ICSA-301
ISA Security Compliance Institute –
IIoT Component Security Assurance –
Maintenance of ISASecure® certification

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

Requirements

FOREWORD

This is one of a series of documents that defines ISASecure® ICSA (IIoT Component Security Assurance) certification 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 current list of documents related to ISASecure ICSA can be found on the ISCI web site https://www.isasecure.org/.

1 Scope

This document specifies the criteria for maintaining ISASecure® ICSA (IIoT Component Security Assurance) certification for an IIoT (Industrial Internet of Things) device or an IIoT gateway, as the threat environment, the component, and the ISASecure ICSA criteria evolve over time. IIoT devices and gateways are subtypes of one of the product types: embedded devices, host devices, and network devices, defined in the standard IEC 62443-4-2. [ICSA-100] provides an overview of the ICSA certification scheme and all related specifications. The present document covers certification situations where:

- time has passed since ICSA certification of a component, whether or not the component has been modified after its certification (where requirements ISASecure_SMA.R1 and R2 of clause 5 define the time period); or
- a certified component has subsequently been modified; or
- the ISASecure ICSA certification criteria have changed; or
- both the component and the certification criteria have changed.

A certification is called an *initial* certification if it *does not* take into account the results of a prior certification for the component or for a prior version of the component. The criteria for a component to earn an initial certification are defined in [ICSA-300].

In overview, in order to obtain an initial ISASecure ICSA certification, a supplier must hold an ISASecure SDLA (Security Development Lifecycle Assurance) development process certification such that the component to be evaluated is in the scope of that process. This criterion is called SDLPA-IC (Security Development Lifecycle Process Assessment for IIoT components). A supplier may at their option apply for ICSA and SDLA certifications in parallel.

ISASecure ICSA certification of components has three additional elements:

- Security Development Artifacts for IIoT components (SDA-IC);
- Functional Security Assessment for IIoT components (FSA-IC); and
- Vulnerability Identification Testing for IIoT components (VIT-IC).

Both SDLPA-IC and SDA-IC assess development process. SDLA certification demonstrates that the supplier has a documented secure product development lifecycle process, that is compliant with [IEC 62443-4-1], and that there is evidence the process is followed. SDA-IC examines the artifacts that are the outputs of the supplier's development processes as they apply specifically to the component to be ICSA certified. FSA-IC examines the security capabilities of the component. In accordance with [IEC 62443-4-2], requirements for security functionality differ based upon 62443 component type, that is, whether the component is an embedded device, host device, network device, and/or software application. The certifier determines all 62443 component types applicable to a product, and whether it is an IIoT device and/or an IIoT gateway. FSA-IC then incorporates requirements for all component types applicable to the product.

VIT-IC scans the component for the presence of known vulnerabilities.

An ICSA certification has an associated certification tier, which may be Core tier or Advanced tier. The required underlying SDLA certification does not have an associated tier. SDA-IC and VIT-IC are the same for both tiers with the exception of allowable residual risk for known security issues. FSA-IC incorporates more requirements for Advanced tier than for Core tier.

This document specifies:

- **Security Maintenance Audit:** A periodic surveillance audit required for maintaining an ICSA certification for a component over time, which is applicable whether or not the component has undergone modification; and

- **Maintenance of certification when component or certification criteria are modified:** when and how the results of a previous certification may be used for certification of a modified component, for certification to a later version of the ISASecure ICSA criteria, or for certification to a higher tier. It specifies the incremental evaluations that are performed when evidence from a prior certification evaluation does not fully apply to the new certification being sought. To specify this, the document discusses this topic in turn for each of the elements of ISASecure ICSA certification listed above**;** and

- **ICSA certification for CSA-certified product:** How an ICSA certification may be obtained for a component for which the current or a previous version has been certified under the ISASecure CSA program.

NOTE Security Maintenance Audit has been introduced for ICSA, and at this time is not required to maintain a CSA certification.

2 Normative references

2.1.1 ISASecure Specifications

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

[ICSA-200] *ISA Security Compliance Institute IIoT Component Security Assurance – ISASecure ICSA chartered laboratory operations and accreditation,* as specified at https://www.ISASecure.org

[ICSA-204] *ISA Security Compliance Institute IIoT Component Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at https://www.ISASecure.org

[ICSA-300] *ISA Security Compliance Institute IIoT Component Security Assurance – ISASecure certification requirements,* as specified at https://www.ISASecure.org

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

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

[SSA-420] *ISA Security Compliance Institute System Security Assurance – Vulnerability Identification Test Specification*, as specified at https://www.ISASecure.org

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

[SDLA-300] *ISA Security Compliance Institute Security Development Lifecycle Assurance – Requirements for ISASecure Certification and Maintenance of Certification,* as specified at https://www.ISASecure.org

NOTE The following two documents contain identical information that is used for SDLA certification. They differ in that [SDLA-312] is the reference for the SDA (Security Development Artifacts) element of CSA called SDA-C, and [ISDLA-312] is the reference for the SDA element of ICSA, called SDA-IC.

[ISDLA-312] *ISA Security Compliance Institute Security Development Lifecycle Assurance – Security development lifecycle assessment for IIoT components*, as specified at https://www.ISASecure.org

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

2.1.2 IACS security standards

NOTE 1 [ICSA-100] describes the relationship of ISASecure ICSA to the ANSI/ISA/IEC 62443 series of 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
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
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

[SOURCE text in IEC 62443-3-3 A.2.2]

3.1.3
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.

3.1.4
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 certification programs.

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

[SOURCE IEC 62443-4-2]

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.

[SOURCE IEC 62443-4-2]

3.1.7
evidence impact assessment
identification of that portion of the evidence from the certification evaluation of a product, which may be applied toward the certification of a modified version of the product, and of those aspects of the evaluation which must be performed on the modified product and new evidence created

3.1.8
fix (for a product security issue)
modification of a product and/or its documented security guidance to address a security issue, such that the resulting product version would meet certification criteria specified for initial product certification

NOTE 1 This definition is based upon the usage of the term in IEC 62443-4-1 requirement DM-4, part a).

NOTE 2 Changes that eliminate a security issue may or may not fall under this definition of “fix.” For example, recommending use of the user’s choice of an external firewall to protect against exploitation of a critical vulnerability is not a “fix.” Since the firewall is not part of the product, the product still has a critical vulnerability and so does not meet initial certification criteria. On the other hand, incorporating a specific firewall into the product and satisfying IEC 62443-4-1 requirements for that firewall as a third party component. would count as a fix. As a second example, suppose that a flawed security capability was removed from the product and replaced by instructions for integration with an external system to achieve the security capability. This would be considered a fix if IEC 62443-4-2 explicitly permitted the capability to be achieved by integration into a system, but would not be a fix if 62443-4-2 did not permit this.

3.1.9
good standing (under Security Maintenance Audit)
status of a supplier with respect to a specific component for which they hold an ICSA certification, which designates that Security Maintenance Audit (SMA) has been conducted for the product at times specified under the ICSA program, and there are currently no open nonconformities for the component that were found under SMA

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.).

[SOURCE IEC 62443-4-2]

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

[SOURCE IEC 62443-4-2]

3.1.12
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]

3.1.13
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 FDIS 20924, 3.2.4 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 3.1.15).

3.1.14
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 3.1.18).

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

3.1.15
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).

