CSA-312

ISA Security Compliance Institute – Embedded Device Security Assurance –

Security development artifacts for components

Version 3.2

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
V1R3-03082010	2010.03.08	Initial version published to http://www.ISASecure.org
1.4	2010.06.08	Formatting changes
2.0	2015.04.22	Document title and scope changed from SDSA requirements matrix to artifact assessment requirements (SDA-E), with pointer to SDLA-312 for matrix
2.4	2018.01.31	Alignment with approved ISA-62443-4-1: revise treatment of levels as related to SDA-E certification criteria; add reference to EDSA-100 for relationship to ISA 62443
3.2	2019.08.03	Document title changed from EDSA-312 to CSA-312; clarify definition of term certification level; refer to the CSA program and CSA-311 to cover all component types in IEC 62443-4-2 (EDSA addressed embedded devices only)

Contents

FOREWORD

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

1 Scope

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

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

2 Normative references

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

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

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

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

NOTE The following references that have the same document number 62443-4-2, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

[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
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.4
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].

3.1.5
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

3.1.6
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.

3.1.7
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
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

3.1.9
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.

3.1.10
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.

3.1.11
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.

3.2 Abbreviations

The following abbreviations are used in this document

DCS	distributed control system
CSA	component security assurance
IACS	industrial automation and control system
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
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
SIS	safety instrumented system
SSA	system security assurance

4 Background

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

The evaluation of secure development lifecycle processes 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 CSA for a component, both aspects are required. First, a Security Development Lifecycle Process Assessment for components (SDLPA-C) 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. Secondly, the ISASecure CSA 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 a CSA evaluation is called Security Development Artifacts for components, or SDA-C. SDA-C 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 [SDLA-312] covers both the requirements assessed for an SDLPA-C evaluation of a supplier’s product development process, and the requirements assessed for the SDA-C element of an ISASecure CSA 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 methods that comprise that process, the SDA-C requirements call for artifacts resulting from these same methods, *for the specific component* that is a candidate for ISASecure CSA certification.

A component is certified to a specific capability security level. This level will impact the SDA-C evaluation as described in the following section.

5 Criterion for passing SDA-C for CSA certifications

Requirement ISASecure_SDA-C.R1 – Criterion for passing SDA-C

A component SHALL pass the Security Development Artifacts evaluation (SDA-C) element of an evaluation for an ISASecure CSA Capability Security Level *n* certification, if requirements in [SDLA-312] in rows that have the "**Component**" column marked with an 'X,' pass validation.

Validation is performed per the column labeled "**Component or System Validation Activity**" in [SDLA-312]. Validations that depend upon capability security level SHALL be assessed for capability security level *n*.

NOTE 1 Most SDA-C requirements are validated in the same manner for all capability security levels. In SDLA-312 version 5.5, this is true for all requirements except SDLA-DM-4.

NOTE 2 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 3 For existing products which predate an organization's adoption of a well-defined secure development process, artifacts to satisfy SDA-C may be created during the organization's transition to that process.