CSA-300

ISA Security Compliance Institute – Component Security Assurance –

ISASecure® certification requirements

Version 4.2

August 2019

A. DISCLAIMER
ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES
To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

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

Revision history

version	date	changes
2.0	2010.06.06	Initial version published to http://www.ISASecure.org
2.8	2014.12.10	Add VIT; add ISASecure SDLA and SDA-E references; add figure for elements of certification and revise figure illustrating levels; remove 5.3 about maintenance of certification (redundant with EDSA-301); ERT.R3 revised; terminology updates: essential services to essential functions; device vendor to device supplier
3.2	2018.01.31	Alignment with approved ANSI/ISA-62443-4-1: add terms and modify background section, treatment of levels for SDLPA and SDA-E certification criteria; apply erratum from EDSA-102 v3.1
3.6	2018.10.01	Alignment with approved ANSI/ISA-62443-4-2: revise Clause 1 references to allocating requirements in text and Figure 1, replace reference EDSA-311 by CSA-311 and add 62443 references in Clause 2, update requirement ED.R5 so that FSA-E conforms to CSA-311; in 4.2 remove statement that VIT depends upon FSA-E
4.2	2019.08.03	Change title from EDSA-300 to CSA-300; clarify definition of term certification level; cover all component types; remove CRT certification element; add applicant submission requirements formerly in EDSA-310

Contents

Certification requirements

FOREWORD

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

1 Scope

This document specifies the criteria for granting an initial ISASecure® CSA (Component Security Assurance) certification for an IACS (Industrial Automation and Control System) component. 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. To specify CSA certification criteria, this document references other specification documents that cover detailed requirements for the elements of certification:

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

While SDLPA-C is an evaluation of the product supplier's secure product development lifecycle process for components, SDA-C examines the artifacts that are the outputs of that process for the component to be certified. FSA-C examines the security capabilities of the component, while recognizing in accordance with [IEC 62443-4-2] that requirements for security functionality differ by component type. The certifier determines all component types applicable to a product; FSA-C then incorporates requirements for all component types applicable to the product. VIT-C scans the component for the presence of known vulnerabilities.

The following figure illustrates the elements of ISASecure CSA certification.