3.1.16
IIoT system
system providing functionalities of Industrial Internet of Things

NOTE IIoT system is inclusive of IIoT devices, IIoT gateways, sensors, actuators, analytics and processing software together with its hardware/software environment, and related human interfaces.

[SOURCE ISO/IEC FDIS 20924, 3.2.7 (for IoT, incorporating additions to NOTE)]

3.1.17
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

3.1.18
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.

[SOURCE IEC 62443-4-2]

3.1.19
product supplier
organization that is responsible for compliance of a product with ISASecure requirements

NOTE The definition of product supplier in [IEC 62443-4-2] is “manufacturer of hardware and/or software product.” The definition is revised here since the product manufacturer may not always be the organization responsible for achieving ISASecure certification for the product.

3.1.20
proximity network
network that connects the 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 text in [IICRA]]

3.1.21
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.

[SOURCE IEC 62443-3-3]

3.1.22
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.

[SOURCE IEC 62443-4-2]

3.1.23
supplier
product supplier

3.1.24
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.

3.1.25
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]

3.1.26
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]

3.1.27
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

[SOURCE IEC 62443-4-2]

3.1.28
upgrade
incremental hardware or software change in order to add new features

[SOURCE IEC 62443-4-2]

3.1.29
version (of component)
well defined release of a component, typically identified by a release number

3.1.30
version (of ISASecure certification)
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 ICSA 1.0.0

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
CVE	common vulnerabilities and exposures
CVSS	common vulnerability scoring system
DCS	distributed control system
DM	(security) defect management
FDIS	final draft international standard
FSA-C	functional security assessment for components
FSA-IC	functional security assessment for IIoT components
HMI	human-machine interface
IACS	industrial automation and control system
IC	IIoT component
ICM	IIoT component maintenance of certification
ICSA	IIoT component security assurance
ID	identifier
IEC	International Electrotechnical Commission
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
OS	operating system
PLC	programmable logic controller
SDA-C	security development artifacts for components
SDA-IC	security development artifacts for IIoT components
SDL	security development lifecycle
SDLA	security development lifecycle assurance
SDLPA-IC	security development lifecycle assessment for IIoT components
SIS	safety instrumented system
SMA	security maintenance audit
SR	security requirement
SSA	system security assurance
SUM	security update management
TR	technical report
TS	technical specification
VIT-IC	vulnerability identification testing for IIoT components

4 Overview

This section summarizes the approach to maintenance of ISASecure ICSA certification as a component and the ISASecure ICSA certification requirements evolve, and due to the passage of sufficient time even if neither the component nor ISASecure is modified. The intent of the overall approach is to leverage previous certification results wherever possible to achieve cost effectiveness, while maintaining the integrity of the certification result over time. Sections 5 - 12 provide formal detailed requirements for the various certification maintenance scenarios described in this section.

4.1 SDLA certification prerequisite

In order to achieve any ISASecure ICSA certification and to retain validity of the certificate, the supplier must hold the ISASecure SDLA certification described in [SDLA-100] for their secure product development lifecycle process. In accordance with [SDLA-300], recertification for SDLA is required every three years.

4.2 Security maintenance audit

To retain the validity of an ICSA certification, the supplier must maintain good standing under an ongoing surveillance audit called Security Maintenance Audit, abbreviated as SMA. SMA is performed at specified times whether or not the product version as certified has been modified. Further details for when and how the certifier evaluates conformance to these requirements are found in Section 5 below. *Good standing* under SMA (see 3.1.9) for a supplier of an ICSA-certified component, formally means that SMA for the component has been conducted as required by this specification, and there are currently no open SMA nonconformities for the component.

The SMA audit reviews evidence that the supplier is operating in conformance with selected 62443-4-1 requirements under the Defect Management and Security Update Management practices of that standard. The audit applies to a previously certified product, with goal to maintain the security of ICSA-certified components over time. The first time SMA is performed for a certified IIoT component, it may be based upon historical performance one year before certification. This option offers an efficiency and cost benefit for suppliers with mature, auditable processes for maintaining the security of their products, where these processes have been applied to prior versions of the component which is now under evaluation for ICSA certification. If based on supplier performance after certification, the audit examines a period of the component lifecycle 9-18 months long after initial ICSA certification. Later, SMA occurs at the time of SDLA recertification. If the supplier has a large number of ICSA-certified components, the certifier may select from them for SMA evidence sampling, after the first SMA has been performed for each component.

Requirements audited under SMA are:

- Supplier is tracking security issues from internal and external sources that may be applicable to the certified component, and is identifying those that are applicable (62443-4-1 requirements DM-1 and DM-2)
- Supplier can provide reasonable rationale for severe security issues, and all user-reported security issues, that have no associated fix (as defined in 3.1.8) available at the time of the SMA (62443-4-1 requirement DM-4)
- Supplier's actions conform with their stated policy for timely delivery of security updates (62443-4-1 requirement SUM-5).

4.3 Modified components

Different approaches are used for certification of component updates (bug fixes) and component upgrades (new component functionality). The terms *update* and *upgrade* are formally defined in [IEC 62443-4-2] and in the present document in 3.1.27 and 3.1.28.

The intent of the ICSA maintenance of certification policy is that certification of upgrades would require a new certification, and updates do not, as long as an ISASecure SDLA certified development process is maintained for a component and the supplier maintains good standing under SMA for that component. Certification evaluations for component upgrades will leverage prior certification evidence as described in this document.

4.3.1 Component updates

Certification applies to a specific component version together with its updates. Once a supplier earns an ICSA certification, that certificate remains valid for the initial certified component version and all component updates per the definition in 3.1.27 as long as:

- the component remains in a support status such that an SDLA certified SDL process for security management still applies; and
- the supplier retains their SDLA certification; and
- the supplier is in good standing under SMA for the component, or is within the grace period determined for remediating an open SMA nonconformity.

Once issued, an ICSA certificate is amended to list version numbers for currently supported updates of the component, at the time of each SMA. [ICSA-204] provides the format for a certificate including these amendments. Optionally the certifier MAY revise the certificate to show intermediate updates of the component that occur between SMA's, for example to clarify that a particular numbered release is an update (and therefore falls under the certification) or to show a critical update on the certificate.

Section 6 provides requirements for certification of component updates.

4.3.2 Component upgrades

A component supplier is not *required* to obtain a component certification for every component upgrade. The decision to certify an upgrade is ultimately an optimization of end customer opinion and cost to the supplier. However, the component supplier is required to clearly communicate to the marketplace which versions of their component fall under an ISASecure ICSA certificate, and which version of the ISASecure criteria is met, as stated in Requirement ISASecure_IC.R3 of [ICSA-300].

If a component has achieved certification, and a component upgrade is submitted for certification to the same ISASecure ICSA version and tier, the supplier may at their option request consideration for the prior certification evidence for any or both of the certification elements SDA-IC and FSA-IC. For those elements for which consideration is requested, a well-defined evidence impact assessment is performed by the certifier that ultimately determines which aspects of the certification evaluation will need to be carried out for the modified component. Given the scope of changes to the component, if such an assessment is determined not to support revision of the evaluation with confidence, the certifier may elect to perform one or both of the evaluation elements in full for the modified component.

