ISASecure-119

ISA Security Compliance Institute — Comparison of IIoT Component Security Assurance (ICSA) and Component Security Assurance (CSA) Certifications

Version 1.0

February 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
1.0	2023.02.28	Initial version published to https://www.isasecure.org/

Contents

Table of Tables

FOREWORD

This is an informative document that compares the certification program ISASecure® ICSA (IIoT Component Security Assurance) with the certification program CSA (Component Security Assurance). ISASecure CSA certifies control system components to the standard IEC 62443-4-2. The scope of CSA certification is software applications, embedded devices, host devices, and network devices, which are the component types defined by that standard, that are used to build control systems. ICSA certifies a subcategory of such components, which are Industrial Internet of Things (IIoT) devices and gateways, that operate incorporating a direct connection to an untrusted network. Both CSA and ICSA are developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). A description of these certification programs and the current list of documents that define them, as well as other ISASecure certification programs, can be found on the web site https://www.isasecure.org/.

1 Scope

This document provides an informative overview of differences between the product certification scheme ISASecure® CSA (Component Security Assurance) and the product certification scheme ISASecure ICSA (IIoT Component Security Assurance). The purpose of this document to help component suppliers and users to determine which certification(s) are appropriate for components they supply or use. Suppliers that have interest in ICSA who have already obtained CSA certification, can use this document to assess the delta required for ICSA certification. The document also provides a convenient introduction to the ICSA program for those already familiar with CSA or with the IEC 62443-4-2 standard [IEC 62443-4-2] to which CSA demonstrates conformance.

ISASecure CSA is a certification program for IACS (Industrial Automation and Control System) components. An IACS component is an entity that is used to build control systems and that exhibits the characteristics of one or more of a software application, embedded device, host device, or network device. These component types are defined in 62443-4-2 and in 3.1 of the present document. ISASecure CSA certifies against the 62443-4-2 technical security requirements standard, which in turn incorporates conformance to the secure product development lifecycle standard 62443-4-1 [IEC 62443-4-1]. Normative documents that formally define the ISASecure CSA certification scheme can be found at https://www.isasecure.org/.

ISASecure ICSA is a certification program for a subset of IACS components. Briefly, that subset is those physical IIoT (Industrial Internet of Things) components that have a connection to the Internet or other untrusted network. Stated formally, ICSA applies to IACS components that are IIoT devices or IIoT gateways, as defined in [ICSA-100] and in 3.1 of the present document. ICSA applies all CSA certification criteria for product development lifecycle and nearly all CSA certification criteria for technical product capabilities. ICSA then adds additional requirements to those for CSA, for both product development lifecycle and technical product capabilities. All normative documents that formally define the ISASecure ICSA certification scheme can be found at https://www.isasecure.org/.

This document is intended as an informative reference, and not as a definitive description for the CSA or ICSA programs. Normative CSA and ICSA specifications referenced for program comparison are listed in 2.2 and 2.3 of this document.

Background and rationale for the development and content of the ICSA certification scheme can be found in [IIoTCert2021].

2 References

2.1 Industry papers

[IIoTCert2021] *IIoT Component Certification Based on the 62443 Standard*, ISA Security Compliance Institute and ISA Global Cybersecurity Alliance, available at https://gca.isa.org/iiot-component-certification-based-on-62443

2.2 CSA specifications

2.2.1 General technical specifications

NOTE 1 The following is the highest level document that describes the ISASecure CSA certification program.

[CSA-100] *ISCI Component Security Assurance – ISASecure Certification Scheme v4.3*, as specified at https://www.isasecure.org/

NOTE 2 The following document is the overarching technical specification for ISASecure CSA certification.

[CSA-300] *ISCI Component Security Assurance – ISASecure Certification Requirements v4.2,* as specified at https://www.isasecure.org/

[CSA-301] *ISCI Component Security Assurance – Maintenance of ISASecure Certification v3.2,* as specified at https://www.isasecure.org/

2.2.2 Specifications for certification elements

NOTE 1 The following documents provide the technical evaluation criteria for the Functional Security Assessment element (FSA-C) of a CSA evaluation.

[CSA-311] *ISCI Component Security Assurance – Functional security assessment for components v2.3,* as specified at https://www.isasecure.org/

NOTE 2 The following documents provide the overall technical evaluation criteria for the Security Development Artifacts element of a CSA evaluation. [SDLA-312] also provides the technical evaluation criteria for the ISASecure SDLA certification of a supplier's secure product development lifecycle process.

[CSA-312] *ISCI Component Security Assurance – Security development artifacts for components v3.2,* as specified at https://www.isasecure.org/

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment v6.3*, as specified at https://www.isasecure.org/

NOTE 3 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product development lifecycle processes.

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme v2.1*, as specified at https://www.isasecure.org/

NOTE 4 The following document describes the procedures and policy parameter values used to perform the VIT (vulnerability identification testing) element of a CSA evaluation (VIT-C).

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Specification v4.5*, as specified at https://www.isasecure.org/

2.3 ICSA specifications

2.3.1 General technical specifications

NOTE 1 The following is the highest level document that describes the ISASecure ICSA certification program.

[ICSA-100] *ISCI IIoT Component Security Assurance – ISASecure Certification Scheme v1.1*, as specified at https://www.isasecure.org/

NOTE 2 The following document is the overarching technical specification for ISASecure ICSA certification.