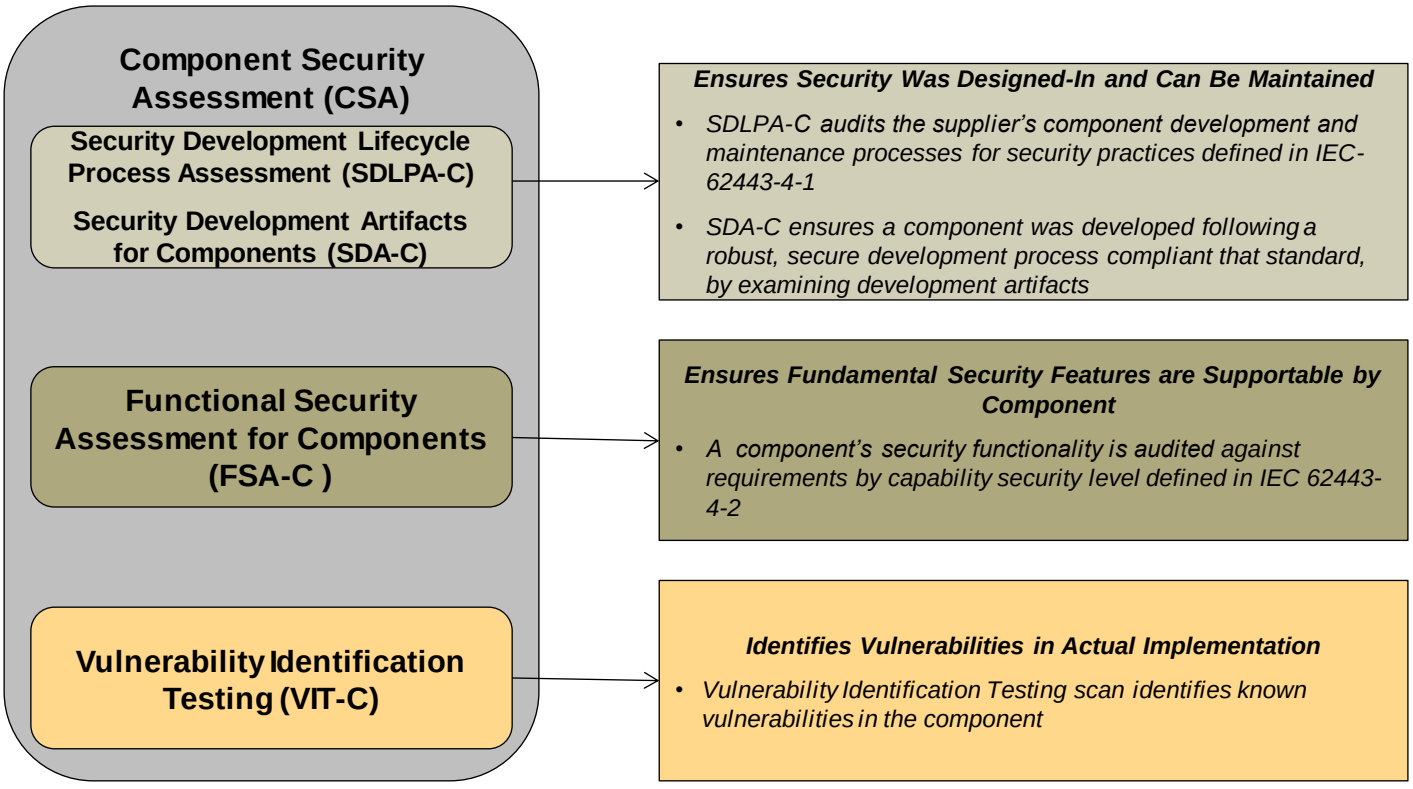

Figure 1 - Evaluation Elements for ISASecure CSA Certification

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 [CSA-301] *ISA Security Compliance Institute 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:

- An update of a certified product maintains the product certification if the supplier maintains a certified development process compliant with [IEC 62443-4-1], and the update is made following this process.

- 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.

It is a goal for the ISASecure programs to support and align with the developing standards ANSI/ISA/IEC 62443 for IACS security. [CSA-100] discusses the relationship between ISASecure CSA and the ANSI/ISA/IEC 62443 effort.

2 Normative references

2.1 Technical specifications

[CSA-100] *ISCI Component Security Assurance – ISASecure Certification Scheme*, as specified at http://www.ISASecure.org

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

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

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme*, as specified at http://www.ISASecure.org

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

NOTE 2 The following specification defines the FSA-C element of the ISASecure component certification, for all component types.

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

NOTE 2 The following specification defines the VIT-C element of the ISASecure component certification.

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

2.2 IACS security standards

NOTE 1 [CSA-100] describes the relationship of ISASecure CSA 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

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

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
certification level
capability security level for which conformance is demonstrated by a certification

NOTE It is intended that a component that achieves certification to CSA capability security level *n* will meet requirements for capability security level *n* as defined in [IEC 62443-4-2].

3.1.4
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

3.1.5
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.

3.1.6
essential function
function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.

3.1.7
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.).

3.1.8
independent test
form of requirements validation that requires the certifier's exercise of the entity under evaluation itself, 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.

3.1.9
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

3.1.10
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

3.1.11
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 CSA 1.0.0

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
security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

NOTE Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.14
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
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.16
upgrade
incremental hardware or software change in order to add new features

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-C	functional security assessment for components
HMI	human machine interface
IACS	industrial automation and control system
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
OS	operating system
PLC	programmable logic controller
SDA-C	security development artifacts for components
SDLA	security development lifecycle assurance
SDLPA-C	security development lifecycle process assessment for components
SIF	safety instrumented function
SIS	safety instrumented system
VIT-C	vulnerability identification test for 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 (IACS). ISASecure CSA 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 certifications for 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 levels

The CSA program defines four certification levels for a component, offering increasing levels of security assurance. Levels offered are capability security levels 1, 2, 3, and 4. The corresponding certifications are called ISASecure CSA Capability Security Level 1, ISASecure CSA Capability Security Level 2, ISASecure CSA Capability Security Level 3, and ISASecure CSA Capability Security Level 4. A product that achieves certification to CSA capability security level *n* is certified to meet requirements for capability security level *n* as defined in [IEC 62443-4-2], which includes a requirement for compliance to [IEC 62443-4-1]. A CSA certification earned by a particular product will indicate the applicable component type(s) and level, and thus

be expressed for example, as ISASecure CSA Capability Level 3 (Software Application) or ISASecure CSA Capability Security Level 2 (Embedded Device, Network Device).