If an evidence impact assessment is performed and shows that the modifications to the component and its documentation would not affect the certification results for one or both of these elements, then no certification tests or evaluations will be necessary in order for the modified component to pass that element of certification. In other cases, partial evaluations may be sufficient. The nature of modifications together with the quality of the analysis of the modifications that is required to be submitted by the supplier to the certifier in support of the certifier's evidence impact assessment, are the major factors in determining the effort required to obtain a certification for a component upgrade. However, by policy, VIT-IC is always run in its entirety on the upgraded component.

User documentation changes are evaluated along with changes to the component itself when a component upgrade is submitted for certification.

Section 7 provides requirements for certification of component upgrades.

NOTE An amended certificate for SMA, or a new certificate for a component upgrade, may be granted by the same chartered laboratory that granted the prior certificate, or by a different chartered laboratory.

4.4 Updated ISASecure criteria

As in the case of component upgrades, a component supplier is not required to revise a component certification for the latest ISASecure version. Hence, for example, a component certified to ISASecure ICSA 1.0.0 is not required to obtain a certification to ISASecure ICSA 2.0.0. However, all components going through an initial

certification or certification of an upgrade after ISASecure ICSA 2.0.0 becomes available, will be certified to that ISASecure ICSA version in accordance with the ISASecure published transition policy.

Consider the case where a component achieved certification under ISASecure ICSA 1.0.0, and this same component version is submitted for certification to the new ISASecure version, ISASecure ICSA 2.0.0. This certification process will consist of carrying out the defined delta between the two certification versions. Since the prior certificate for ICSA 1.0.0 may apply to several updates of a component, the supplier will determine one of these update versions to be used as the first certified version to be listed on a new ICSA 2.0.0 certificate. That component version will be used for examining the delta certification requirements between ICSA 1.0.0 and ICSA 2.0.0. All updates of this first version will fall under the new certificate.

An upgraded component may be submitted for certification to an ISASecure ICSA certification version that also has changed. Consider the case where a component achieved certification under ISASecure ICSA 1.0.0, and a component upgrade is submitted for certification to ISASecure ICSA 2.0.0. This certification process will be logically equivalent to first certifying the component upgrade to ISASecure ICSA 1.0.0 using the approach described in 4.3.2, and then carrying out the defined evaluation delta between the two certification versions ICSA 1.0.0 and ICSA 2.0.0 on the upgraded component.

Section 8 provides requirements for certification to modified ISASecure ICSA certification criteria. Section 9 provides requirements for certifications when both the component and the certification criteria have changed.

4.5 Certification to a higher tier

Once a component has achieved a Core tier ISASecure ICSA certification, the component supplier may modify the component and/or available process evidence as deemed necessary, and then apply for an Advanced tier ICSA certification. As noted in 4.1, the supplier must hold an ISASecure SDLA certification for an SDL process that applies to the component going forward to achieve an Advanced tier ICSA certification (as for any ICSA certification). Any component modifications are first assessed to the original tier following the approaches outlined in 4.3.

The validations for SDA-IC evaluation criteria related to residual risk due to known security issues will differ by certification tier, as will FSA-IC requirements. The certifier will therefore evaluate the SDA-IC and FSA-IC certification criteria for Advanced tier, where different from those for Core tier. Finally, the certifier will rerun VIT-IC and apply the pass/fail criterion for Advanced tier. If no component modifications are required to achieve Advanced tier, since the prior Core tier certificate may apply to several updates of a component, the supplier will determine which one of these update versions will be used as the first certified version to be listed on the new Advanced tier certificate. That component version will be used for examining the delta certification requirements between the two certification tiers.

Section 10 provides requirements for this case.

NOTE In ISDLA-312 version 6.3, the validation activities for the requirements SDLA-SR-2J-ICSA, SDLA-2K-ICSA, SDLA-SR-4-ICSA, and SDLA-DM-4-ICSA1 are dependent upon tier.

4.6 ICSA for previously CSA certified components

Sections 11 and 12 describe a streamlined process via which a supplier may obtain an ICSA certification for a component that previously was certified under the ISASecure CSA program. The certifier will assess only the delta requirements between these programs and an updated VIT-IC result.

5 Requirements for security maintenance audit

This section describes the SMA process, which consists of a series of audits performed over the lifetime of an ICSA certified product. A supplier is required to maintain good standing under the SMA process in order for their ICSA product certificates to remain valid, as stated below in Section 6 ISASecure_ICM.R2.

Requirement ISASecure_SMA.R1 – Time period and subject releases for first security maintenance audit

For the first SMA for an ICSA certified product, the supplier SHALL elect a time period and subject releases for audit coverage which SHALL be one of:

- ***One year before certification (historical):*** The one-year period before the ICSA certification process takes place. The subject releases for this audit are prior versions of the product that is under ICSA evaluation, whether or not these prior versions were certified (called “Historical SMA”). The SMA in this case SHALL be performed at the same time as initial certification. Its results would not impact the initial certification result; or

- ***One year after certification:*** The one-year period after ICSA certification. The subject releases of this audit are the certified version of the product and its updates and upgrades, whether or not certified; or

- ***Next SDLA recertification:*** The period from the point of ICSA certification, up to the time of the next SDLA recertification of the supplier, where the recertification applies to the SDL for which the product falls under the scope of that SDL. This option MAY be selected IF this period is between 9 months and 18 months in length. The subject releases of this SMA are the certified version of the product and its updates and upgrades, whether or not certified. This option allows SMA activities and SDLA recertification activities to be coordinated for efficiency where feasible.

The first option, historical SMA, SHALL be permitted only if previous versions of the product have been available from the supplier for a year or more.

NOTE 1 The historical SMA offers a benefit for an organization with a mature and ongoing security maintenance process, so that they may maintain their ICSA certification with fewer separate interactions with the certifier. This option combines the SMA audit, which is intended to gain confidence in a supplier’s security maintenance process for a specific product, with the initial certification activity for that product. Use of this option will be successful if there is product history that supports this confidence.

Requirement ISASecure_SMA.R2 – Time period and subject releases for security maintenance audit after first one

After the first SMA for an ICSA certified product, later SMAs as specified in ISASecure-SMA.R3 SHALL occur

- *if the prior SMA did not use the historical SMA option (so took place after initial certification):* at the time of each SDLA recertification for the supplier

- *if the prior SMA used the historical SMA option:* at a time selected by the supplier which SHALL be a minimum of nine months and a maximum of two years after initial certification, and which MAY be at the same time as SDLA recertification if desired, assuming the SDLA certification falls within this time period.

The SDLA recertification SHALL be for the SDL for which the product falls under the scope of that SDL. The subject releases for this SMA SHALL be the certified product and all updates and upgrades, whether or not certified, for the time period between the prior SMA and this SMA.

Requirement ISASecure_SMA.R3 – Content of security maintenance audit

A certifier SHALL perform the following verification actions to carry out a Security Maintenance Audit for each ICSA-certified product, under the schedule defined under ISASecure_SMA.R1 and SMA.R2, except where sampling applies as described under ISASecure_SMA.R4.

NOTE 2 In the following, the term “fix” has the meaning described in 3.1.8.

- *Receiving notifications of security-related issues:* For the SMA time period and subject releases as determined by ISASecure_SMA.R1 or R2, determine whether there have been notifications received from each major source for security-related issues potentially related to those subject product releases, that were ultimately determined to be applicable to those releases (as described in 62443-4-1 requirements DM-1 and DM-2). If not, verify that no issues can be identified in at most one day of research, that should have been received from those sources and classified as applicable to those releases.