[ICSA-300] *ISCI IIoT Component Security Assurance – ISASecure Certification Requirements v1.1,* as specified at https://www.ISASecure.org

[ICSA-301] *ISCI IIoT Component Security Assurance – Maintenance of ISASecure Certification v1.1,* as specified at https://www.ISASecure.org

2.3.2 Specifications for certification elements

NOTE 1 The following documents provide the technical evaluation criteria for the Functional Security Assessment element (FSA-IC) of an ICSA evaluation.

[ICSA-311] *ISCI IIoT Component Security Assurance – Functional security assessment for IIoT components v2.3,* as specified at https://www.ISASecure.org

[ICSA-500] *ISCI IIoT Component Security Assurance – Selected commonly accepted security practices v1.1*, available at https://www.ISASecure.org.

[ICSA-312] *ISCI IIoT Component Security Assurance – Security development artifacts for IIoT components v1.1,* as specified at https://www.ISASecure.org

NOTE 2 The [SDLA-312] and [ISDLA-312] documents contain identical information that is used for SDLA certification (SDLPA-C or SDLPA-IC). 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] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment for ICSA v6.3*, as specified at https://www.ISASecure.org

NOTE 3 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product development lifecycle processes.

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme v2.1*, as specified at https://www.ISASecure.org

NOTE 4 The following document describes the procedures and policy parameter values used to perform the VIT (vulnerability identification testing) element of an ICSA evaluation (VIT-IC). The same document is listed above for CSA.

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Testing Specification v4.5*, as specified at https://www.ISASecure.org

2.4 IACS security standards

These external references are documents that are maintained outside of the ISASecure ICSA and CSA programs and are used by the programs.

NOTE 1 [ICSA-100] and [CSA-100] describe the relationship of these programs 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
accreditation
for ISASecure certification programs, assessment and recognition process via which an organization is granted chartered laboratory status

3.1.2
artifact
tangible output from the application of a specified method that provides evidence of its application

NOTE Examples of artifacts for secure product development methods are a threat model document, a security requirements document, meeting minutes, internal test results.

3.1.3
asset owner
individual or company responsible for one or more IACS

NOTE 1 Used in place of the generic term end user to provide differentiation.

NOTE 2 This includes the components that are part of the IACS.

NOTE 3 In the context of this document, an asset owner also includes the operator of the IACS.

3.1.4
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.5
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.

3.1.6
certificate
document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

NOTE For ISASecure CSA and ISASecure ICSA, there are certificates for certified components and chartered laboratories.

3.1.7
certification
third party attestation related to products, processes, or persons that conveys assurance that specified requirements have been demonstrated

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

3.1.8
certification scheme
overall definition of and process for operating a certification program

3.1.9
certification level
capability security level for which conformance is demonstrated by a certification

NOTE 1 It is intended that a component that achieves certification to CSA capability security level *n* will meet requirements for capability security level *n* as defined in IEC 62443-4-2 "Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components."

NOTE 2 ICSA uses the term and concept "certification tiers" as defined in 3.1.36.

3.1.10 certified component
component that has undergone an evaluation by a chartered laboratory, has met the ISASecure CSA or ICSA criteria and has been granted certified status under one of these programs by the chartered laboratory

3.1.11
chartered laboratory
organization chartered by ASCI to evaluate products or development processes under one or more ISASecure certification programs and to grant certifications under one or more of these programs

NOTE A chartered laboratory is the conformity assessment body for the ISASecure certification programs.

3.1.12
conformity assessment
demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled

3.1.13
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.14
compartmentalization

use of any method or technology to separate multiple functions during execution, where separation limits their interactions to those intended

NOTE Examples of compartmentalization methods are containerization, virtual machines, hardware separation (by chip or board), enforced memory allocation, software-based micro segmentation

3.1.15
conformity assessment body

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

NOTE This is an ISO/IEC term and concept. For ISASecure CSA and ICSA, the conformity assessment body is a chartered laboratory.

3.1.16
embedded device

special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

3.1.17
essential function

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

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

3.1.18
end user

organization that purchases, uses, or is impacted by the security of IACS products

3.1.19
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 IEC 62443-4-2 did not permit this.

3.1.20
functional security assessment

assessment of a defined list of security features for a control system, or for a component of a control system

3.1.21
host device

general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

3.1.22
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]

3.1.23
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 3.1.25).

3.1.24
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 Industrial Internet Consortium Reference Architecture and Security Framework: "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 3.1.28).

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

3.1.25
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).

3.1.26
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)]

3.1.27
industrial automation and control system

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

3.1.28
network device

device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

3.1.29
pass
meet the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.30
product supplier
organization that is responsible for compliance of a product with ISASecure requirements

3.1.31
secure development artifacts
assessment of artifacts that demonstrates that secure product development and maintenance methods have been applied to a particular product

NOTE In some cases these artifacts will be created during an organization's transition to a secure product development process, for products which predate that process, but will be maintained under it going forward.

3.1.32
security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

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

3.1.33
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1 Software applications typically execute on host devices or embedded devices.

NOTE 2 Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

3.1.34
supplier
product supplier

3.1.35
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.36
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.

