ICSA-204
ISA Security Compliance Institute – IIoT Component Security Assurance –
Instructions and Policies for Use of the ISASecure® Symbol and Certificate

Version 2.0

April 2023

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
1.4	2022.12.09	Initial version published to https://www.ISASecure.org
2.0	2023.04.21	Do not permit logo placement on physical component

Contents

Table of Figures

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 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). A description of the ISASecure ICSA program and 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

This document outlines the procedure and conditions which govern the use of the ISASecure® symbol and certificate by ISASecure ICSA (IIoT Component Security Assurance) chartered laboratories and component vendors, and any references to their ASCI license by such laboratories. The reference [ICSA-100] provides an overall description of the ISASecure ICSA program. The program certifies IIoT (Industrial Internet of Things) devices and IIoT gateways, as defined in [ICSA-300]. One or both of these definitions may apply to a component.

2 Normative references

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

[ICSA-205] *ISCI IIoT Component Security Assurance – Certificate Document Format,* 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

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 62443-4-1:2019 *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*

[ISO/IEC 17065] ISO/IEC 17065, "*Conformity assessment - Requirements for bodies certifying products, processes, and services*", September 15, 2012

[ISO/IEC 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories*", November 2017

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", November 2017

[ISO/IEC 17000] ISO/IEC 17000 "*Conformity assessment — Vocabulary and general principles*"

[ISO/IEC 28] ISO/IEC Guide 28, "*Conforming assessment – Guidance on a third-party certification system for products,*" 2004

[ISO/IEC 23] ISO/IEC Guide 23 "*Methods of indicating conformity with standards for third-party certification systems,"* 1982

3 Definitions and abbreviations

3.1 Definitions

As a general rule, definitions of ISO/IEC 17000 are applicable.

3.1.1
accreditation body
third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment

3.1.2
accreditation body logo
logo used by an accreditation body to identify itself.

3.1.3
accreditation certificate
formal document or a set of documents issued by an accreditation body, stating that accreditation has been granted for the defined scope.

3.1.4
accreditation symbol
symbol issued by an accreditation body to be used by chartered laboratories to indicate their accredited status.

3.1.5
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.

3.1.6
certifier
chartered laboratory

NOTE This term is used when a shorter designation for this organization is more appropriate to the context.

3.1.7
chartered laboratory
organization chartered by ASCI to evaluate products and/or 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 ICSA program.

3.1.8
ISASecure symbol
graphic affixed or displayed to designate that ISASecure certification has been achieved

NOTE The ISASecure symbol is the mark of conformity for the ASCI certification scheme. The symbol or mark is licensed by ASCI for use by suppliers that have achieved certified products and by ISASecure laboratories to signify their participation in the ISASecure program.

3.1.9
ISASecure version
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 3-place number such as ISASecure ICSA 1.0.0

3.1.10
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.

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CSA	component security assurance
ICSA	IIoT component security assurance
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
ILAC	International Laboratory Accreditation Cooperation
ISCI	ISA Security Compliance Institute
ISA	International Society of Automation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
SMA	Security Maintenance Audit

4 ISASecure symbol and references

4.1 General

The ISASecure symbol is defined as the sequence of letters “ISASecure,” where the first four letters only are capitalized. The ISASecure symbol shall be displayed only in the appropriate form, size, and color detailed on the ISASecure website: https://www.ISASecure.org.

When displayed in isolation such as on letterhead, the ISASecure symbol shall always be accompanied by the trademark notation, as in ISASecure®. When used within a document that has several occurrences of the symbol, such as a brochure or press release, the first occurrence shall have the trademark notation. In addition, in this case, the document shall also include the statement:

ISASecure® is a registered Trademark of ASCI. All rights reserved.

An ISASecure chartered laboratory and/or its clients shall neither use the ISASecure symbol in any misleading manner, nor shall imply in use of the symbol or in any reference that ASCI or ISCI approves of its products.

In particular, a chartered laboratory and/or its clients shall not use the ISASecure symbol in any way that might mislead the reader regarding the status of the laboratory or the certification of a component or a specific version of a component.

All references that contain the ISASecure symbol shall clearly define the particular ISASecure certification program to which they are related, which in the present case would be the ISASecure ICSA certification program.