- *Addressing user reported issues:* For the SMA time period and subject releases as determined by ISASecure_SMA.R1 or R2, view the list of any security issues reported to the supplier by users of the subject releases. Among those, identify any issues where either:

- the supplier has not yet reviewed their applicability to product releases or has not yet determined how to address them, or
- the supplier has assessed them as not applicable to the product release, or
- a decision has been made to address them with some option listed under 62443-4-1 requirement DM-4 other than (a) to fix, or
- the option (a) to fix, has been selected but the update is not available at the time of this evaluation.

If any issues are found meeting these criteria, verify there is an overall pattern of reasonable explanations (such as low CVSS score, use of non-recommended configuration by customer, review of applicability is in accordance with timeliness criterion required for conformance with 62443-4-1 DM-2 for reviewing security-related issues, fix is in progress and evidence shows that planning for the fix considered the policy required under 62443-4-1 SUM-5 for timely delivery of security patches).

- *Addressing severe issues:* Identify any severe security issues reported to the supplier from any source, during the SMA time period and for the subject releases as determined by ISASecure_SMA.R1 or R2. Severe is specified for Core tier as base CVSS score high or above or a similar score, and for Advanced tier as CVSS Medium or above or a similar score. Determine the subset of these that were determined applicable to a product release but not addressed by fixing per option a) of IEC 62443-4-1 requirement DM-4, as of the time of this evaluation. Verify for a sample of these that there is a pattern of either reasonable documented explanations for the decision not to fix, or reasonable explanations why a fix is not yet available. Examples of such explanations in addition to those mentioned above are: that the fix is planned for an upgrade with delivery in 2 months (where 6 months might be unreasonable), or that the full fix is too extensive for one release, so parts of it have been planned for later releases.

- *Delivering timely security updates:* Verify that any security updates delivered in the time period for the SMA, for components that are subject releases for the SMA as determined by SMA.R1 or R2, conform to either the SDLA policy for timely delivery of security updates in place at the time of the SMA, or a prior SDLA policy on this topic applicable to these updates.

A specific SMA SHALL be recorded as “passed” if all verifications in this requirement are recorded as “Met.”

Requirement ISASecure_SMA.R4 – Use of product sampling for security maintenance audit

This requirement applies for SMA’s after the first SMA for a product, when a supplier has more than three products for which an SMA is required at the time of the supplier’s SDLA recertification. Any required remediation of nonconformities found during the SMA for products under this sampling process SHALL proceed as described under ISASecure_SMA.R5. The status of certificates for those products SHALL be managed in accordance with ISASecure_ICM.R2.

The following steps describe the sampling process, which is illustrated in Figure 1.

The process in some situations specifies selection of products to create two or three sample sets. If at any point in this process there is an insufficient number of ICSA certified products remaining to create a sample set with the number of products specified, then all remaining products SHALL comprise the sample set and be audited under SMA.

Select first sample set The certifier SHALL select three products among the supplier’s ICSA-certified products for which to apply the SMA evaluation specified in ISASecure_SMA.R3. For this initial sample set, one product SHOULD be selected at random, and the others on the judgement of the certifier, based upon factors that influence risk as described below.

No nonconformities in first sample set If SMA passes (per ISASecure_SMA.R3) for the three products, then all of the supplier’s products due for SMA at the time of this SDLA recertification SHALL be recorded as passing their SMA. The ICSA SMA sampling process for this period is complete.

Nonconformities in first sample set If nonconformities were found in the first SMA sample set, the following further steps SHALL be taken.

Supplier self audit The supplier SHALL carry out a self-audit to determine if the cause of the nonconformities found in the first sample set is systemic or a unique circumstance, and to determine if other products are impacted. The supplier SHALL create a related action plan based on the self-audit results. The certifier SHALL verify that the supplier has performed a self-audit and has created an action plan consistent with the results of that audit.

Select second sample set The certifier and the supplier SHALL agree on a time for selection of a second sample set of three products for which to perform SMA. This time SHOULD be 15-45 days from when the nonconformities in the first SMA sample set were reported to the supplier.

No nonconformities in second sample set If no nonconformities are found in the second sample set, all ICSA certified products of the supplier SHALL be recorded as passing SMA, with the exception of those from the first sample set still undergoing remediation.

Nonconformities in second sample set If nonconformities were found in the second SMA sample set, the following further steps SHALL be taken.

Select third sample set The certifier and the supplier SHALL agree on a time for selection of a third sample set of three products for which to perform SMA. This time SHOULD be 15-45 days from when the nonconformities in the second SMA sample set were reported to the supplier.

No nonconformities in third sample set If no nonconformities are found in the third sample set, all ICSA certified products of the supplier SHALL be recorded as passing SMA, with the exception of those from prior sample sets still undergoing remediation.

Nonconformities in third sample set If a product is found with SMA nonconformities in the third sample set, no grace period SHALL be granted for these nonconformities, and the certifier SHALL suspend the certificate for that product in accordance with ISASecure_ICM.R2. Sampling ceases and all ICSA certified products SHALL be individually audited under SMA to maintain their ICSA certificates.

In selecting products for a sample set, the certifier SHOULD give priority to products with these factors that increase risk:

- Nonconformities found in internal audits or prior certification audits
- Different from other products in the sample set selected
- Use of new technology by the product
- Use of new development resources, processes, or tools for the product
- Short product history
- Significant amount of development activity on the product over the time period to be audited
- Significant amount of development activity on third party components of the product over the time period to be audited
- Highly complex product
- Potential risk to health, safety, or the environment as the product is applied by asset owners.

