# ISASecure-117

# ISA Security Compliance Institute — ISASecure® certification programs

**Policy for transition to CSA 1.0.0 and SSA 4.0.0**

Version 1.2

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 |
|---|---|---|
| 1.2 | 2019.08.02 | Initial version published to http://www.ISASecure.org |
| | | |
| | | |

# Contents

## FOREWORD

This is one of a series of documents that defines ISASecure® certification programs. This document describes the policy for transition of certification operations to the revised certification versions ISASecure CSA 1.0.0 (Component Security Assurance) and SSA 4.0.0 (System Security Assurance). The CSA program is a revision and extension of the prior ISASecure EDSA (Embedded Device Security Assurance) program. The list of ISASecure certification programs and documents for these new program versions, and for the prior program versions EDSA 3.0.0 and SSA 3.0.0, can be found on the web site http://www.ISASecure.org.

## 1 Background and scope

ISCI (ISA Security Compliance Institute) has operated a product certification program for embedded devices, called ISASecure® EDSA (Embedded Device Security Assurance) and a certification program for control systems, called ISASecure SSA (System Security Assurance). The prior versions of these programs were denoted EDSA 3.0.0 and SSA 3.0.0.

ISASecure CSA (Component Security Assurance) replaces the ISASecure EDSA program. The scope of CSA includes embedded devices, as well as software applications, host devices and network devices, as defined in the standard [IEC 62443-4-2] and 3.1 of this document.

The CSA certification criteria for embedded devices also have been revised from EDSA. CSA requires deeper and broader technical audit of supplier robustness testing practices, and removes the requirement for certifier-performed testing previously known as EDSA CRT (communication robustness testing). This change in assessment approach is also implemented in SSA 4.0.0, for system assessment.

This document specifies the timeline and related policies for transition of certification operations for embedded devices to CSA 1.0.0, and for systems to SSA 4.0.0.

Modifications previously incorporated in EDSA 2.1.0 and SSA 2.1.0 to the process for maintaining ISASecure product certificates over time continue to apply for CSA 1.0.0 and SSA 4.0.0. These changes were previously documented in prior transition documents [ISASecure-115] and [ISASecure-116] which stated that those documents superseded all other specifications regarding the maintenance of certification process. For CSA 1.0.0 and SSA 4.0.0, these maintenance of certification modifications are now fully integrated across the ISASecure specifications. They are therefore no longer carried forward as part of the present transition document.

## 2 Normative references

The policies for prior transitions for ISASecure certification versions are described in:

[ISASecure-115] *ISCI ISASecure Certification Programs - Policy for transition to SDLA 2.0.0, EDSA 2.1.0 and SSA 2.1.0* as specified at http://www.ISASecure.org

[ISASecure-116] *ISCI ISASecure Certification Programs - Policy for transition to EDSA 3.0.0 and SSA 3.0.0* as specified at http://www.ISASecure.org

Standards with which ISASecure programs align are as follows. The table in Section 5 shows the correspondence between these standards and ISASecure certification programs and versions.

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-62443-3-3] ANSI/ISA−62443−3−3 (99.03.03) - 2013 *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

[IEC 62443-3-3] IEC 62443−3−3:2013 *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

[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*

An ISASecure certification program version program is defined by a set of associated specification documents and document versions. The documents associated with the programs named in Clause 1 are published at http://www.ISASecure.org.

The present document refers specifically to:

[CSA-301] *ISCI Component Assurance – Maintenance of ISASecure certification,* as specified at http://www.ISASecure.org

## 3 Definitions and abbreviations

### 3.1 Definitions

**3.1.1**
**accreditation**
for ISASecure certification programs, assessment and recognition process via which an organization is granted chartered laboratory status

**3.1.2**
**accreditation body**
third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out a specific conformity assessment

**3.1.3**
**certification**
third party attestation related to products, processes, or persons that conveys assurance that specified requirements have been demonstrated

NOTE Here, this refers to either a successful authorized evaluation of a product or a process to ISASecure criteria. This outcome permits the product supplier or organization performing the process to advertise this achievement in accordance with certification program guidelines.

**3.1.4**
**certification body**
an organization that performs certification

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

NOTE A chartered laboratory is the conformity assessment body for the ISASecure certification programs. ASCI is the legal entity representing ISCI.

**3.1.7**
**conformity assessment body**
body that performs conformity assessment services and that can be the object of accreditation

NOTE Examples are a laboratory, inspection body, product certification body, management system certification body and personnel certification body. This is an ISO/IEC term and concept.

**3.1.8**
**control system**
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

**3.1.9**
**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.

**3.1.10**
**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.).

**3.1.11**
**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

**3.1.12**
**initial certification**
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of a product under evaluation or of any of its prior versions

**3.1.13**
**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.

**3.1.14**
**release**
any software/hardware delivered by the supplier to the customer

**3.1.15**
**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.

**3.1.16**
**update**
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

**3.1.17**
**upgrade**
incremental hardware or software change in order to add new features

**3.1.18**
**version (of ISASecure certification)**
ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a three-place number, such as ISASecure CSA 1.0.0

**3.1.19**
**version (of product)**
identifier for a release, usually numerical

NOTE For a system, may incorporate many individual component versions.