4.2 Use by ISASecure chartered laboratory

When a chartered laboratory displays the ISASecure symbol in printed or online documentation, its license number (chartered laboratory identification, in five-digit format) issued by ASCI shall be printed centrally under the ISASecure symbol. Its accreditation number may also appear.

In particular, the ISASecure symbol may be displayed on organizational stationery/letterhead by a chartered laboratory only if the mark or title of the laboratory is also shown, along with its license number.

The following is an example of correct use of the ISASecure symbol by a chartered laboratory:

ISASecure® ICSA

Accreditation Number: WWWWW

License Number: XXXXX

A chartered laboratory is entitled to use the phrase, "An ISASecure Chartered Laboratory – Accreditation number WWWWW, License Number XXXXX" in combination with the ISASecure symbol.

To request approval to use one of the above phrases, a laboratory shall:

a) Submit a request to use the wording to the ASCI Managing Director; and

b) Submit a pictorial representation of how the wording is to appear

c) Submit a pictorial representation of how the wording is to appear in conjunction with the accreditation body's mark/symbol, the ISASecure symbol or any other mark or symbol of conformity.

The ASCI Managing Director shall respond within 30 days as to whether the use of the wording as proposed by the laboratory is acceptable.

The chartered laboratory shall bear responsibility for obtaining any required copyrights and for monitoring the use of the wording and ensuring that the wording is not misused.

ISASecure laboratories are entitled to incorporate the ISASecure symbol in public material that refers to accredited services, provided that the conditions in this procedure are met. ISASecure laboratories are also entitled to make general reference to the ASCI license provided they ensure that ASCI recognition is not implied for aspects of any program for which the laboratory is not recognized.

Any use of the ISASecure symbol by a laboratory that might contravene the conditions set out in this procedure will be considered a misuse of the symbol and subject to legal action which may include withdrawal of the ASCI license, or publication of the transgression or other action deemed necessary by ASCI to maintain the integrity of its mark.

4.3 Use by component vendor

When a vendor for a certified component displays the ISASecure symbol in printed or online documentation, the certification number issued by the certification body (chartered laboratory) shall be printed centrally under the ISASecure symbol, The ISASecure version and certification tier (Core or Advanced) shall also appear.

The following is an example of correct use of the ISASecure symbol by a component vendor:

ISASecure® ICSA 1.0.0 Core Tier

Certification number: YYYYY

The vendor shall not place the ISASecure symbol on a certified component or its packaging. This policy recognizes that most products incorporate software which potentially may be replaced by later versions that may or may not be certified. The policy does not prohibit marking such a product with the logo of a certification body, nor does it preclude modification of this policy in the future to align with evolving industry marking practices and/or regulatory requirements.

The attainment of ISASecure ICSA certification does not imply attainment of the ISASecure CSA certification, nor vice versa. A vendor may use these designations only if they have received a certificate under those individual programs, respectively.