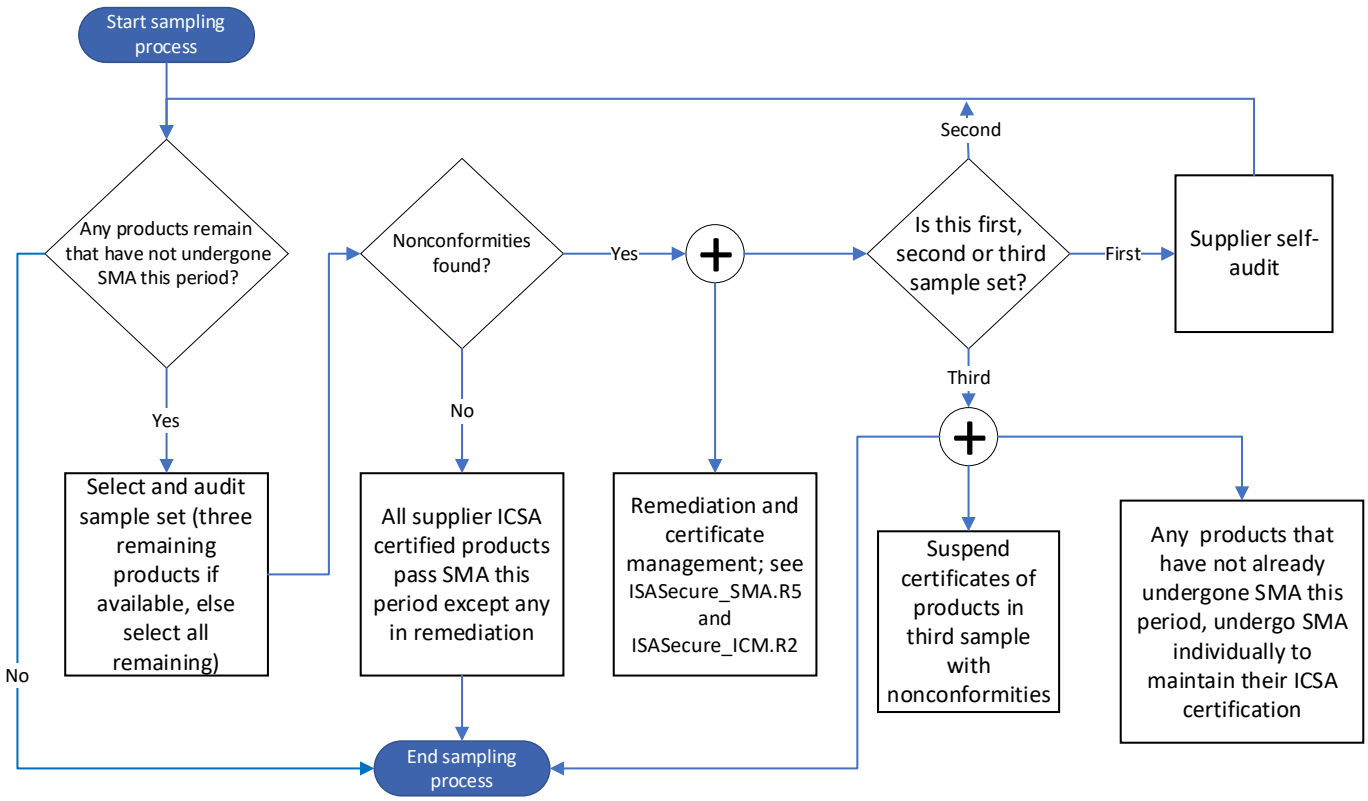

Figure 1. SMA Product Sampling

Requirement ISASecure_SMA.R5 – Closing a nonconformity under security maintenance audit

If an SMA for a certified component does not pass, an audit finding that is a reason why the product did not pass, is called an SMA nonconformity for the component. The certifier and the supplier SHALL agree on a grace period within which evidence is to be submitted of remediation of this SMA nonconformity. This time should be 30-90 days from when the nonconformity was reported to the supplier. If the criteria for remediation are met, the SMA nonconformity SHALL be closed. For each SMA topic for which SMA did not pass, the certifier SHALL verify the following criteria for remediation are met:

- *Receiving notifications of security-related issues*: Supplier has selected an option as described under under 62443-4-1 DM-4, for addressing those specific issues identified by the certifier as not being received, and those identified by the certifier as received, but possibly incorrectly classified as inapplicable to the product. Supplier at a minimum has assigned adequate resources and tasking to carry out the selected option. Supplier has identified any process weaknesses contributing to this nonconformity and modified the process to address any such weaknesses. Supplier has applied their modified process to identify any additional notifications for security issues that should be received or reassessed for applicability to the product, and likewise has selected an option to address these issues and at a minimum assigned adequate resources and tasking to carry out the selected option. For each of these issues not fixed per option a) of 62443-4-1 requirement DM-4, as of the time of submission of SMA remediation evidence to the certifier, there is a reasonable documented explanation for a decision not to fix, or for why the fix is not yet available.

NOTE 3 See note under ISASecure_SMA.R3 regarding the meaning of the term “fix.”

- *Addressing user reported issues:* For user reported issues whose status was judged by the certifier as not supported by a reasonable explanation, supplier has revisited their selection of options as described

under 62443-4-1 DM-4 to address these issues. At a minimum the supplier has assigned adequate resources and tasking to carry out any resulting actions. The supplier has resubmitted documented rationale to the certifier for the status of those issues that meet the criteria described under ISASecure_SMA.R3 as of the time of submission of remediation evidence to the certifier. User issues from the SMA period under remediation, and any new issues submitted by users after that SMA period are to be included. There is a pattern of reasonable explanations for the status of these user-reported issues as described under ISASecure_SMA.R3.

- *Addressing severe issues:* For all severe issues as defined under ISASecure_SMA.R3, supplier has revisited their selection of options as described under 62443-4-1 DM-4 to address these issues. At a minimum the supplier has assigned adequate resources and tasking to carry out any resulting actions. The supplier has submitted documented rationale for those not fixed, as of the time of submission of remediation evidence to the certifier. Severe issues from the SMA period under remediation, and newly found after that SMA period, are to be included. For a new sample of these issues selected by the certifier, there is a pattern of reasonable documented explanations for their status.

- *Delivering timely security updates:* Supplier has identified root cause and any process weaknesses contributing to this nonconformity, and modified the process to address any such weaknesses. An additional partial SMA covering this topic is scheduled for one year after the SMA requiring this remediation.

6 Requirements for certification of component updates

This section addresses maintenance of certification for updates of a component, which are defined in 3.1.27.

Requirement ISASecure_ICM.R1 – Identification of updates and upgrades

A chartered laboratory SHALL reach agreement with an applicant for ICSA certification, on a policy that can be applied based upon examining component version numbers, that determines whether a new version falls under an existing certificate, or would require a new certification. The intent of the policy is that upgrades of a certified component (see 3.1.28) SHALL require a new certification, and updates (see 3.1.27) SHALL NOT.

NOTE 1 A new ICSA certificate would be issued when:

- a component achieved initial ICSA certification per the criteria in [ICSA-300]; or
- an upgrade of an initially ICSA certified component achieved certification under the processes in the present document; or
- any ICSA certified component achieved certification to a new certification version or tier under the processes in the present document; or
- a CSA certified component achieved ICSA certification under the process in the present document.

Requirement ISASecure_ICM.R2 – Component and update certification, suspension and withdrawal

An ICSA certification remains valid for a certified component, and applies to any update of a certified component (as identified under ISASecure_ICM.R1), for as long as:

- the supplier of the component maintains an ISASecure SDLA certification; and
- the scope of the SDLA certified process includes the component; and
- the component remains in a support status such that the certified SDL process for security management still applies; and
- the supplier is in good standing under SMA for that component (see 3.1.9) or is within an SMA remediation grace period for any open SMA nonconformities (as described in ISASecure_SMA.R5).

If a supplier does not maintain an SDLA certification with scope that includes the ICSA certified component, then after a one-year grace period, the ICSA certification for that component SHALL be withdrawn.

If a supplier has an open SMA nonconformity for a component, and if after the agreed grace period per ISASecure_SMA.R5, has not closed the nonconformity, the ICSA certification for that component SHALL be suspended. If all open SMA nonconformities for a product have been closed within a year of the report of those nonconformities to the supplier, a suspended ICSA certification SHALL be restored. If an open nonconformity has not been closed within a year of the report of that nonconformity to the supplier, the ICSA certification for the component SHALL be withdrawn.

A supplier SHALL inform the certifying chartered lab when a certified component has transitioned to a minimal or no support status, such that the certified SDL process for security management no longer applies. The chartered laboratory SHALL withdraw the certificate upon receiving this notification.