All levels of certification include the certification elements defined in Clause 1. SDLPA-C does not have an associated level. SDA-C and VIT-C assessments are the same for all certification levels with the exception of allowable residual risk for known security issues. FSA-C incorporates more requirements at higher levels, aligned with the requirements assigned to each capability security level in [IEC 62443-4-2].

NOTE In SDLA-312 v5.5, certifier validation for requirement SDLA-DM-4 which applies for SDA-C, differs by capability security level. SDLA-DM-4 states that products certified to higher capability security levels require lower residual risk, in particular where this is affected by the severities of unmitigated vulnerabilities identified in the product.

5 Certification requirements

5.1 Certification level and version

Requirement ISASecure_C.R1 – Application for a certification level

When a supplier applies for certification of a component, the certification applicant SHALL specify the maximum capability security level for which they would like to achieve component certification. The levels possible are 1, 2, 3, or 4. The certifier SHALL award certification to a component at the highest level for which the component qualifies, up to this maximum level.

Requirement ISASecure_C.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 certification, which is offered as evidence toward this certification.

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

Requirement ISASecure_C.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 CSA certification applies, and the version of the certification achieved, such as ISASecure CSA 1.0.0.

NOTE It is not necessary to list all certified 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_C.R4 – ISASecure application requirements for an initial certification

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

a) List of essential functions of the component, in accordance with the definition in 3.1.6, 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-C and VIT-C)

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) 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.

f) other technical items as required by the specifications listed in Clause 2; and

g) administrative and potentially additional technical items defined by the certifier.

[SDLA-312] contains lists of requirements on component development process that a certifier assesses for SDLPA-C and SDA-C. [CSA-311] contains the security functions list that is assessed by component type, for FSA-C. [SSA-420] defines requirements on a certifier for carrying out VIT-C, and criteria for passing this element of the certification. Validation activities for compliance with these requirements include documentation review and independent test. The following requirement states the full set of criteria for CSA certification, which relies upon these detailed specifications.

Requirement ISASecure_C.R5 – Criteria for granting an initial certification

An initial ISASecure CSA certification for capability security level *n* SHALL be granted for a component if the following requirements are met, as defined in the reference documents shown.

Table 1 - Requirements for initial CSA certification

Topic	Element	Requirement	Reference Document
Secure Development Processes Implemented by Supplier	SDLPA-C	The supplier holds an ISASecure SDLA certification at the time of issuance of the CSA certificate. The component is within the stated scope of the certified process, for development going forward.	[SDLA-100] [SDLA-300] [SDLA-312]
Secure Development Processes Applied to Component	SDA-C	The component passes SDA-C, a review of secure product development artifacts, for capability security level *n*.	[CSA-312] [SDLA-312]
Security Functions of Component	FSA-C	The certifier determines which component type(s) (software application, embedded device, host device, network device) apply to the product submitted for certification, in accordance with the [IEC 62443-4-2] definitions for these component types found in 3.1 of the present document. All criteria in [CSA-311] applicable to any component type of the product, and applicable to capability security level *n,* are assessed as either *Met, Met by component, Met by integration into system, or Not Relevant,* per the criteria specified in the validation activity.	[CSA-311]
Vulnerability Identification	VIT-C	The system passes VIT-C, per the pass/fail criteria for capability security level *n*.	[SSA-420]

NOTE 1 A product developed for a particular capability security level, could achieve certification to any capability security level less than or equal to that intended capability security level. Thus, a supplier may specify and develop a product as capability security level 2, and apply for certification to ISASecure CSA Capability Security Level 1, for example, as an interim milestone.

NOTE 2 Since the component is within the scope of the SDL which achieved SDLA certification, that certified SDL process would have met any process certification criteria that apply for the capability security level that the supplier assigned to the component in the component security requirements. However, the SDLA certification itself does not have a certification level.

NOTE 3 It is acceptable to apply for both SDLA and CSA certifications at the same time. In effect, in this case, the supplier achieves, along with their component *product* certification, a *process* certification that applies toward certifications for other products going forward.