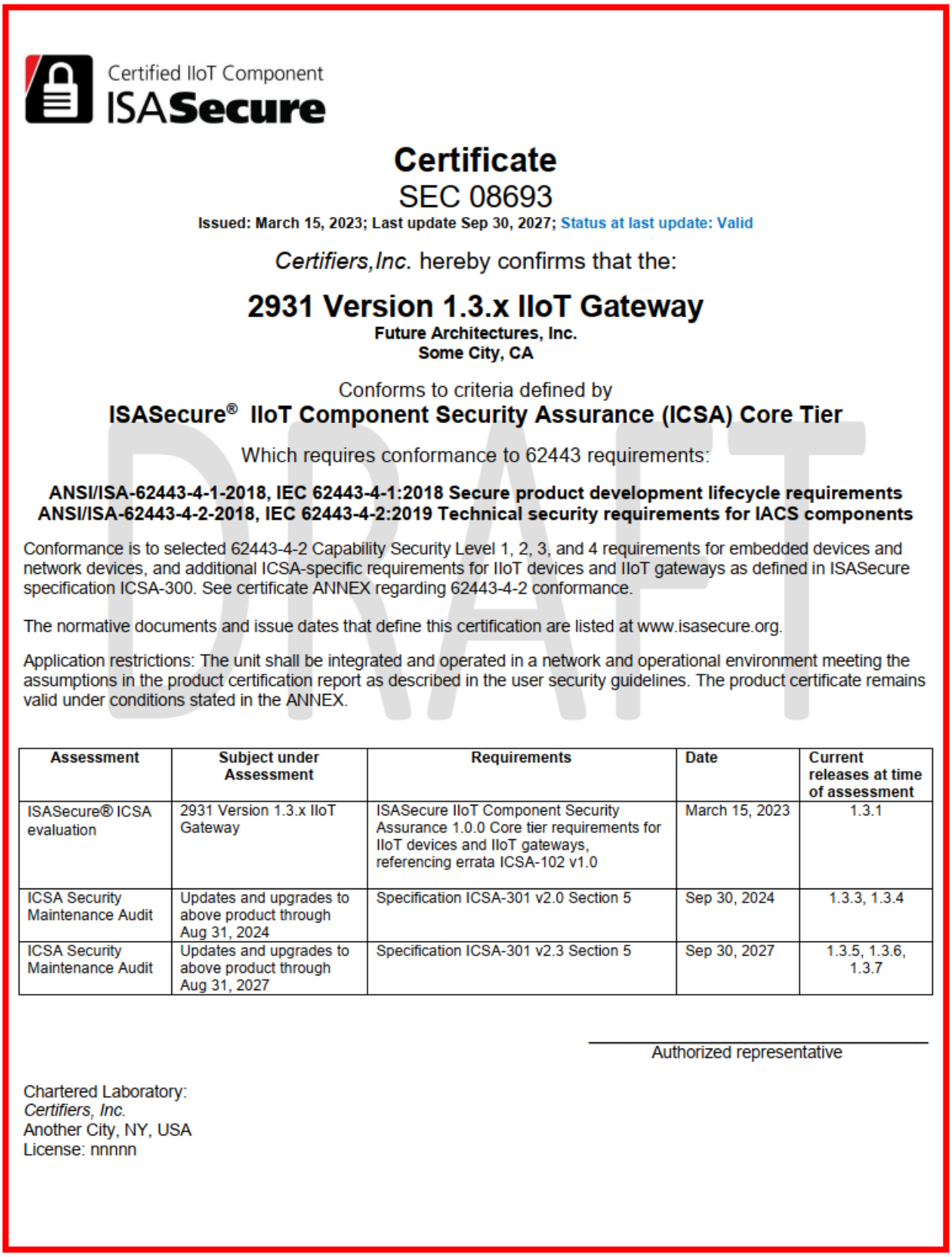
As specified in [ISO/IEC 17065], the consequences of transgressions by clients of a chartered laboratory are managed by the chartered laboratory.

5 Certificates

The certification certificate issued by a chartered laboratory to its clients must be the one recognized by the ASCI program. The document [ICSA-205] posted on the ISASecure website contains the approved certificate format in an editable form suitable for use as a template. Figure 1 and Figure 2 (certificate annex) illustrate this format. If alterations are made to the approved certificate, prior to its use, the ASCI Managing Director must approve the certification certificate used by the chartered laboratory.

The certificate includes a status annotation which may be one of Valid, Suspended, Terminated or Withdrawn.

NOTE 1 Additional explanation regarding the content shown on this certificate can be found in [ICSA-301].



Certified IIoT Component
ISASecure

Certificate

SEC 08693

Issued: March 15, 2023; Last update Sep 30, 2027; Status at last update: Valid

Certifiers, Inc. hereby confirms that the:

2931 Version 1.3.x IIoT Gateway

Future Architectures, Inc.
Some City, CA

Conforms to criteria defined by

ISASecure® IIoT Component Security Assurance (ICSA) Core Tier

Which requires conformance to 62443 requirements:

ANSI/ISA-62443-4-1-2018, IEC 62443-4-1:2018 Secure product development lifecycle requirements
ANSI/ISA-62443-4-2-2018, IEC 62443-4-2:2019 Technical security requirements for IACS components

Conformance is to selected 62443-4-2 Capability Security Level 1, 2, 3, and 4 requirements for embedded devices and network devices, and additional ICSA-specific requirements for IIoT devices and IIoT gateways as defined in ISASecure specification ICSA-300. See certificate ANNEX regarding 62443-4-2 conformance.

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

Application restrictions: The unit shall be integrated and operated in a network and operational environment meeting the assumptions in the product certification report as described in the user security guidelines. The product certificate remains valid under conditions stated in the ANNEX.

Assessment	Subject under Assessment	Requirements	Date	Current releases at time of assessment
ISASecure® ICSA evaluation	2931 Version 1.3.x IIoT Gateway	ISASecure IIoT Component Security Assurance 1.0.0 Core tier requirements for IIoT devices and IIoT gateways, referencing errata ICSA-102 v1.0	March 15, 2023	1.3.1
ICSA Security Maintenance Audit	Updates and upgrades to above product through Aug 31, 2024	Specification ICSA-301 v2.0 Section 5	Sep 30, 2024	1.3.3, 1.3.4
ICSA Security Maintenance Audit	Updates and upgrades to above product through Aug 31, 2027	Specification ICSA-301 v2.3 Section 5	Sep 30, 2027	1.3.5, 1.3.6, 1.3.7

Authorized representative

Chartered Laboratory:
Certifiers, Inc.
Another City, NY, USA
License: nnnnn

Figure 1 - Example certificate

CERTIFICATE SEC 08693

Issued: March 15, 2023; Last update Sep 30, 2027

ANNEX

CERTIFICATE VALIDITY

Product certificate remains valid under conditions:

- The following SDLA certificate remains valid: ISASecure® Security Development Lifecycle Assurance certificate number SEC 08691 issued to *Future Architectures, Inc.*
- 2931 Version 1.3.x IIoT gateway remains under the security management practices thereby certified
- Product meets program criteria under ongoing security maintenance audit (SMA) as recorded on the certificate.

COMPLIANCE TO 62443-4-2

Certification to ICSA Core tier for a component that is both an IIoT device and an IIoT gateway includes verification that a component:

- Conforms to all 62443-4-2 requirements applicable to the 62443-4-2 component type(s) embedded device and network device, for capability security level 2 (SL-C=2), with the one exception of requirement CR 7.3 RE (1); and
- Conforms to 62443-4-2 requirements applicable to its 62443-4-2 component type(s) as follows, where the subset of the total 62443-4-2 requirements for each capability security level is indicated: SL-C=1: 44/44; SL-C=2: 78/79; SL-C=3: 87/100; SL-C=4: 88/106. See document ISASecure -119 for this 62443-4-2 requirement list.

Figure 2 - Example certificate annex

NOTE 2 In this example, release 1.3.2 was out of support by Sep 30, 2024, so that it does not appear on this certificate. It held the status of a certified version during the time period while it was under support. This is in accordance with the use of "1.3.x" in the title of this certificate, and based upon the conditions that (1) the supplier was maintaining their SDLA certification during that time period, and (2) version 1.3.2 was an update release.

If as described in 4.3.1 of [ICSA-301], the certifier chooses to revise the certificate to show intermediate updates of the component that occur between Security Maintenance Audits (SMA's), these are added to the table on the certificate as in the third row of the following example table. Such intermediate updates are optional.

Assessment	Subject under Assessment	Requirements	Date	Current releases at time of assessment
ISASecure® ICSA evaluation	2931 Version 1.3.x IIoT Gateway	ISASecure IIoT Component Security Assurance 1.0.0 Core tier requirements for IIoT gateways, referencing errata ICSA-102 v1.0	March 15, 2023	1.3.1
ICSA Security Maintenance Audit	Updates and upgrades to above product through Aug 31, 2024	Specification ICSA-301 v2.0 Section 5	Sep 30, 2024	1.3.3, 1.3.4
Certification valid for component update	2931 Version 1.3.4 IIoT Gateway	Specification ICSA-301 Requirement ISASecure_ICM.R1	May 12, 2025	1.3.4, 1.3.5
ICSA Security Maintenance Audit	Updates and upgrades to above product through Aug 31, 2027	Specification ICSA-301 v2.3 Section 5	Sep 30, 2027	1.3.5, 1.3.6, 1.3.7

6 Change in accreditation status

Upon withdrawal or suspension of its accreditation, a chartered laboratory shall immediately cease to display or issue certificates and any other materials displaying the ISASecure symbol, license or containing reference to ASCI recognition.

7 Modification of the ISASecure symbol

Upon any modifications to the ISASecure symbol, ASCI must immediately inform ISASecure laboratories of its changes and proper use. The effective date for the use of the new symbol must be published on the website: https://www.ISASecure.org.

8 Use of accreditation certificates and symbol

A chartered laboratory use of the accreditation certificates issued by the accreditation body and the associated symbols must follow the policies and procedures of the accreditation body.

Bibliography

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

— — — — — —