After initial certification, it is possible that previously unknown vulnerabilities may become known in the product version initially certified, or in one of its updates. It is possible that the severity of such a vulnerability exceeds the risk threshold established for the product per ISDLA-312 requirement SDLA-DM-4-ICSA1, or that the vulnerability prevents the product from meeting one or more functional requirements for certification. In these situations, if the supplier concludes that it is infeasible or impractical to fix the issue with a product update, the supplier SHALL inform the certifying chartered laboratory, who SHALL withdraw the certification. The certification body SHALL reasonably coordinate with the supplier so that the supplier may communicate with product users before the certification is withdrawn, but in all cases SHALL withdraw the certification at most 90 days after being informed by the supplier that the vulnerability will not be fixed by a product update. The supplier SHALL communicate with product users regarding the vulnerability as required by IEC 62443-4-1 Requirement DM-5 Disclosing security-related issues.

NOTE 2 The chartered laboratory informs ISCI about certificates granted and changes in certificate status as described in Requirement ISASecure__ICSA.R39 in [ICSA-200].

7 Requirements for certification of component upgrades

The requirements in this section cover certifying a component upgrade, when a previous version of the component has already been certified to the same ISASecure ICSA version and tier.

7.1 Criteria for applying prior certification evidence to component upgrade

The following requirements provide the general criteria under which evidence from prior certifications of a component is considered applicable toward earning certification for a component upgrade. Specific requirements on how these criteria are evaluated follow in Section 7.3.

Requirement ISASecure_ICM.R3 – SDA-IC certification element for component upgrade

If a component has been ICSA certified, then a component upgrade SHALL on the basis of that prior evidence pass the SDA-IC element of certification if:

- the certifier determines that an evidence impact assessment to determine whether the component modifications may have impacted each applicable line item of the SDA-IC can be performed with confidence. An applicable line item is a cell in the "Component or System Evaluation Activity" column in a single SDLA ID row in the [ISDLA-312] matrix, where that row has the "Component" column marked with an ‘X’; and

- the certifier carries out this assessment; and

- the certifier has evaluated at their discretion, any (and possibly all) of the artifacts associated with the potentially impacted SDA-IC line items, and given them pass status.

The SDA-IC report in this case MAY include only a summary of the evidence impact assessment relative to SDA-IC, and the validations performed, plus a reference to the prior SDA-IC evaluation for the component. If the certifier judges that such an evidence impact assessment cannot be performed with confidence, the certifier SHALL carry out a full SDA-IC evaluation for the component as described in [ICSA-312].

Requirement ISASecure_ICM.R4 – FSA-IC certification element for component upgrade

If a component has been ICSA certified, then a component upgrade SHALL on the basis of that prior evidence pass the FSA-IC element of certification if:

- the certifier determines that an evidence impact assessment for the prior FSA-IC results for the component can be performed with confidence; and
- the certifier carries out this assessment and shows that component modifications have either not impacted these results, or may have impacted few FSA-IC line items in [ICSA-311] in a manner isolated from other line items; and
- the certifier has evaluated any potentially impacted FSA-IC line items and given them pass status.

Component modifications SHALL be shown to have no impact on results for a line item of the FSA-IC by showing:

- no architecture change, functionality change or significant new code has been incorporated related to a security feature referenced by the line item of the FSA-IC.

In this case the certification report covering FSA-IC MAY consist of only a summary of the FSA-IC evidence impact assessment, results for those line items that were evaluated, and a reference to the prior certification report for the component. If the certifier determines that an FSA-IC evidence impact assessment cannot be performed with confidence, or that component changes related to the FSA-IC are widespread, then the certifier SHALL perform the full FSA-IC for the component and a full report SHALL be provided for that certification element.

NOTE It is well understood that security features do not stand alone and are inherently interrelated in providing coherent protection for a component. Therefore, if there are sufficient changes to security functionality for a component which it appears may interact, then the full FSA-IC is likely to be performed on the modified component. This is because an evidence impact assessment attempting to isolate the line items affected by the modifications, will likely need to examine all FSA-IC line items to gain confidence, which will make this assessment essentially equivalent to simply performing a full FSA-IC.

Requirement ISASecure_EDM.R5 – Deleted

7.2 VIT-IC assessment for a component upgrade

VIT-IC is always rerun for a component upgrade, as detailed in the following requirements. The concept of "consideration for prior evidence" does not apply for the VIT-IC certification element.

Requirement ISASecure_ICM.R6 – VIT-IC certification element for component upgrade

If a component has been ICSA certified, and a component upgrade later presented for certification, VIT-IC SHALL be executed on the modified component such that the test meets the same requirements as for an initial certification, as described in [ICSA-300] and [SSA-420]. In some cases, it may be run by the supplier instead of the chartered laboratory. In particular, if any FSA-IC validations by independent test are required by [ICSA-311] for the certification of the component upgrade per Requirement ISASecure_ICM.R4, then VIT-IC SHALL be performed by the chartered laboratory. If no FSA-IC validations by independent test are required, the chartered laboratory MAY permit the supplier to perform VIT-IC in accordance with the requirements in [SSA-420], and to submit the results. The chartered laboratory MAY rerun the test at their discretion.

Requirement ISASecure_ICM.R7 – Requirements on supplier-executed VIT-IC for component upgrade

If a supplier executes VIT-IC toward certification of a component upgrade under the conditions in Requirement ISASecure_ICM.R6, this process SHALL meet the following requirements:

- supplier personnel responsible for the VIT-IC SHALL have successfully completed a training class or 1 year of job experience demonstrating proficiency with the VIT tool to be used;
- the supplier SHALL run the test with a policy file provided by the chartered laboratory;

- the chartered laboratory SHALL witness execution of the VIT-IC by the supplier, including starting the test, saving the report file, and signing of the report. This witnessing MAY be achieved remotely.

- the supplier SHALL submit as evidence of VIT-IC:

    - documentation of the tested component configuration, that contains the same information the chartered laboratory would record if they performed the test;

    - the policy file used to run the test;

    - the command line that was executed to run the test; and

    - the full report from the VIT tool; and

- the VIT-IC evidence submitted to the chartered laboratory SHALL be signed by a responsible representative of the supplier.

7.3 Evidence and assessment for criteria

If based upon the criteria in Section 7.1, a component supplier believes that some of the evidence used to certify a previous version of a component is applicable toward certification of a component upgrade, they may request consideration for this evidence. In this case, their submission of data toward certification of the modified component will include supporting evidence to demonstrate that the criteria stated in the requirements of 7.1 are met. This section specifies the nature of that supporting evidence and how the certifier carries out an evidence impact assessment relative to the evidence from the prior certification evaluation, based upon the supplier's supporting evidence regarding component changes.

Requirement ISASecure_ICM.R8 – Submission of component modification data

A component supplier applying for certification for a component upgrade, MAY request consideration for SDA-IC and/or FSA-IC evaluations done on a prior version of the component that achieved certification. If so, the applicant SHALL submit to the certification process:

- a high level description of modifications to the component since the prior ICSA evaluation of the component (which may have been for an initial certification or a prior upgrade);

- a mapping from the elements of this description to a detailed change log extracted from the change management system for the component software; and

- evidence that this extraction from the change management system constitutes all changes in the modified component; and

- a list of any third party sub components that had new CVE reports against them since the prior certification; whether or not addressed by the time of application for certification; and

- a list of any changes in third-party supplied sub components such as an OS service pack update; and

- a high level summary of any changes to user documentation related to component security.