3.1.37
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues

3.1.38
upgrade
incremental hardware or software change in order to add new features

3.1.39
validation activity
activity performed to assess conformance to a requirement

3.1.40
version (of component)
well defined release of a component, typically identified by a release number

3.1.41
version (of ISASecure certification)
ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a three-place number, such as ISASecure CSA 1.0.0 or 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
ADV	Advanced (ICSA certification tier)
CR	component requirement
CSA	component security assurance
DCS	distributed control system
DM	Defect Management
DoS	denial of service
EDR	embedded device requirement
FDIS	Final Draft International Standard
FSA-C	functional security assessment for components
FSA-IC	functional security assessment for IIoT components
HDR	host device requirement
HMI	human-machine interface
IACS	industrial automation and control system(s)
IC	IIoT component
ICSA	IIoT Component Security Assurance
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ILAC	International Laboratory Accreditation Cooperation
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
NDR	network device requirement
OS	operating system
PART	partial
PLC	programmable logic controller
RE	requirement enhancement

SD	secure design
SDA-C	security development artifacts for components
SDA-IC	security development artifacts for IIoT components
SDL	security development lifecycle
SDLA	security development lifecycle assurance OR security development lifecycle assessment
ISDLA	security development lifecycle assessment for ICSA
SDLPA-C	security development process assessment for components
SDLPA-IC	security development process assessment for IIoT components
SG	security guidelines
SIF	safety instrumented function
SIS	safety instrumented system
SL-C	capability security level
SMA	security maintenance audit
SR	security requirements
SSA	system security assurance
SUM	security update management
TS	technical specification
VIT-C	vulnerability identification test for components
VIT-IC	vulnerability identification test for IIoT components

4 Areas of difference between CSA and ICSA

4.1 Overview

A high percentage of CSA and ICSA certification criteria are identical. The difference between these programs most immediately apparent is that ICSA offers two tiers of certification, whereas CSA offers four capability security levels. ICSA Core tier is most similar to CSA capability security level 2; ICSA Advanced tier is most similar to CSA capability security level 4. CSA assesses conformance to all applicable 62443-4-1 and 62443-4-2 requirements; ICSA adds five security development sub practices and up to 24 technical security requirements not in 62443-4-1 and 62443-4-2. For some 62443-4-2 and 62443-4-1 requirements common to both programs, ICSA specifies IIoT scenarios or augments the methods used under CSA for assessing conformance. ICSA further identifies four 62443-4-2 requirements for which conformance is not required. Both CSA and ICSA require maintaining the development process certification ISASecure SDLA as a prerequisite, and to maintain product certification. ICSA adds an additional post-certification assessment called Security Maintenance Audit (SMA) as a requirement to maintain certification. SMA is a periodic audit of defect management and security update management practices for a certified component after initial certification.

The remainder of this document enumerates these areas of difference in detail and provides related references to the ICSA specifications. Broad areas of difference are enumerated in 4.2. Section 5 – Section 12 provide details for each area.

4.2 Areas of difference

There are four elements for an initial CSA certification for a component as described in requirement ISASecure_C.R5 in [CSA-300]. These elements are listed below. They are specified in the documents shown in parentheses after each element:

- **SDLPA-C** Security Development Lifecycle Process Assessment for components: supplier holds an ISASecure SDLA certification. Requires documented processes that conform to 62443-4-1. In some cases, will also look for evidence of compliance among products that fall under the process. (Column “Development Organization and SDL Validation Activity” in SDLA-312)

- **SDA-C** Security Development Artifacts for components: lifecycle artifacts for component show it has been developed in accordance with 62443-4-1 and the documented security development lifecycle (column “Component or System Validation Activity” in SDLA-312)
- **FSA-C** Functional Security Assessment for components: component conforms with 62443-4-2 (CSA-311)
- **VIT-C** Vulnerability Identification Testing for components: Results of Nessus scan for known vulnerabilities meet defined threshold (SSA-420)

Four similar certification elements apply for ICSA. These are called SDLPA-IC, SDA-IC, FSA-IC and VIT-IC, where IC is an abbreviation for “IIoT Component.”

Areas of difference between CSA and ICSA for general topics and for these four parallel certification elements are enumerated in Table 1 below. Each area is further described in the section of the present document shown in the fourth column of the table. The reference in the last column is the location for the formal definition of criteria for passing that certification element, in the ICSA specifications.

The published specifications ICSA-311 and ISDLA-312 highlight areas of change from the corresponding CSA specification, in red font.

Table 1. Areas of difference between CSA and ICSA

Area of difference	**CSA**	**ICSA (considering both IIoT devices and gateways)**	**Further information in this document**	**ICSA Specification**
Products in scope for the certification	Component types: Software application, embedded device, host device, and network device, as defined in 3.1 of the present document	Embedded device, host device, or network device that is also an IIoT device or IIoT gateway, all as defined in 3.1 of the present document. Software-only components not addressed.	Section 5	ICSA-300 section 1

Certifications available	Capability security level 1, 2, 3, or 4	Core tier or Advanced tier	Section 6	ICSA-100 section 4.3;
				ICSA-300 section 4.2;
				ICSA-300 Requirement ISASecure_IC.R5