### 3.2 Abbreviations

The following abbreviations are used in this document.

| | |
|---|---|
| ANSI | American National Standards Institute |
| ASCI | Automation Standards Compliance Institute |
| CRT | communication robustness testing |
| CSA | component security assurance |
| DCS | distributed control system |
| EDSA | embedded device security assurance |
| ERT | embedded device robustness testing |
| FSA | functional security assessment |
| DCS | distributed control system |
| HMI | human-machine interface |
| IACS | industrial automation and control system(s) |
| IEC | International Electrotechnical Commission |
| ISA | International Society of Automation |
| ISCI | ISA Security Compliance Institute |
| ISO | International Organization for Standardization |
| NA | not applicable |
| OS | operating system |
| PLC | programmable logic controller |
| SDA | security development artifacts |
| SDL | security development lifecycle |
| SDLPA | security development lifecycle process assessment |
| SDLA | security development lifecycle assurance |
| SIS | safety instrumented system |
| SRT | system robustness testing |
| SSA | system security assurance |

## 4 Transition policy

The following policies apply to ISASecure chartered laboratories, which are the certification bodies for the ISASecure certification programs.

- **CSA 1.0.0 Mandatory Policy** An embedded device submitted for ISASecure certification where the SDL activity for that product release started after March 31, 2020, SHALL be evaluated using the CSA 1.0.0 (or later) specifications. This applies to both initial certifications and upgrades of embedded devices (as defined in 3.1.17) that have an EDSA certification prior to the upgrade.

- **CSA 1.0.0 Optional Policy** An embedded device submitted for ISASecure certification where the SDL activity for that product release started before March 31, 2020, and where the product is submitted for certification before March 31, 2023, MAY be evaluated using the CSA 1.0.0 specifications or an EDSA certification version permitted by the transition documents [ISASecure-115] and [ISASecure-116].

- **Maintenance of EDSA Certifications** For embedded devices that earned an EDSA 2.1.0 or 3.0.0 certification, updates of the embedded device (as defined in 3.1.16), may continue to maintain that EDSA certification in accordance with the maintenance of certification policy described in [ISASecure-115] and [ISASecure-116].

- **Conversion of EDSA to CSA Certification** A supplier MAY at their option submit a specific version of an embedded device that holds an EDSA certification, to obtain CSA 1.0.0 certification. The associated evaluation would fall under the procedures described in [CSA-301] for updating to a new ISASecure version. This involves evaluation of the new and changed requirements in CSA 1.0.0 relative to the EDSA certification version already held by the embedded device.

- **SSA 4.0.0 Mandatory Policy** An SSA certification granted for a system where the SDL activity for that product release started after March 31, 2020, SHALL use the SSA 4.0.0 (or later) specifications. This applies to both initial certifications and upgrades of systems (as defined in 3.1.17) that have a prior SSA certification.

- **SSA 4.0.0 Optional Policy** An SSA certification granted for a system where the SDL activity for that product release started during or before March 31, 2020 and where the product is submitted for certification before March 31, 2023, MAY use the SSA 4.0.0 specifications or a prior SSA certification version permitted by the transition documents [ISASecure-115] and [ISASecure-116].

In addition to certification of embedded devices, CSA 1.0.0 also supports certification of software applications, host devices and network devices. The ISASecure program did not previously certify such components, so no related transition policy applies for them.

## 5 Alignment with ANSI/ISA/IEC 62443 Standards

The policy in Section 4 provides stakeholders several options for which certification versions to specify, achieve, and grant. To assist in this decision, the following table describes the alignment of certification versions with related ANSI/ISA/IEC 62443 standards.

ISASecure certifications in most cases preceded publication of related 62443 standards, and were aligned with those standards shortly after the standards were published.

**Table 1. 62443 Alignment of EDSA, CSA, SSA**

| | EDSA 2.0.0 | EDSA 2.1.0 | EDSA 3.0.0 | CSA 1.0.0 | SSA 2.0.0 | SSA 2.1.0 | SSA 3.0.0 | SSA 4.0.0 |
|---|---|---|---|---|---|---|---|---|
| Aligned with 62443-3-3 | NA | NA | NA | NA | Y | Y | Y | Y |
| Aligned with 62443-4-1 | N | Y | Y | Y | N | Y | Y | Y |
| Aligned with 62443-4-2 | N | N | Y | Y | NA | NA | NA | NA |
| Entities certifiable | Embedded devices | Embedded devices | Embedded devices | Embedded devices, software applications, host devices, network devices | Systems | Systems | Systems | Systems |