Requirement ISASecure_ICM.R9 – Submission of analysis of modifications for component upgrade

If a component supplier has submitted evidence per Requirement ISASecure_ICM.R8 – Submission of component modification data, then they SHALL in addition submit the following to the certification process:

- if consideration is requested for prior SDA-IC evidence:

    - an analysis of the SDA-IC matrix, that for each numbered requirement and SDLA ID, considering the validation activity in the column labeled "Applies for Component or System Certification" in [ISDLA-312], either:

- States that no additional actions beyond those previously carried out to meet this requirement for the prior certification are required to meet this validation requirement for this certification, or

- Briefly describes additional actions beyond those previously carried out to meet this requirement for the prior certification, which were carried out to meet this validation requirement for this certification.

- if consideration is requested for FSA-IC: an analysis of the FSA-IC matrix, that notes for each numbered line item in [ICSA-311] that applies to the component types and tier for the ICSA certification, whether there is any change to the functionality or code described by this requirement, among the component modifications since the previous certification. If so, the applicant SHALL provide a mapping to the related code modifications at the CM level of detail (as reported under Requirement ISASecure_ICM.R8).

Requirement ISASecure_ICM.R10 – Determination of no evidence impact for SDA-IC line item

When performing an evidence impact assessment for a component upgrade where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a particular line item of the SDA-IC evaluation have occurred if:

- the analysis submitted of the SDA-IC matrix as described under Requirement ISASecure_ICM.R9 reports no impact; and

- a certifier review of evidence submitted per Requirement ISASecure_ICM.R8 and Requirement ISASecure_ICM.R9 finds no indication of such an impact after consultation with the component supplier.

Requirement ISASecure_ICM.R11 – Determination of no evidence impact for FSA-IC line item

When assessing modifications for a component upgrade where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a specific FSA-IC line item have taken place if:

- the analysis submitted of the FSA-IC matrix as described under Requirement ISASecure_ICM.R9 reports no changes to functionality covered by this line item of the FSA-IC since the last certification; and

- a certifier review of evidence submitted per Requirement ISASecure_ICM.R8 and Requirement ISASecure_ICM.R9 finds no indication of such changes after consultation with the component supplier.

Requirement ISASecure_EDM.R12 – Deleted

Requirement ISASecure_ICM.R13 – Criteria for granting a certification for component upgrade

If a component has been ICSA certified, then a component upgrade SHALL be granted certification to the same tier and ISASecure ICSA certification version if:

- the organization that will develop the component going forward holds an ISASecure SDLA certification. In particular, the supplier SHALL hold an SDLA certification at the time of application for the certification of the component upgrade, and the scope of the process certified SHALL include that component; and

- the supplier is in good standing under SMA for the previously certified component (as defined in 3.1.9); and

- criteria for passing the SDA-IC element of certification are met per ISASecure_ICM.R3 and Requirement ISASecure_ICM.R10 ; and

- criteria for passing the FSA-IC element of the certification are met per ISASecure_ICM.R4 and Requirement ISASecure_ICM.R11; and

- criteria for passing the VIT-IC element of certification are met per ISASecure_ICM.R6 and R7.

Alternatively, for each of the evaluation elements SDA-IC or FSA-IC for which the supplier did not request consideration for the prior certification per Requirement ISASecure_ICM.R8, the certifier SHALL evaluate that element under the criteria for initial certification found in [ICSA-300].

8 Certification to updated ISASecure criteria

The requirements in this section cover certification of a component that holds a prior certification, to a later version of the ISASecure certification criteria. These requirements suffice in the case that the component itself has not undergone upgrade modifications as well. If it has, see Section 9.

Requirement ISASecure_ICM.R14 – SDA-IC element for certification to a later ISASecure version

A component that has been ISASecure ICSA certified SHALL pass the SDA-IC element of a certification to a later ISASecure ICSA version at the same tier as this previous certification, if any changed SDA-IC requirements or changed validations in this ISASecure ICSA version for this tier, are assessed as pass for the component.

NOTE It is possible that this requirement may be met for a component, even though the related new or changed process requirement is not yet fully implemented as a change to the SDLA-certified development process under which the component is developed. The requirement may therefore be met for this component, but not met (yet) for all components under that process. The requirement for maintenance of the development process itself for new ISASecure requirements, is described in [SDLA-300].

Requirement ISASecure_ICM.R15 – FSA-IC element for certification to a later ISASecure version

A component that has been ISASecure ICSA certified SHALL pass the FSA-IC element of a certification to a later ISASecure ICSA version at the same tier as this previous certification if:

- any new FSA-IC requirements added in this ISASecure version that are applicable to this tier, are assessed for the component as either *Met, Met by component, Met by integration into system, or Not Relevant,* per the criteria specified in the validation activity in [ICSA-311]; and
- any changed FSA-IC requirements or changed validations in this ISASecure version that are applicable to this tier, are likewise assessed for the component as either *Met, Met by component, Met by integration into system, or Not Relevant*.

Requirement ISASecure_ICM.R16 – VIT-IC element for certification to a later ISASecure version

A component that has been ISASecure ICSA certified SHALL pass the VIT-IC element of a certification to a later ISASecure ICSA version if the component passes VIT-IC as specified for that later ISASecure version, under the same requirements in 7.2 that apply when certifying component upgrades.

Requirement ISASecure_ICM.R17 – Criteria for granting a certification to a later ISASecure version

A component that has been ISASecure ICSA certified SHALL be granted a new certification to a later ISASecure ICSA version at the same tier as this previous certification if:

- the organization that will develop the component going forward holds an ISASecure SDLA certification. In particular, the supplier SHALL hold the SDLA certification at the time of application for the certification of the component, and the scope of the process certified SHALL include that component; and
- the supplier is in good standing under SMA for the previously certified product, (as described in 3.1.9); and
- certification criteria for passing SDA-IC for this tier are met per ISASecure_ICM.R14; and
- certification criteria for passing the FSA-IC for this tier are met per Requirement ISASecure_ICM.R15 ; and
- certification criteria for passing the VIT-IC for this tier are met per Requirement ISASecure_ICM.R16.

The certification report SHALL cover only the tests and assessments performed for the certification as defined by these requirements.

9 Certification for both component upgrade and new ISASecure version

It will be a common scenario that a certified component will have been upgraded by the time a new version of ISASecure ICSA certification criteria is released. Thus, it will be useful to be able to certify a component upgrade to a newer version of ISASecure ICSA, without repeating the overall process. The following requirement provides a means to achieve this. It states that requirements are met in this case for both certification of component upgrades and certification to the later ISASecure ICSA version.

Requirement ISASecure_ICM.R18 – Certification of a component upgrade to a later ISASecure version

For a component, that previously received an ISASecure ICSA certification, a certifier SHALL grant a new certification to a later ISASecure ICSA version for a component upgrade, if the criteria in both Requirement ISASecure_ICM.R13 and Requirement ISASecure_ICM.R17 are met.

10 Certification to a higher ISASecure ICSA tier

Once a component has achieved certification at ISASecure CSA Core tier, the supplier may modify the component or available process evidence as deemed necessary, and then apply for Advanced tier certification. The following requirement applies in this situation.