Area of difference	CSA	ICSA (considering both IIoT devices and gateways)	Further information in this document	ICSA Specification
Secure product development lifecycle process assessment (SDLPA)	Supplier holds SDLA certification. SDLA assessment verifies existence of documented process for most 62443-4-1 requirements	Supplier holds SDLA certification. No difference from CSA.	Section 7	ICSA-300 Requirement ISASecure_IC.R5
Secure product development lifecycle artifact assessment (SDA)	Artifacts required for most requirements in 62443-4-1 Validation activities described in SDLA-312	All CSA SDA-C criteria, EXCEPT that SDLA-SR-4b about intended SL-C for component, instead refers to tier AND additional certification guidance on verifying seven 62443-4-1 requirements, including security context and threat model topics AND documentation and artifacts for five additional lifecycle sub practices	Section 8	ICSA-300 Requirement ISASecure_IC.R5; ISDLA-312

Area of difference	**CSA**	**ICSA (considering both IIoT devices and gateways)**	**Further information in this document**	**ICSA Specification**
Functional security requirements (FSA)	Requirements in 62443-4-2 for selected capability security level (SL-C), applicable to component type(s) of component	Overall: Requirements in 62443-4-2 applicable to component type(s) EXCEPT four, AND up to 24 additional requirements not in 62443-4-2. Each requirement is specified as Core tier or Advanced tier, and as applicable to IIoT device, or IIoT gateway or both. Example: Core tier IIoT device requires: all CSA FSA-C criteria for SL-C=2 EXCEPT two, AND eight SL-C>2 requirements, AND seventeen additional requirements not in 62443-4-2	Section 9	ICSA-311
Certifier assessment of functional security requirements (FSA)	Assessment methods defined in CSA-311, in column labelled "Validation Activity"	Modifications to explicitly address IIoT-specific scenarios or augment CSA-311 methods for assessing selected 62443-4-2 requirements	Section 10	ICSA-311
Vulnerability identification testing (VIT)	Test approach described in SSA-420 Pass criterion depends upon SL-C	Test approach described in SSA-420 Pass criteria for Core tier is same as CSA for SL-C=2 For Advanced tier is same as CSA for SL-C=3.	Section 11	ICSA-300 Requirement ISASecure_IC.R5; SSA-420

Area of difference	CSA	ICSA (considering both IIoT devices and gateways)	Further information in this document	ICSA Specification
Validity of certification after initial evaluation	All updates certified if maintain SDLA certification, maintain product under certified SDL, no new vulnerabilities discovered that preclude an update from meeting certification criteria	All updates certified if meet criteria described for CSA AND maintain good standing under ICSA SMA (Security Maintenance Audit)	Section 12	ICSA-301 Sections 4.2 and 5

5 Products in scope for certification

In summary, all products eligible for ICSA certification are eligible for CSA certification. A subset of the products eligible for CSA certification are eligible for ICSA certification.

A software application, embedded device, host device, or network device can be certified under CSA. These types of components are defined in 62443-4-2; these definitions are also found in the present document in 3.1. If a device meets the definition for more than one of these types of components, the requirements associated with all of its types must be met, in accordance with 62443-4-2 Clause 3.3.

An embedded device, host device, or network device that is also an IIoT device or IIoT gateway can be certified under ICSA. Definitions of these IIoT component types are found in 3.1. In accordance with those definitions, a software-only product is not in scope for ICSA, nor is a device not intended to connect with an untrusted network such as the Internet. Examples of components certifiable under ICSA are:

- *IIoT Devices:*
    - Internet or cellular network connected sensor
    - Device running algorithms to monitor and optimize operations of actuators with which it has a two-way connection, and that sends summary data over the Internet to a cloud application
    - PLC with connection to Internet
- *IIoT Gateways:*
    - Device that collects telemetry data from a number of sensors, converts it to another protocol, and forwards it over the Internet to a cloud application
    - Device that collects operations data from a number of actuators, converts it to another protocol, and forwards it over the Internet to a cloud application.

If a component is both an IIoT Device and an IIoT gateway, ICSA specifies that it will be evaluated against requirements for both component types.

Since an IIoT device or an IIoT gateway eligible for ICSA can be classified as one or more of the component types defined in 62443-4-2, it could also be certified under ISASecure CSA. This would be a separate certification from ICSA. However, CSA and ICSA have most certification criteria in common, so that if both certifications were obtained, there would be significant leverage across these certification efforts. As can be seen from Table 1, an IIoT device certified at the Core Tier would need to demonstrate two additional functional requirements to meet the FSA-C criteria for CSA certification of an embedded device at capability security level 2.

A supplier that wishes to demonstrate to the marketplace their security posture for the IIoT environment, may wish to obtain an ICSA certification. If a supplier's customers require 62443-4-2 compliance, they may wish to obtain CSA certification. [ICSA-301] describes a streamlined process via which a supplier may obtain an ICSA certification for a component that previously was certified under the ISASecure CSA program.

6 Certifications available

CSA certifications may be granted for capability security level 1, 2, 3, or 4. The supplier for a component determines the level desired, which determines the corresponding set of functional security requirements to be applied from 62443-4-2. For ICSA, the supplier for a component determines whether they will apply for certification to the Core tier, or to the Advanced tier.

For FSA certification criteria, ICSA Core Tier is similar to CSA capability security level 2, modified to remove a few 63443-4-2 level 2 requirements, add a few level 3 and 4 requirements, and add IIoT-specific requirements not in 62443-4-2. Advanced Tier is similar to capability security level 4, modified to remove a few level 4 requirements, and to add a larger set of IIoT-specific requirements not required by 62443-4-2. Section 9 enumerates these differences in detail.

Differences between ICSA and CSA for the SDA product lifecycle artifact assessment are the same for Core or Advanced tier, as enumerated in Section 8.

7 Secure product development lifecycle assessment (SDLPA)

For CSA, the criterion for passing SDLPA-C is that the supplier holds an ISASecure SDLA certification where the certified component is in the scope of the certified process going forward. This same criterion must be met for ICSA SDLPA-IC.

8 Secure development artifacts (SDA)

For the CSA certification scheme, documents CSA-312 and SDLA-312 specify validation activities via which the certifier assesses conformance of development process artifacts for the component being evaluated, against 62443-4-1 requirements and the supplier's documented processes. This part of a CSA assessment is called SDA-C (Security Development Artifacts for components). The documents ICSA-312 and ISDLA-312 fulfill this role for ICSA.

All SDA criteria for CSA must be met for ICSA, noting that the SDA validation activity for 62443-4-1 SR-4b about identifying the capability security level for a component, instead refers to ICSA tier, as seen above in Table 1. Artifact assessments as described in Table 2 below are required by ICSA but not by CSA.

The ICSA scheme requires that the additional verifications of lifecycle process artifacts listed in Table 2 be included in certifier validation activity, for both the Core and Advanced tier. Four of these assessments require process documentation not required for SDLA certification, as well as related artifacts. These are SDLA-SD-4-ICSA1, SDLA-SD-4-ICSA-2, SDLA-SUM-2-ICSA, and SDLA-SG-3-ICSA2 (shown in bold in Table 2). Note that the requirement SUM-2-ICSA requires two new sub practices: one about notification regarding available security updates and one about advance notification regarding withdrawal from support for security updates.

The non-bold requirements listed do not require the certifier to review new process documentation, but do require artifacts to demonstrate the items listed for the product under evaluation.

Table 2. ICSA SDA-IC criteria not required by CSA SDA-C
(bold entries require both additional process documentation and artifacts)

IEC 62443-4-1 requirement	ID for SDA-IC validation activity	Additional Validation Activity for ICSA not required by CSA
SR-2 *Threat model*	SDLA-SR-1-ICSA	IIoT aspects included in security context
SR-4 *Product security requirements content*	SDLA-SR-4-ICSA	Security requirements include requirement for ICSA tier
SR-5 *Security requirements review*	SDLA-SR-5-ICSA	Cloud expert included in security requirements review
SR-4 *Secure design best practices*	**SDLA-SD-4-ICSA1**	Supplier has documented secure design practice for compartmentalization*
SR-4 *Secure design best practices*	**SDLA-SD-4-ICSA2**	Supplier has documented secure design practice for topic of failing securely; threat model for component identifies threats from detectable failures.
SR-2 *Threat model*	SDLA-SR-2-ICSA	Threat model for component includes threats due to shared resources internal to component.
DM-1 *Receiving notifications of security-related issues*	SDLA-DM-1-ICSA1	Supplier is tracking sources for security issues for any dependent components including related cloud functionality.
DM-4 *Addressing security related issues*	SDLA-DM-4-ICSA1	Threshold for residual security issues is same as CSA capability security level 2 for Core tier, and CSA capability security level 3 for Advanced tier.
SUM-2 *Security update documentation*	**SDLA-SUM-2-ICSA**	Component is in scope of documented processes for both proactive notification of available updates, and timely notification of withdrawal from support.
SG-3 *Security hardening guidelines*	SDLA-SG-3-ICSA1	User documentation describes physical elements of component that are shared between functions of component (functions delivered, or supported for user addition).
SG-3 *Security hardening guidelines*	**SDLA-SG-3-ICSA2**	Supplier has documented process for documenting cloud dependencies, including ongoing network communication of component with supplier. This documentation exists for component.

*Under FSA-IC requirement FSA-ICSA-12 found in ICSA-311, the certifier verifies this practice has been followed for the IIoT component under assessment.

9 Functional security requirements (FSA)

Regarding FSA, two topics are separately addressed in this section and the following section:

- What differences are there in the list of functional security requirements that must be met for ICSA certification as compared to CSA? (this section)

- What differences are there in how the certifier will verify conformance to those functional security requirements that are required under both certification schemes? (Section 10)

Table 3 describes FSA criteria for ICSA, for Core tier IIoT device and for Core tier IIoT gateway certification, as differences from the FSA criteria for a CSA capability security level 2 certification. The FSA criteria for a CSA capability security level 2 certification are to meet all 62443-4-2 capability security level 2 requirements applicable to the component types of the component. It is assumed that an IIoT device would have been evaluated as an embedded device under CSA, and might be evaluated in addition as a host device and/or software application. It is assumed that an IIoT gateway would have been evaluated as a network device under CSA, and might be evaluated in addition as a host device and/or software application.

The first column of Table 3 shows differences from CSA that are common to ICSA certification of either an IIoT device or an IIoT gateway. The next two columns show any additional difference unique to certification of an ICSA IIoT device or IIoT gateway.

As shown in Table 3, ICSA Core tier requires conformance to all existing 62443-4-2 capability security level 2 requirements with one exception for IIoT gateways, and two for IIoT devices, and adds a few requirements from capability security levels 3 and 4. The capability security level of these added requirements is shown in parentheses after those requirements.

In addition to these existing 62443-4-2 requirements, Core tier requires additional technical security requirements as listed.

Table 3. ICSA FSA-IC Core Tier certification criteria, differences from CSA FSA-C SL-C=2

Core – Common to IIoT Device and IIoT Gateway References for this table: ICSA-300 v1.1 Requirement ISASecure_IC.R5; ICSA-311 v2.3	**Core IIoT Device Only** **(embedded device, may also be host device and/or software application)**	**Core IIoT Gateway Only** **(network device, may also be host device and/or software application)**
62443-4-2 capability security level 2 requirements, applicable to component types of the component EXCEPT CR 7.3 RE (1) *Backup integrity verification**	Additional exception: CR 2.1 RE(2) *Permission mapping to roles*	---
AND 62443-4-2 capability security level 3 and 4 requirements: • CR 1.2 RE(1) *Unique identification and authentication* (3) • CR 2.7 *Concurrent session control* (3) • CR 2.9 RE(1) *Warn when audit record storage capacity threshold reached* (3) • CR 2.12 RE(1) *Non-repudiation for all users* (4) • CR 4.2 RE(1) *Erase of shared memory resources* (3)	AND additional 62443-4-2 capability security level 3 and 4 requirements: • EDR 2.13 RE(1) *Active Monitoring* (3) • HDR 2.13 RE(1) *Active Monitoring* (3) (if host device)	AND additional 62443-4-2 capability security level 3 and 4 requirements: • NDR 2.13 RE(1) *Active Monitoring* (3) • HDR 2.13 RE(1) *Active Monitoring* (3) (if host device) • NDR 5.2 RE(2) *Island mode* (3)

Core – Common to IIoT Device and IIoT Gateway References for this table: ICSA-300 v1.1 Requirement ISASecure_IC.R5; ICSA-311 v2.3	**Core IIoT Device Only** **(embedded device, may also be host device and/or software application)**	**Core IIoT Gateway Only** **(network device, may also be host device and/or software application)**
• CR 6.1 RE(1) *Programmatic access to audit logs* (3) • CR 7.6 RE(1) *Machine-readable reporting of current security settings* (3)		
AND additional ICSA specific requirements to those required by CSA: • FSA-ICSA-1 Default secure configuration • FSA-ICSA-2 Unique initial passwords and keys • FSA-ICSA-3 Integrity of software and data in use • FSA-ICSA-4 Confidentiality for software and data in use • FSA-ICSA-5 Remote update and upgrade • FSA-ICSA-6 Control of update and upgrade • FSA-ICSA-7 Update/upgrade maintains user security settings • FSA-ICSA-9 Authentication of non-human users from untrusted networks • FSA-ICSA-10 Protection from untrusted management traffic • FSA-ICSA-11 Block connection with untrusted network • FSA-ICSA-18 Low battery power	---	AND additional ICSA requirements to those required by CSA: • FSA-ICSA-8 Integrity of runtime data**
AND functional compartmentalization requirements: • FSA-ICSA-12 Component application partitioning • FSA-ICSA-13 Zones at trust boundaries • FSA-ICSA-14 Safety zones • FSA-ICSA-15 Enterprise zones • FSA-ICSA-16 Zone separation methods • FSA-ICSA-17 Physical separation of safety functions	---	---

* However, CR 7.3 RE (1) *Backup integrity verification* is conditionally required by ICSA Core tier for both IIoT devices and IIoT gateways. In particular backup integrity verification is required if the component supports restoration of backup over an untrusted network. See requirement FSA-CR 7.3 RE(1) (PART) in ICSA-311.

** FSA-ICSA-8 Integrity of runtime data is not shown as an addition for IIoT devices because it is already required for embedded devices under CSA to meet 62443-4-2 requirement FSA-EDR 3.14 for SL-C=1.

Table 4 describes FSA criteria for ICSA, for Advanced tier IIoT device and Advanced tier IIoT gateway certification, as differences from the FSA criteria for a CSA capability security level 4 certification. The FSA criteria for a CSA capability security level 4 certification are to meet all 62443-4-2 capability security level 4 requirements applicable to the component types of the component. As shown in Table 4, Advanced Tier requires conformance to all 62443-4-2 capability security level 4 requirements with four exceptions. In addition to these existing 62443-4-2 requirements, Advanced tier requires additional technical security requirements as listed.

There are no effective differences between IIoT devices and gateways in this case, because as noted following Table 3, FSA-ICSA-8 is already met for level 1 embedded devices under 62443-4-2 requirement FSA-EDR 3.14.

Table 4. ICSA FSA-IC Advanced Tier certification criteria, differences from CSA FSA-C SL-C=4

Advanced – Common to IIoT Device and IIoT Gateway References for this table: ICSA-300 v1.1 Requirement ISASecure_IC.R5; ICSA-311 v2.3	**Core IIoT Device Only** **(embedded device, may also be host device and/or software application)**	**Core IIoT Gateway Only** **(network device, may also be host device and/or software application)**
62443-4-2 capability security level 4 requirements, applicable to component type(s) of component EXCEPT • CR 1.7 RE(1) *Password generation and lifetime restrictions for human users* • CR 2.1 RE(3) *Supervisor override* • CR 2.1 RE(4) *Dual approval* • CR 3.9 RE(1) *Audit records on write-once media*	---	---

Advanced – Common to IIoT Device and IIoT Gateway References for this table: ICSA-300 v1.1 Requirement ISASecure_IC.R5; ICSA-311 v2.3	**Core IIoT Device Only** **(embedded device, may also be host device and/or software application)**	**Core IIoT Gateway Only** **(network device, may also be host device and/or software application)**
AND additional ICSA specific requirements to those required by CSA: • Core tier ICSA specific requirements that are common to IIoT device and IIoT gateway, shown in Table 3 • FSA-ICSA-19 Component enforcement of security status of connecting portable and mobile device • FSA-ICSA-22 Limit component self-documentation • FSA-ICSA-23 Presence of component can be monitored	---	AND additional ICSA requirements to those required by CSA: • FSA-ICSA-8 Integrity of runtime data**
AND functional compartmentalization requirements: • Core tier additional functional compartmentalization requirements that are common to IIoT device and IIoT gateway, shown in Table 3 • FSA-ICSA-20 Hardware compartmentalization of security functions • FSA-ICSA-21 Independence from non-control system functions • FSA-ICSA-24 Hardware based protection of software and data in use	---	---

** See note after Table 3.

10 Certifier assessment of functional security requirements (FSA)

10.1 Types of enhancements to FSA validation activities

For the CSA certification scheme, the document CSA-311 specifies certifier validation activities for assessing conformance to 62443-4-2 requirements. Selected validation activities in CSA for 62443-4-2 requirements have been enhanced for ICSA to specifically address the IIoT environment, within the requirement scope already intended by 62443-4-2. Enhancements are of the following types:

- **Include IIoT scenarios:** Verification of conformance to the requirement will include consideration of specified IIoT scenarios to which the requirement applies.

- **Verify by testing:** Verification of conformance to the requirement will include certifier review of the supplier's test artifacts for the requirement, or the certifier performing tests directly.
- **Refer to commonly accepted practices for IIoT:** Verification of conformance to the requirement will include verifying that the approach taken to conform to that requirement conforms to commonly accepted practices for IIoT.

10.2 Examples of enhanced validation activities for 62443-4-2 requirements

This section provides examples of enhancements to validation activities for 62443-4-2 requirements, for each of the types of enhancements described in 10.1. All such enhancements are listed in the present document in Section 13 Appendix 1, and are fully specified in ICSA-311.

- Examples for **Include IIoT scenarios**
    - Consider requirement for integrity of the boot process in scenario in which attacker has physical possession of the component (FSA-EDR|HDR|NDR 3.14 *Integrity of the boot process*).
    - Consider DoS events that disable connection to untrusted network (FSA-CR 7.1 *Denial of service protection*).
- Examples for **Verify by testing**
    - Review supplier tests of protections against unauthorized access to diagnostic or test interfaces (FSA-EDR|HDR|NDR 2.13 *Use of physical diagnostic and test interfaces*).
    - Certifier to test any configurable one-way traffic feature (FSA-NDR 5.2 *Zone boundary protection*).
- Examples for **Refer to commonly accepted practices for IIoT**
    - Human user identification and authentication methods conform to commonly accepted practices for IIoT (FSA-CR 1.1 *Human user identification and authentication*).
    - Methods of communication integrity protection conform to commonly accepted practices for IIoT (FSA-CR 3.1 *Communication integrity*).

As guidance for the assessment of whether an approach taken for a component to meet a requirement conforms to commonly accepted practices for IIoT, ISCI has published the informative document ICSA-500 *ISCI IIoT Component Security Assurance – Selected commonly accepted security practices v1.1* [ICSA-500].

11 Vulnerability Identification Testing (VIT)

For CSA, the ISASecure specification SSA-420 [SSA-420] describes the approach for using Nessus™ for Vulnerability Identification Testing (VIT). For CSA capability security level 2, the criteria for passing VIT-C are that all "critical" and "high" issues identified by Nessus are either corrected or the reason for them not being relevant has been documented. For CSA capability security level 3, this is required also for all “medium” issues identified by Nessus. For CSA level 4, this is required for all issues identified.

The approach to using Nessus described in SSA-420 is also used in ICSA for VIT-IC. In some cases, the SSA-420 specification requires determining whether particular capabilities are present in a component, and this determination will affect the scans run for different components. However, the same component certified under either CSA or ICSA would require the same scans under VIT.

The VIT pass criterion for CSA is specified by capability security level, as described above. For ICSA, the pass criterion depends upon certification tier. For Core tier, the pass criterion for VIT-IC is the same as the CSA criterion for SL-C=2. For the Advanced tier, the pass criterion for VIT-IC is the same as the CSA criterion for SL-C=3.

12 Security Maintenance Audit (SMA)

For CSA 1.0.0, a component and its updates (as defined in 3.1.37) maintain their CSA certification as long as (1) the component remains supported under an SDLA certified development process, and (2) no vulnerabilities are found after initial certification that preclude a product update from meeting certification criteria. Security Maintenance Audit (SMA) defines an additional requirement for maintaining ICSA certification, not required under CSA 1.0.0. SMA does not affect initial ICSA certification.

SMA is a periodic surveillance audit of a certified ICSA component, after initial certification. SMA is applicable whether or not a component has undergone modification. Maintaining good standing under SMA is a requirement for maintaining ICSA certification. SMA scheduling options and requirements are specified in ICSA-301. 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 3.1.19) 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).

See ICSA-301 for a full description of SMA, including the option for use of sampling when a supplier has a number of ICSA certified components that require SMA.

13 Appendix 1 – Differences between CSA and ICSA FSA validation activities

All FSA requirements common to CSA and ICSA that have a modified validation activity under ICSA are summarized in Table 5.

The published specification ICSA-311 highlights these areas of change from the corresponding CSA specification, in red font. Editorial changes with no impact on certification activity are also highlighted in red in ICSA-311, but are not shown in Table 5.

Table 5. Enhancements to CSA FSA-C validation activities for ICSA FSA-IC

FSA requirements from IEC 62443-4-2	For ICSA, enhancement to certifier validation activity for CSA References: CSA-311 v2.3 and ICSA-311 v2.3 (CSA level 2 compared to ICSA Core; CS level 4 compared to ICSA Advanced)
FSA-CR 1.1 *Human user identification and authentication*	Untrusted network not relied upon for identification/authentication for essential functions Human user identification and authentication methods conform to commonly accepted practices for IIoT
FSA-CR 1.1 RE(1) *Unique identification and authentication (human users)*	Untrusted network not relied upon for identification/authentication for essential functions Human user identification and authentication methods conform to commonly accepted practices for IIoT
FSA-CR 1.1 RE(2) *Multifactor authentication for all interfaces*	Untrusted network not relied upon for identification/authentication for essential functions
FSA-CR 1.2 RE(1) *Unique identification and authentication (all users)*	Untrusted network not relied upon for identification/authentication for essential functions Non-human user identification and authentication methods conform to commonly accepted practices for IIoT
FSA-CR 1.5D *Authenticator management - protect authenticators*	Review supplier analyses or tests Consider attacks enabled by physical possession of component
FSA-NDR 1.13 *Access via untrusted networks*	Consider access for management purposes
FSA-EDRHDR|NDR 2.13 *Use of physical diagnostic and test interfaces*	Review supplier tests
FSA-CR 3.1 *Communication integrity*	Methods of communication integrity protection conform to commonly accepted practices for IIoT

FSA requirements from IEC 62443-4-2	For ICSA, enhancement to certifier validation activity for CSA References: CSA-311 v2.3 and ICSA-311 v2.3 (CSA level 2 compared to ICSA Core; CS level 4 compared to ICSA Advanced)
FSA-CR 3.1 *Communication integrity* (ADV)	For advanced tier, also consider communication between zones internal to component
FSA-CR 3.1 RE(1) *Communication authenticity*	Consider management communication Methods to verify authenticity conform to commonly accepted practices for IIoT
FSA-CR 3.3 *Security functionality verification*	Methods supported to test security functions cover all functions in ICSA-311
FSA-CR 3.4 *Software and information integrity*	Certifier test Preserve integrity check results locally, if using untrusted network for reporting results Method for integrity check conforms to commonly accepted practices for IIoT
FSA-CR 3.4 RE(1) *Authenticity of software and information*	Preserve results locally if using untrusted network for reporting results Certifier test
FSA-EDR|HDR|NDR 3.11 *Physical tamper resistance and detection*	Review supplier tests
FSA-EDR|HDR|NDR 3.11 RE(1) *Notification of a tampering attempt*	Review supplier tests (Advanced tier)
FSA-EDR|HDR|NDR 3.12 *Provisioning product supplier roots of trust - protection*	Threats to supplier root of trust mitigated by hardware protections
FSA-EDR|HDR|NDR 3.13B *Provisioning asset owner roots of trust - inside zone*	Consider internal zones Certifier test
FSA-EDR|HDR|NDR 3.14 *Integrity of the boot process*	Consider attacks enabled by physical possession of component
FSA-EDR 3.14 RE(1) *Authenticity of the boot process*	Consider attacks enabled by physical possession of component

FSA requirements from IEC 62443-4-2	For ICSA, enhancement to certifier validation activity for CSA References: CSA-311 v2.3 and ICSA-311 v2.3 (CSA level 2 compared to ICSA Core; CS level 4 compared to ICSA Advanced)
FSA-CR 4.1A *Information confidentiality - at rest*	Protection methods conform to commonly accepted practices for IIoT
FSA-CR 4.1B *Information confidentiality - in transit*	Consider confidential data for which explicit read authorization not configurable Protection methods conform to commonly accepted practices for IIoT
FSA-CR 4.1B *Information confidentiality - in transit* (ADV)	For Advanced tier, Consider confidential data for which explicit read authorization not configurable Protection methods conform to commonly accepted practices for IIoT Consider information in transit between internal zones of component
FSA-NDR 5.2 *Zone boundary protection*	Applies to both IIoT devices and gateways Consider internal zone boundaries Certifier test of any configurable one-way traffic feature
FSA-NDR 5.2 RE(1) *Deny all, permit by exception*	Review of supplier tests Consider ongoing communication of component with supplier
FSA-NDR 5.3 *General purpose, person-to-person communication restrictions*	Review of supplier tests
FSA-CR 6.2 *Continuous monitoring*	Events monitored and reporting interfaces conform to commonly accepted practices for IIoT
FSA-CR 7.1 *Denial of service protection*	Consider DoS events against associated cloud functionality, against connection to untrusted network, and involving low battery power
FSA-CR 7.3 RE(1) (PART) *Backup integrity verification*	For Core tier, required only if component supports restore over untrusted network
FSA-CR 7.4 *Control system recovery and reconstitution*	Consider failed update or upgrade Consider drained battery power