale and structure of the ICSA program as it relates to SDA-IC.

The evaluation of secure development lifecycle processes based upon [IEC 62443-4-1] is a key characteristic of the ISASecure certification programs. This evaluation has two aspects. The first aspect is to determine whether a supplier *has defined and is maintaining* a documented secure product development lifecycle process. The second aspect is to determine whether the supplier is *following* the documented process.

In order to achieve a product certification under ISASecure ICSA for a component, both aspects are required. First, a Security Development Lifecycle Process Assessment for IIoT components (SDLPA-IC) is required to determine whether the supplier has defined and is maintaining a documented development process that meets ISASecure SDLA requirements, that apply to components. This assessment is done as part of the evaluation toward an ISASecure SDLA certification of the supplier's development process as described in [SDLA-100], which is a prerequisite for ICSA certification. Secondly, the ISASecure ICSA certifier will verify that the required artifacts that result from carrying out the documented secure product development lifecycle process exist for the specific component that has been presented as a candidate for certification. This aspect of an ICSA evaluation is called Security Development Artifacts for IIoT components, or SDA-IC. SDA-IC also incorporates five development sub-practices required for ICSA certification but not for SDLA certification at this time. These are found associated with validation activities for [IEC 62443-4-1] requirements SD-4, SUM-2, and SG-3 in [ISDLA-312]. Further, periodic audit of artifacts related to the maintenance of security of the product *after* certification has been achieved, is addressed by the Security Maintenance Audit (SMA) aspect of ICSA, described in [ICSA-301]. SDA-IC is the topic of the present document.

The requirements for a secure product development lifecycle process and the requirements on the artifacts that result from the implementation of that process are closely related. For this reason, the document [ISDLA-312] covers both the requirements assessed for an SDLPA-IC evaluation of a supplier's product development process, and the requirements assessed for the SDA-IC element of an ISASecure ICSA certification evaluation of a supplier's component. Whereas an ISASecure SDLA certification requires examining process documentation and *representative samples* of artifacts for secure product development practices that comprise that process, the SDA-IC requirements call for artifacts resulting from these same practices, as well as from the five additional practices unique to ICSA at this time (as noted in the previous paragraph), *for the specific component* that is a candidate for ISASecure ICSA certification.

An IIoT component is certified to a specific tier, either Core or Advanced. This tier will impact the SDA-IC evaluation as described in the following section.

## 5 Criterion for passing SDA-IC for ICSA certifications

**Requirement ISASecure_SDA-IC.R1 – Criterion for passing SDA-IC**

A component SHALL pass the Security Development Artifacts evaluation (SDA-IC) element of an evaluation for an ISASecure ICSA certification to the Core or Advanced tier, if requirements in [ISDLA-312] in rows that have the "**Component**" column marked with an 'X,' pass validation as follows.

Validation is performed per the column labeled "**Component or System Validation Activity**" in [ISDLA-312]. Validations that depend upon whether the certification is for Core or Advanced tier, SHALL be assessed as specified for the tier of the certification.

NOTE 1 Most SDA-IC requirements are validated in the same manner for both tiers. In ISDLA-312 version 6.3, the validation activities for the four requirements SDLA-SR-2J-ICSA, SDLA-SR-2K-ICSA, SDLA-SR-4-ICSA, and SDLA-DM-4-ICSA1 are dependent upon tier.

NOTE 2 Most SDA-IC validation activities in [ISDLA-312] involve examining artifacts that result from executing an aspect of the SDL process that meets requirements for SDLA certification. However, ICSA includes examining the component's artifacts for some additional SDL practices not required by SDLA certification (nor by [IEC 62443-4-1]), as well as verifying the existence of a documented processes that codify these practices. These differences are highlighted in [ISDLA-312] and enumerated in the document [ISASecure-119].

NOTE 3 For existing products which predate an organization's adoption of a well-defined secure development process, artifacts to satisfy SDA-IC may be created during the organization's transition to that process.

## 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