Requirement ISASecure_ICM.R19 – Certification of a component to a higher tier

For a component, that previously received an ISASecure ICSA certification to Core tier, a certifier SHALL grant a certification to Advanced tier for a (possibly upgraded) component if:

- if the component has been upgraded since the ICSA Core tier certification was received, the criteria for granting a certification for Core tier for the modified component are met per Requirement ISASecure_ICM.R13; and
- the additional FSA-IC requirements present for Advanced tier certification that are not present for Core tier certification, or for which validation criteria differ between Core and Advanced tier, have been assessed as pass; and
- the SDA-IC requirements for which validation criteria differ between Core tier and Advanced tier, have been assessed as pass; and
- the supplier holds an ISASecure SDLA certification at the time of granting of the certification that applies to the component going forward; and
- the supplier is in good standing under SMA for the component as previously certified (as described in 3.1.9); and
- VIT-IC has passed for Advanced tier, per the same requirements in 7.2 that apply when certifying component upgrades.

In this case the certification report SHALL provide content per Requirement ISASecure_ICM.R13 as well as report on the new requirements assessed to achieve Advanced tier.

NOTE In accordance with [ICSA-300] and [ICSA-312], SDA-IC requirements for which validation differs by ICSA tier, are those requirements with validation activities explicitly defined as dependent upon the tier for the component. In ISDLA-312 version 6.3, this is true for the requirements SDLA-SR-2J-ICSA, SDLA-SR-2K-ICSA, SDLA-SR-4-ICSA, and SDLA-DM-4-ICSA1.

11 Certification to ICSA for component previously CSA certified

The requirements in this section describe a process for obtaining ICSA certification for a component that holds an ISASecure CSA certification. These requirements suffice in the case that the component itself has not undergone upgrade modifications as well. If it has, see Section 12.

Requirement ISASecure_ICM.R20 – SDA-IC element for component previously CSA certified

A component that has been ISASecure CSA certified SHALL pass the SDA-IC element of certification for ISASecure ICSA for a selected tier, if the following validation activities are carried out as specified for ICSA and pass for the component:

- Validation activities for SDA-IC requirements for the selected ICSA tier, that are added or modified from those that apply for the capability security level of the component's CSA certification.

NOTE 1 These are the validation activities in the document [ISDLA-312] with SDLA ID containing the string "ICSA" An example is SDLA-SR-1-ICSA.

Requirement ISASecure_ICM.R21 – FSA-IC element for component previously CSA certified

A component that has been ISASecure CSA certified SHALL pass the FSA-IC element of certification for ISASecure ICSA for a selected tier, if the following are assessed as specified for ICSA and pass for the component:

- FSA-IC requirements for the selected ICSA tier that are additions to FSA-C requirements that apply for the capability security level of the component's CSA certification; and

- Identical FSA requirements that apply both for the selected ICSA tier and the capability security level for the component's CSA certification, but have different validation activities under these two programs.

NOTE 2 All FSA-IC requirements for ICSA that are not present in FSA-C for CSA at any level, are found in the "ICSA additions" section of [ICSA-311]. Changes to validation activities for identical requirements used for both CSA and ICSA, are shown in a distinguished font in other sections of [ICSA-311]. The informative document [ISASecure-119] describes the differences between ISASecure CSA and ISASecure ICSA. Differences are enumerated specifically between CSA capability security level 2 and ICSA Core tier, and between CSA capability security level 4 and ICSA Advanced tier. These would be the most common cases for leveraging a CSA certification to obtain an ICSA certification, but other situations are not ruled out in the present requirement. It is expected that certification bodies will advise their clients on the most efficient path to achieve their client's desired certification(s).

Requirement ISASecure_ICM.R22 – VIT-IC element for component previously CSA certified

A component that has been ISASecure CSA certified SHALL pass the VIT-IC element of a certification for ISASecure ICSA for a selected tier, if the component passes VIT-IC for that tier under the same requirements in 7.2 that apply when certifying component upgrades.

Requirement ISASecure_ICM.R23 – Criteria for granting ICSA certification for component previously CSA certified

A component that has been ISASecure CSA certified SHALL be granted a new certification to ICSA for a selected tier if:

- the organization that will develop the component going forward holds an ISASecure SDLA certification. In particular, the supplier SHALL hold the SDLA certification at the time of application for the ICSA certification of the component, and the scope of the process certified SHALL include that component; and

- certification criteria for passing SDA-IC for the selected tier are met per Requirement ISASecure_ICM.R20; and

- certification criteria for passing FSA-IC for the selected tier are met per Requirement ISASecure_ICM.R21; and

- certification criteria for passing VIT-IC for the selected tier are met per Requirement ISASecure_ICM.R22.

The certification report SHALL cover only the tests and assessments performed for the certification as defined by these requirements.

12 Certification to ICSA for upgrade of component previously CSA certified

A supplier may wish to obtain an ICSA certification for a component that was previously CSA certified, where the component has been upgraded after its most recent CSA certification. Thus, it will be useful to be able to certify such a component upgrade directly to ICSA, without first formally extending the CSA certification for that upgrade (although this can also be done if desired by the supplier). There are three possible scenarios under which an upgrade to a previously CSA certified component might obtain ICSA certification. These are:

- **Pre-upgrade functionality already qualifies for ICSA:** The component before the upgrade already meets ICSA FSA-IC criteria, and is expected to continue to meet these criteria after the upgrade.

- **Upgraded functionality to qualify for ICSA, keeping qualification for CSA:** The component before the upgrade does not meet ICSA FSA-IC criteria, but meets both CSA FSA-C and ICSA FSA-IC criteria after the upgrade.

- **Upgraded functionality to qualify for ICSA, not keeping qualification for CSA:** The component before the upgrade does not meet ICSA FSA-IC criteria, but meets ICSA FSA-IC criteria after the upgrade. However it will no longer meet CSA FSA-C criteria after the upgrade. This case is logically possible, since after the upgrade, some functional security capability required for CSA, may no longer be supported by the component. This might be due in part to the fact that there are a few functional capabilities required for CSA, but not required for ICSA.

The following requirement provides streamlined methods to achieve ICSA certification in the first two of these three scenarios. The third scenario in which security capabilities are removed by the component upgrade, is expected to be a rare occurrence. Since the removal of a security capability may often affect others, at this time ICSA does not specify a streamlined ICSA certification method for this scenario. In this case, an initial ICSA certification would be performed in accordance with [ICSA-300].

Requirement ISASecure_ICM.R24 – Criteria for granting ICSA certification for upgrade of component previously CSA certified

See the definitions above for the two cases described here. For a component that has an ISASecure CSA certification, a certifier SHALL grant a new certification for a selected ICSA tier, for a component upgrade, if either:

- **Where the component pre-upgrade functionality already qualifies for ICSA:** The criteria in ISASecure_ICM.R23 (for achieving ICSA certification) are met for the product before upgrade, and the criteria in Requirement ISASecure_ICM.R13 (for certification of an upgraded ICSA certified product) are met for the upgraded product. In other words, that requirements are met for both certifying the pre-upgrade product under ICSA, and then for certifying the upgraded product under ICSA.

- **Where the component functionality was upgraded to qualify for ICSA, keeping qualification for CSA**: The criteria specified in [CSA-301] ISASecure_CM.R13, and the criteria in the present document specified in ISASecure_ICM.R23, are both met for the component after upgrade. In other words, requirements are met for both certifying the upgraded product under CSA, and then for certifying the same upgraded product under ICSA.

NOTE The [CSA-301] requirement cited here provides criteria to grant CSA certification to an upgrade of a previously CSA certified component. These same criteria are applied here regardless of whether the supplier wishes to obtain a CSA certification along with their ICSA certification for the upgraded component.

Bibliography

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

[IICRA] Industrial Internet Consortium Reference Architecture, available at https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf