# ISASecure-130

# ISA Security Compliance Institute — ISASecure® certification programs

**Certification process for product families**

Version 1.1

November 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 |
|---|---|---|
| 1.1 | 2023.11.02 | Initial version published to https://www.isasecure.org/ |
| | | |
| | | |

# Contents

## List of tables

## List of figures

## List of requirements

# FOREWORD

This is one of a series of documents that defines ISASecure® certification programs. This document describes the policies and procedures for obtaining certification of a family of closely related products under one certification project and one certificate. The list of all ISASecure certification programs and documents can be found on the web site https://www.isasecure.org/.

# 1 Background and scope

ISCI (ISA Security Compliance Institute) operates the following certification programs:

- ISASecure® CSA (Component Security Assurance), product certification for control system components for conformance to IEC 62443-4-2 and IEC 62443-4-1
- ISASecure ICSA (IIoT Component Security Assurance), product certification for IIoT devices and IIoT gateways, based on IEC 62443-4-2 and IEC 62443-4-1 with exceptions and extensions for the IIoT environment
- ISASecure SSA (System Security Assurance), product certification for off-the-shelf control systems, for conformance to IEC 62443-3-3
- ISASecure SDLA (Security Development Lifecycle Assurance), process certification for an organization's secure product development lifecycle for conformance to IEC 62443-4-1.

In the future other product or process certification programs may be offered.

The present document addresses the scenario in which an organization has developed a set of closely related products and would like to achieve a product certification for all of those products in an efficient manner. Streamlined policies, procedures, and requirements are specified for a supplier to obtain and maintain certification for all members of such a *product family*. Efficiency is achieved initially by organizing the certification of all of the family members as a single certification project, within which conformance evidence and evaluation results may be reused across all or a subset of the product family members. Efficiency is further obtained by tracking certification for the products in the family on a single certificate.

This streamlined process is called *product family certification*. Eligibility of a set of products for the product family certification process is dependent upon the relationship between products in the set, and not upon how the supplier presents the set of products to the marketplace. The process may in some cases cover the entire set of products that a supplier describes to the marketplace as a product family (or in similar terms such product suite, available in several option packages, etc.). In other cases, such a supplier-defined product family might be divided for certification purposes into parts where each part is found eligible for the streamlined certification process. A set of related supplier products that the supplier has not presented as a family to the marketplace, might also be eligible for product family certification. If a set of products is eligible for this process, each product could be individually certified, but product family certification is offered as an option for the supplier.

# 2 Normative references

## 2.1 ISASecure specifications

The specifications that define the existing CSA, ICSA, SSA and SDLA certification programs are listed in:

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

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

[SSA-100] SSA-100 *ISCI System Security Assurance – ISASecure certification scheme,* as specified at https://www.isasecure.org/

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

The most current version of each specification and any published errata are listed in the most currently posted version of the following documents:

[CSA-102] CSA-102 *ISCI Component Security Assurance – Baseline documents and errata for CSA 1.0.0 specifications,* as specified at https://www.isasecure.org/

[ICSA-102] ICSA-102 *ISCI IIoT Component Security Assurance – Baseline documents and errata for ICSA 1.0.0 specifications,* as specified at https://www.isasecure.org/

[SSA-102] SSA-102 *ISCI System Security Assurance – Baseline documents and errata for SSA 4.0.0 specifications,* as specified at https://www.isasecure.org/

[SDLA-102] SDLA-102 *ISCI Security Development Lifecycle Assurance – Baseline documents and errata for SDLA 3.0.0 specifications,* as specified at https://www.isasecure.org/

Likewise, the documentation for all ISASecure certifications will include a 100-series document that provides a program overview and lists all specifications that define that certification program, as well as a 102-series document that identifies the most current versions of those specifications for a specific version of the overall certification program.

Following are additional specifications for the CSA, ICSA, SSA and SDLA certification programs that are specifically referenced in the present document.

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

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

[SSA-204] SSA-204 *ISCI System Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at https://www.isasecure.org/

[CSA-300] CSA-300 *ISCI Component Security Assurance – ISASecure certification requirements*, as specified at https://www.isasecure.org/

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

[SSA-300] SSA-300 *ISCI System Security Assurance – ISASecure certification requirements*, as specified at https://www.isasecure.org/

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

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

[SSA-301] SSA-301 *ISCI System Security Assurance – Maintenance of ISASecure certification,* as specified at https://www.isasecure.org/

[CSA-303] *ISASecure CSA Sample Report*, available on request to ISCI

[ICSA-303] *ISASecure ICSA Sample Report*, available on request to ISCI

[SSA-303] *ISASecure SSA Sample Report*, available on request to ISCI

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

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

[SSA-311] *ISCI System Security Assurance – Functional security assessment for systems,* as specified at https://www.ISASecure.org

[SDLA-312] SDLA-312 *ISCI Security Development Lifecycle Assurance – Security Development Lifecycle Assessment*, as specified at https://www.isasecure.org/

[ISDLA-312] ISDLA-312 *ISCI Security Development Lifecycle Assurance – Security Development Lifecycle Assessment for ICSA*, as specified at https://www.isasecure.org/

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

### 2.2 International standards

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

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

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

[ANSI/ISA-62443-4-1] ANSI/ISA-62443-4-1-2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[IEC 62443-4-1] IEC 62443-4-1:2018 *Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements*

[ANSI/ISA-62443-4-2] ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

[IEC 62443-4-2] IEC 62443-4-2:2019 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

## 3 Definitions and abbreviations

### 3.1 Definitions

**3.1.1**
**capability security level**
security level that a component or system can provide when properly configured and integrated

NOTE This type of security level states that a particular component or system is capable of meeting a target security level natively without additional compensating countermeasures when properly configured and integrated.

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

**3.1.2**
**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.

[SOURCE ANSI glossary]

**3.1.3**
**certification body**
an organization that performs certification

**3.1.4**
**certifier**
certification body carrying out a particular certification project

**3.1.5**
**certifier direct testing**
certifier testing for conformance to a requirement where the certifier directs the execution of product functions and observes behavior of the product itself

NOTE The term certifier direct testing is used here to distinguish it from the term “testing” which is more broadly defined by ISO/IEC as “determination of one or more characteristics of an object of conformity assessment, according to a procedure.”

**3.1.6**
**common security functionality**
relative to a given set of products, any security functionality found in two or more member products

**3.1.7**
**control system**
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

[SOURCE IEC 62443-4-2, note from [SSA-100]]

**3.1.8**
**cosmetic difference**
difference in appearance with no difference in functionality

**3.1.9**
**document about product**
document that presents facts or assumptions about a product itself and/or its environment

NOTE 1 Some but not all of the supplier documents about a product that may be used as evidence for ISASecure product certification are required for conformance to IEC 62443-4-1.

NOTE 2 Examples of documents required by IEC 62443-4-1 are security requirements, threat model, security context, design document, security guidelines for users. Examples not required by IEC 62443-4-1, but that may be used to support an ISASecure product certification are a list of error messages returned to non-administrative users (for verification of IEC 62443-4-2 requirement CR 3.7 *Error handling*), a list of all information at rest or in transit for which read authorization is supported (for verification of IEC 62443-4-2 requirement CR 4.1A *Information confidentiality*).

**3.1.10**
**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]

**3.1.11**
**functional security assessment**
assessment of a defined list of security features for a control system, embedded device, or other control system component

[SOURCE CSA-100]

**3.1.12**
**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]

**3.1.13**
**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

NOTE The assembly or product might be regarded as a component by a customer.

[SOURCE IEC 62443-4-2]

**3.1.14**
**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]

**3.1.15**
**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 ICSA program, 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 3.1.17).

[SOURCE ICSA-100]

**3.1.16**
**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 to define the scope of the ICSA certification.

NOTE 2 From IIC Reference Architecture: “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 3.1.19).

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

[SOURCE ICSA-100]

**3.1.17**
**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 IEC 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).

[SOURCE ICSA-100]

### 3.1.18
**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 from ICSA-100)]

### 3.1.19
**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]

### 3.1.20
**process evidence**

evidence that indicates whether a particular process was performed, and/or allows verification of whether or not the process met specific auditable requirements

NOTE Examples of process evidence are code review minutes to verify IEC 62443-4-1 requirement SI-1 *Security implementation review* and supplier documentation of the component design and manufacturing process to verify IEC 62443-4-2 requirement EDR 3.12 *Provisioning product supplier roots of trust*.

### 3.1.21
**product family**

set of products from the same supplier that meet criteria for similarity so as to be eligible for the ISASecure product family certification process

### 3.1.22
**product family certification process**

for ISASecure, a process via which a set of products from a single supplier that meet specified criteria for similarity can all be certified under a single certification project and tracked on a single certificate

### 3.1.23
**security context**

security provided to the product by the environment (asset owner deployment) in which the product is intended to be used

NOTE The security provided to the product by its intended environment can effectively restrict the threats that are applicable to the product.

[SOURCE: IEC 62443-4-1]

### 3.1.24
**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]

**3.1.25**
**supplier direct testing**
verification of a requirement as part of a supplier’s security development lifecycle process, where the supplier directs the execution of product functions and observes behavior of the product itself

**3.1.26**
**supplier verification plans and results other than direct testing**
outputs from a supplier’s security development lifecycle process where the supplier performs verification of a product requirement based on activities other than direct testing

NOTE Examples are usage analysis to determine audit storage to verify IEC 62443-4-2 CR 2.9 *Audit storage capacity* or a design analysis to investigate possible attacks on the boot process to verify IEC 62443-4-2 EDR 3.14 *Integrity of the boot process.*

**3.1.27**
**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.

[SOURCE ICSA-100]

**3.1.28**
**update**
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

[SOURCE IEC 62443-4-2]

**3.1.29**
**upgrade**
incremental hardware or software change in order to add new features

[SOURCE IEC 62443-4-2]

## 3.2 Abbreviations

The following abbreviations are used in this document.

| | |
|---|---|
| AC | alternating current |
| ANSI | American National Standards Institute |
| ASCI | Automation Standards Compliance Institute |
| CR | component requirement |
| CSA | Component Security Assurance |
| DC | direct current |
| DFD | data flow diagram |
| DCS | distributed control system |
| DM | defect management |

| | |
|---|---|
| EDR | embedded device requirement |
| FSA | functional security assessment |
| HDR | host device requirement |
| hw | hardware |
| IACS | industrial automation and control system(s) |
| ICSA | IIoT Component Security Assurance |
| IEC | International Electrotechnical Commission |
| IIoT | Industrial Internet of Things |
| I/O | input/output |
| IoT | Internet of Things |
| IP | Internet Protocol |
| ISA | International Society of Automation |
| ISCI | ISA Security Compliance Institute |
| ISO | International Organization for Standardization |
| NDR | network device requirement |
| OS | operating system |
| PKI | public key infrastructure |
| PLC | programmable logic controller |
| SD | secure by design |
| SDA | security development artifacts |
| SDL | security development lifecycle |
| SDLA | Security Development Lifecycle Assurance |
| SDLPA | Security development lifecycle process assessment |
| SG | security guidelines |
| SI | Secure Implementation |
| SIEM | security information and event management |
| SIS | safety instrumented system |
| SL-C | capability security level |
| SM | security management |
| SR | security requirements |
| SSA | System Security Assurance |
| SVV | Security Verification and Validation Testing |
| sw | software |
| VIT | vulnerability identification testing |

## 4 Overview of the certification process for product families

This section provides an informal overview of the ISASecure certification process for product families. Section 5 provides the formal description of this process, in a series of numbered requirements.

## 4.1 High level description

The ISASecure certification process for product families allows a set of products to be evaluated in a unified manner as a single certification project, where there are specified procedures for reusing evidence of conformance across the product family members. The supplier provides input to the certifier to assist in identifying areas of reuse. The certification for all of the family members is tracked on a single certificate. These procedures lower the certification effort and cost from that required to certify each family member individually.

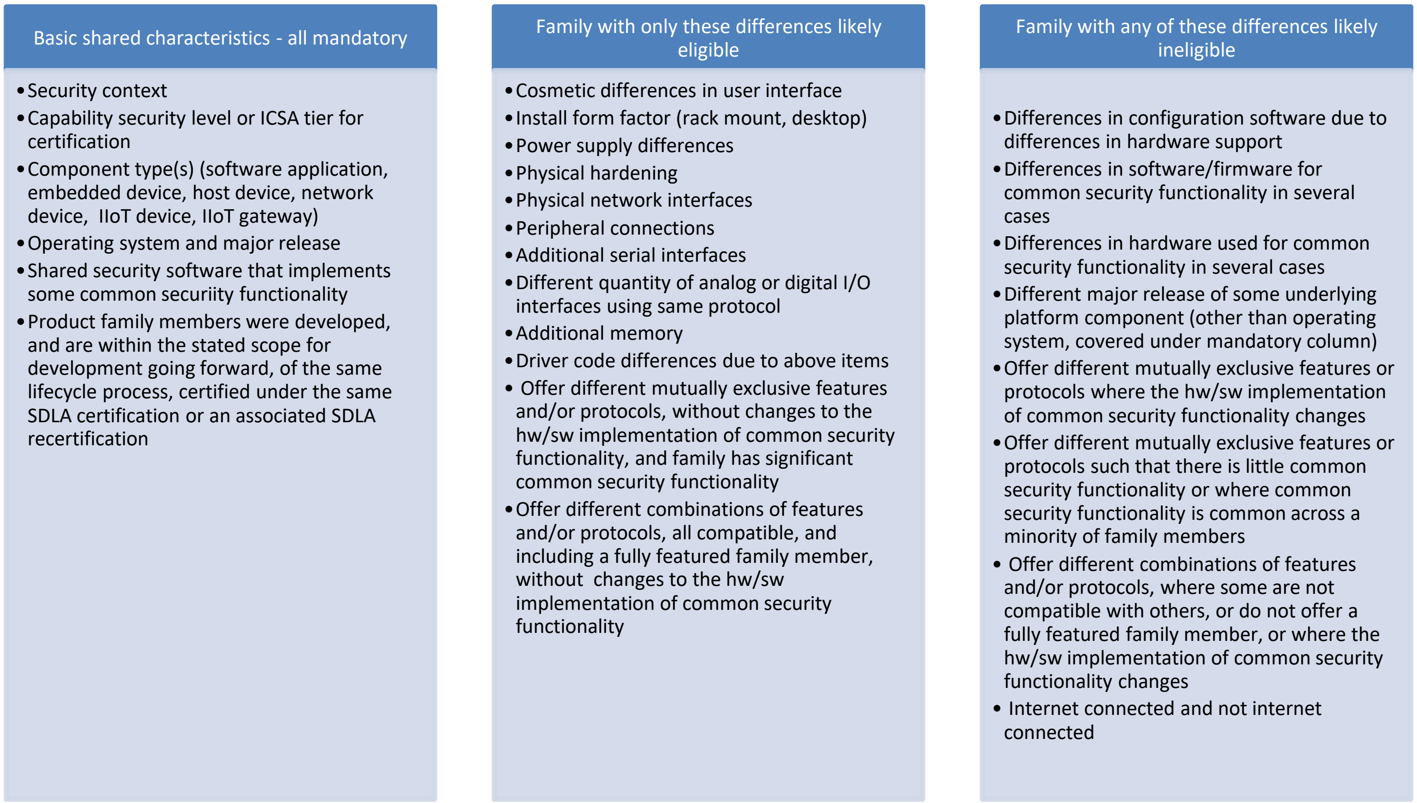
## 4.2 Eligibility

### 4.2.1 Criteria for eligibility

Eligibility of a set of products for the product family certification process depends upon the degree of similarity between individual products in the set, the nature of their differences, and the degree of reuse of certification evidence that is possible across members of the product family. This specification defines (1) mandatory shared characteristics that must be the same among all family members (2) types of differences that are likely to be permitted among members of a product family, and (3) types of differences that are likely to not be permitted within a product family. These factors are illustrated in Figure 1.

The term *common security functionality* as used in Figure 1 and elsewhere in this specification, is defined in Section 3.1.6.

A special case of the last two “likely eligible” scenarios in Figure 1 that state “without changes to the hardware/software implementation of common security functionality,” is a case in which all family members are delivered with the same software and firmware. A factory or installation configuration creates the various family member products, and the configuration process does not impact which code is executed for common security functionality.



Basic shared characteristics - all mandatory

- Security context
- Capability security level or ICSA tier for certification
- Component type(s) (software application, embedded device, host device, network device, IIoT device, IIoT gateway)
- Operating system and major release
- Shared security software that implements some common securiity functionality
- Product family members were developed, and are within the stated scope for development going forward, of the same lifecycle process, certified under the same SDLA certification or an associated SDLA recertification

Family with only these differences likely eligible

- Cosmetic differences in user interface
- Install form factor (rack mount, desktop)
- Power supply differences
- Physical hardening
- Physical network interfaces
- Peripheral connections
- Additional serial interfaces
- Different quantity of analog or digital I/O interfaces using same protocol
- Additional memory
- Driver code differences due to above items
- Offer different mutually exclusive features and/or protocols, without changes to the hw/sw implementation of common security functionality, and family has significant common security functionality
- Offer different combinations of features and/or protocols, all compatible, and including a fully featured family member, without changes to the hw/sw implementation of common security functionality

Family with any of these differences likely ineligible

- Differences in configuration software due to differences in hardware support
- Differences in software/firmware for common security functionality in several cases
- Differences in hardware used for common security functionality in several cases
- Different major release of some underlying platform component (other than operating system, covered under mandatory column)
- Offer different mutually exclusive features or protocols where the hw/sw implementation of common security functionality changes
- Offer different mutually exclusive features or protocols such that there is little common security functionality or where common security functionality is common across a minority of family members
- Offer different combinations of features and/or protocols, where some are not compatible with others, or do not offer a fully featured family member, or where the hw/sw implementation of common security functionality changes
- Internet connected and not internet connected

**Figure 1. Product family similarities and differences**

The term “likely” is applied here because although the differences described in the center column in Figure 1 most commonly would not affect eligibility for the product family certification process, there may be cases where architectural changes accompany a difference of one of these types. In this case the certifier may judge that evidence reuse will not be sufficient to carry out the streamlined process. Likewise, although the differences in the right column of Figure 1 will normally indicate the streamlined process will not be effective, there may be other information to be considered. For example, the differences in software/firmware may be judged isolated and minor. Ultimately, eligibility will be based upon the above guidelines together with certifier judgement about the expected impact on certification evidence of these differences, and any others, across members of a proposed product family.

The Annex Section 6 provides examples of the use of these criteria to evaluate eligibility for a set of products presented as a candidate for product family certification.

### 4.2.2 Process for determining eligibility

With input from the supplier, the certifier evaluates at a high level, each type of evidence to be used to support the certification, and the rationale that the evidence, or large portions of that evidence, could apply across several or possibly all prospective product family members. Types of evidence include but are not limited to direct testing by the certifier, documents about the product including design and user documentation, process evidence, and supplier plans for and results from direct testing by the supplier.

If the applicability of evidence to more than one family member is clearly articulated and justified by the supplier, and product differences are in the ”likely eligible” category, this will give the greatest chance for a set of products to be judged eligible for the product family certification process.

### 4.2.3 Benefits

Product family certification streamlines the certification process by providing a specific procedure for reusing evidence of conformance across product family members, rather than requiring repetition of conformance analysis for each family member. Procedures for reuse of each type of evidence are summarized in the following paragraphs and detailed in the formal requirements in the present document.

Some certifier tests (possibly many) for compliance with functional requirements may be performed on a sample of the product family, and serve as evidence for the entire family. Vulnerability Identification Testing may be performed on some family members by the supplier, instead of all by the certifier, in accordance with requirement FAM.R5 below in Section 5.3.

Product documentation evidence for some requirements (possibly many) may serve as evidence for the entire product family. To achieve this, the supplier identifies any differences between products in the family reflected in those documents.

Process evidence or supplier analyses that can be shown to have covered several or all family members, need only be reviewed once to cover those members.

If there are supplier test plans and results where the supplier has not individually tested all family members, these may be accepted based upon certifier review of the tests performed, together with the supplier’s rationale for their selection of sample family members for testing.

### 4.2.4 Decision whether to pursue product family certification

If the members of a proposed family of products meet basic criteria including shared development process and security context/requirements shown in the first column of Figure 1, differ only by the “likely eligible” criteria in that figure, and do not differ by any of the “likely ineligible” criteria, then usually a product family certification will be appropriate. However, it will usually be inappropriate if products in the set have architectural differences, or other hardware or software differences that may influence or provide common security functionality. The supplier should take into consideration that product differences may be found in “non-operational” features such as boot, backup, recovery, and data purging. Product family certification may also not be appropriate if members of the prospective product family may be on a different schedule for product upgrades, for which certification would entail a new certificate.

Ideally, a supplier that decides to apply for a product family certification will create development artifacts from the outset to best support the process described in this specification, rather than adjusting them later during that process. This practice will also support an efficient decision by the certifier as to whether the product family process can be effectively applied.

In particular, the specific family members covered by an artifact of the development lifecycle process should be identified either within the content of that artifact, or documented using some other consistent mechanism. For the specific case of user documentation, requirement FAM.R7 below in Section 5.4 requires this scope information be within the documentation content. Sections of evidence documents that apply in common to a product family, and sections that apply uniquely to some individual family members, should be clearly distinguished. If any supplier tests or analyses are not performed on all family members individually, rationale for this approach that addresses relevance to all family members, should be captured and documented.

## 4.3 ISASecure product certification elements

The following summary of criteria for an ISASecure product certification, is provided as background for understanding the certification process for product families.

Each ISASecure product certification has the following four elements, which are fully specified in the 300-series document for that certification program (CSA-300 for CSA, ICSA-300 for ICSA, SSA-300 for SSA):

- Security Development Lifecycle Process Assessment (**SDLPA**) – supplier holds an ISASecure SDLA (Security Development Lifecycle Assurance) certification
- Security Development Artifacts (**SDA**) – artifacts from the specific product development are assessed for conformance with IEC 62443-4-1
- Functional Security Assessment (**FSA**) – product functional capabilities are assessed for conformance to requirements for the certification program (for example, conformance to IEC 62443-4-2 for CSA)
- Vulnerability Identification Testing (**VIT**) – a Nessus vulnerability scan is performed on the product and meets a specified threshold for vulnerabilities found.

## 5 Requirements for product family certification

This section formally defines requirements for eligibility, certification process, and maintenance for a product family certification.

### 5.1 Certification criteria

**Requirement FAM.R1 – Criteria for initial certification of a product family** A certifier SHALL grant an initial certification to a set of related products via one certification report and listed on one certificate if (1) the set of products meets all in the following list of basic criteria for a product family, and (2) the product family passes the SDA, FSA, and VIT elements of the certification evaluation performed in accordance with requirements of this specification.

- Same security context
- Same capability security level or ICSA tier for certification
- Same component type(s) (embedded device, software application, host device, network device, IIoT device, IIoT gateway)
- Same operating system and major release
- Shared security software that implements some common security functionality
- Product family members were developed, and are within the stated scope for development going forward, of the same lifecycle process, certified under the same SDLA certification, or an associated SDLA recertification.

A supplier MAY propose a set of products for a product family certification. A certifier SHALL determine at their discretion whether single products and/or further refined subsets of the proposed product family, must be certified individually or in smaller product families. The certifier SHALL base this decision on (1) whether the identification of differences between products in the family and of the expected impact of these differences on certification evidence can be determined with confidence, and (2) whether this expected impact on certification evidence is limited, such that application of the processes of this document is expected to be more efficient than separately certifying each product family member.

NOTE 1 The bullet items in this requirement are seen in the first column of Figure 1.

NOTE 2 As noted in 4.3, the elements of certification SDLPA, SDA, FSA, and VIT are specified in the 300-series document for each certification program (CSA-300 for CSA, ICSA-300 for ICSA, SSA-300 for SSA).

NOTE 3 The last bullet item of the requirement implies that all product family members meet the SDLPA criterion for ISASecure certification.

NOTE 4 Although eligibility for the certification process for product families is not formally defined by naming the types of permitted and non-permitted differences present between members of a product family, the types of differences listed below in requirement FAM.R3 (illustrated in the second two columns of Figure 1) will influence eligibility, because they will influence the level of reuse possible for certifier direct testing across the family.

## 5.2 Types of evidence

The product family certification process defines both the eligibility of a prospective set of products to be certified as a product family (FAM.R1); and if eligible, the process then used to evaluate the product family. This specification defines the evaluation process by enumerating types of evidence that may be used to demonstrate conformance to product certification requirements, and then specifying in formal program requirements how each of those types of evidence may be used to evaluate a product family.

The types of evidence required to be used in an ISASecure certification are found in text labeled as “Validation Activity” in the 311 series documents (CSA-311, ICSA-311, SSA-311) which specify how to evaluate functional security for a product, and in the 312 documents SDLA-312 and ISDLA-312 which specify how to evaluate the secure development lifecycle for a product. These validation activities identify the types of evidence listed in Table 1. Definitions for these types of evidence can be found in Section 3.1. The table highlights key points about the treatment in the present specification of these types of evidence, and provides the section reference that contains formal requirements for that evidence type. A formal requirement is also included to address treatment of evidence that may not fall under the types listed.

In summary, direct testing performed by the certifier or supplier can be limited to some subset of product family members (possibly to one member), if a rationale is provided that product differences do not impact that particular test. For other kinds of evidence of conformance to functional or process requirements for FSA, SDA, or VIT, sampling of family members is not employed. Instead, artifacts that support the conformance argument must be presented for each family member. Evidence that describes facts or assumptions about a product or its environment may simply declare those family members described. For evidence that documents a lifecycle process, describes an analysis and/or presents a conclusion, the supplier may document and present rationale to the effect that this evidence addresses a subset of the product family, and possibly the entire product family, for the topic covered.

**Table 1. Types of evidence**

| Evidence type | Approach | Section |
|---|---|---|
| Certifier direct testing | Certifier selects family members as samples for testing, considering commonly permitted and not permitted differences between family members, and supplier input regarding the impact of family differences on individual tests. | 5.3 |
| Documents about product | Artifact itself or other evidence identifies those family members covered. Supplier identifies content unique to some family members. | 5.4 |
| Process evidence | Artifact itself or other evidence identifies those family members covered, and rationale in support of that coverage. | 5.5 |
| Supplier verification evidence other than direct testing | As above. | 5.5 |

| Evidence type | Approach | Section |
|---|---|---|
| Supplier direct testing | Test plans/results mention all family members. If all family members are not directly tested, certifier reviews rationale for the supplier's sampling strategy. | 5.6 |
| Hardware visual inspection | At least one direct physical evaluation is performed by the certifier. Certifier can use photographic evidence for other family members. | 5.7 |

### 5.3 Certifier direct testing

Figure 2 illustrates requirements FAM.R2, FAM.R3 and FAM.R4 below, regarding the use of sample testing for a product family certification, when certifier direct testing is used to show conformance with an FSA requirement.

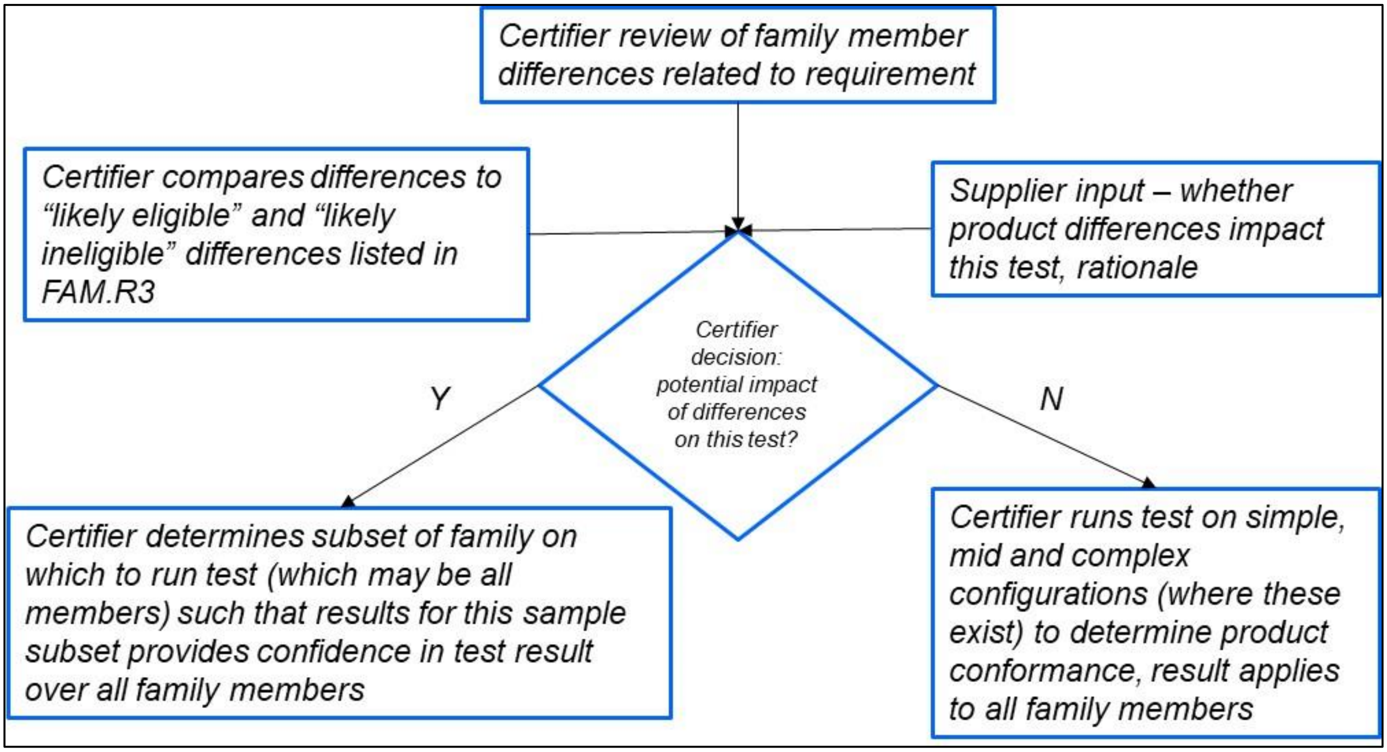

Certifier review of family member differences related to requirement
Certifier compares differences to "likely eligible" and "likely ineligible" differences listed in FAM.R3
Supplier input – whether product differences impact this test, rationale
Certifier decision: potential impact of differences on this test?
Y
N
Certifier determines subset of family on which to run test (which may be all members) such that results for this sample subset provides confidence in test result over all family members
Certifier runs test on simple, mid and complex configurations (where these exist) to determine product conformance, result applies to all family members

**Figure 2. Certifier direct testing of FSA requirement as evidence for product family certification**

<u>**Requirement FAM.R2 – Use of sample testing for certifier direct testing**</u> If security functionality that is unique to one product family member affects conformance to a requirement under the FSA element of certification, then conformance to that requirement SHALL be verified individually for that family member, including direct testing where required by ISASecure specifications. For common security functionality that affects conformance to such a requirement, the certifier SHALL determine whether conformance to be verified by direct certifier testing may be demonstrated on a sample of the members of a product family providing the functionality, where the test results serve as evidence of conformance for all family members. The determination of whether security functionality affects conformance to an FSA requirement and whether sample testing is to be used to verify conformance SHALL be based upon (1) rationale provided by the supplier for

each certifier test for which the supplier states there is no impact of product family differences on the test and (2) certifier review, including review of the factors listed under Requirement FAM.R3. The sample of family members selected for testing by the certifier SHALL be in accordance with Requirement FAM.R4.

NOTE 1 Direct testing is required as evidence for the certification element FSA for those validation activities for requirements (for example in CSA-311, ICSA-311, or SSA-311) which specify "Yes" in the column titled "Validation by Independent Test Required (Yes/No)"). Requirement FAM.R2 also applies if a certifier uses direct testing to verify conformance to certification requirements for which a particular certification method is not specified.

NOTE 2 If a product family includes members with mutually exclusive alternatives for some protocols, the protocol selection will always involve some unique security functionality, and impact some certifier direct tests for FSA. Therefore, in accordance with this requirement, each product with an alternative protocol will be tested in those cases. There may also be found some candidate family members which support only insecure protocols, that must be excluded from the certified product family.  Example requirements in IEC 62443-4-2 for which CSA requires direct certifier test are: CR 1.5B *Authentication management – change default authenticators* and CR 4.1B *Information confidentiality – in transit*.

**Requirement FAM.R3 – Product differences that influence use of sample testing** As part of the process to determine whether sample testing is to be used to verify an FSA requirement for a product family as specified under FAM.R2, the certifier SHALL consider whether product differences within the family are limited to a combination of the factors listed below. If so, this increases confidence in the use of sample testing.

a) Cosmetic differences in user interface

b) Different install form factor (rack mount, desktop)

c) Power supply differences

d) Different physical hardening

e) Different physical network interfaces

f) Different peripheral connections

g) Additional serial interfaces

h) Different quantity of analog or digital I/O interfaces using the same protocol

i) Additional memory

j) Driver code differences due to above items

k) Different family members offer different mutually exclusive features or protocols, without changes to the hw/sw implementation of common security functionality related to this FSA requirement

l) Different family members offer different combinations of features or protocols, all compatible, and including a fully featured family member, without changes to the hw/sw implementation of common security functionality related to this FSA requirement.

The certifier SHALL also consider whether among some family members, some of the following differences have been identified, where the differences might impact this test. If so, this SHALL limit the use of sample testing as described under FAM.R4.

m) Differences in configuration software due to differences in hardware support

n) Differences in software/firmware or hardware implementation for common security functionality related to this FSA requirement, including differences appearing in different family members offering different mutually exclusive features and/or protocols, or in different family members offering different combinations of features and/or protocols

o) Different major release of underlying platform component incorporated in product.

NOTE 3 The items enumerated in this requirement are seen in Figure 1.

NOTE 4 An example situation in which the certifier might exercise their discretion not to allow testing on samples where product differences are limited to a)-l), is if one of these differences comes along with architectural changes to the product.

**Requirement FAM.R4 Selection of sample for testing** If sample testing is used by the certifier, the sample SHALL include at a minimum, a family member with the most interfaces/connections/memory that has all features and protocols offered within the family, a member with the least interfaces/connections/memory that has minimum features and protocols, and a member with intermediate capability between these, where applicable. For any of the differences m)-o) in Requirement FAM.R3, the test SHALL be carried out on at least two members of the product family such that these two members differ from each other in this manner.

**Requirement FAM.R5 – Vulnerability Identification Testing for a product family certification** For all product family members, either the certifier or the supplier SHALL carry out VIT. The certifier SHALL carry out VIT for at least one member of a product family, and MAY do so for more than one at their discretion. If the supplier carries out VIT, the test and reporting process SHALL conform to the same “requirements for supplier-executed VIT” found in ISASecure specifications for maintenance of certification. For CSA, ICSA, and SSA, these are the CSA-301, ICSA-301, and SSA-301 specifications, respectively.

### 5.4 Documents about product

Figure 3 illustrates requirement FAM.R6 below regarding how to efficiently reuse documents about a product to show conformance of a product family with a requirement under SDA or FSA.

Note that this figure (and others following) uses the notation of an “arrow” with a rounded end. This means that along this path, the certification process for product families cannot proceed. Therefore, evidence must be created to allow following the other path offered in the figure. In Figure 3, this means that if a document about the product or products is presented as evidence toward certification, either it or other related evidence must state which family members are covered by the document.

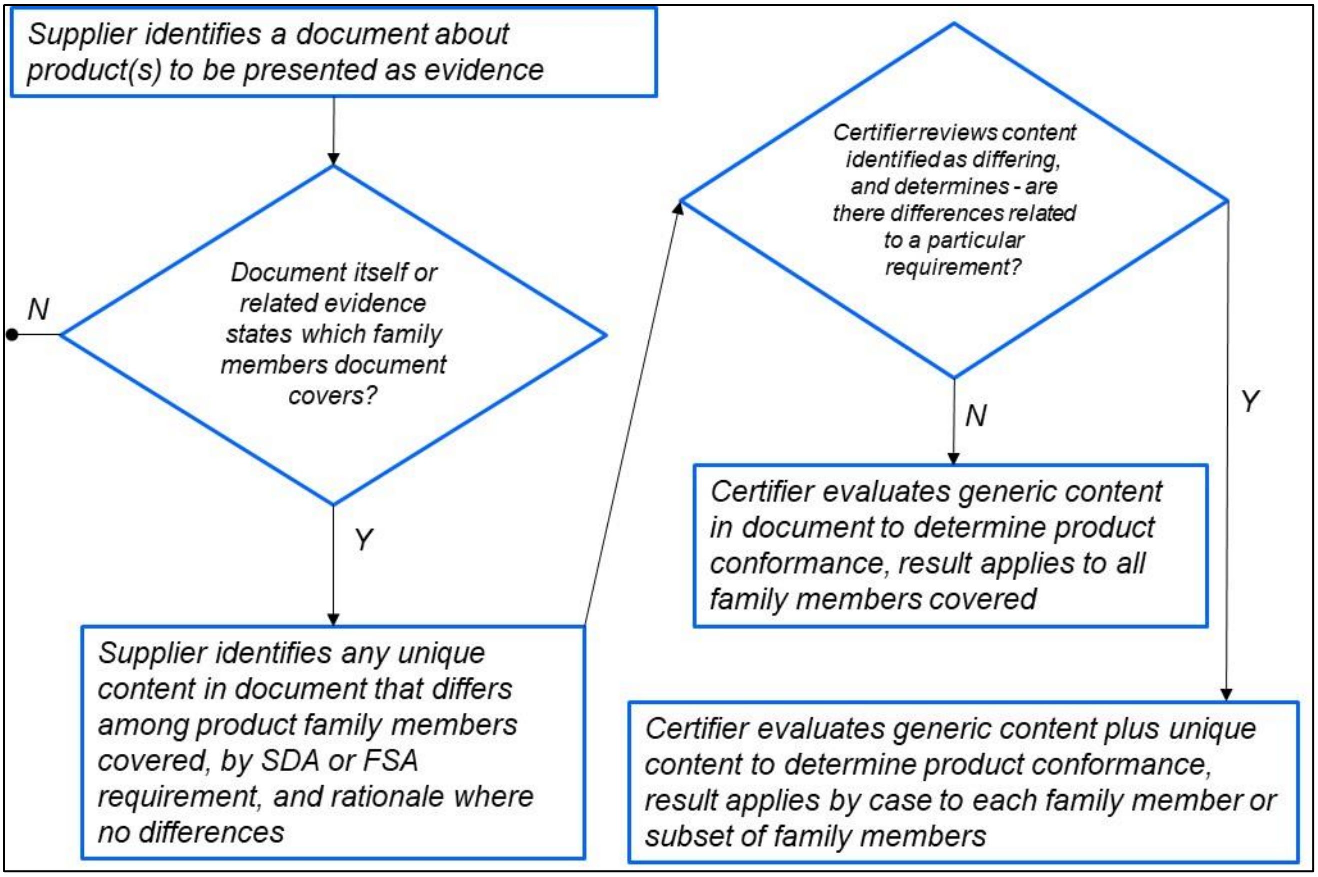

Supplier identifies a document about product(s) to be presented as evidence
Document itself or related evidence states which family members document covers?
N
Y
Supplier identifies any unique content in document that differs among product family members covered, by SDA or FSA requirement, and rationale where no differences
Certifier reviews content identified as differing, and determines - are there differences related to a particular requirement?
N
Y
Certifier evaluates generic content in document to determine product conformance, result applies to all family members covered
Certifier evaluates generic content plus unique content to determine product conformance, result applies by case to each family member or subset of family members

**Figure 3. Document about product as evidence for product family certification**

**Requirement FAM.R6 – Applying documents about product as evidence for a product family certification** This requirement applies in the event that (1) an artifact presented to demonstrate conformance to an SDA or FSA requirement is a document about a product(s) and (2) the document itself, or other related evidence, states that the artifact covers all or some subset of a product family. In this case the supplier SHALL identify for each product family member covered, any content in the artifact document regarding conformance of that family member to the requirement that does not apply for all family members covered by the artifact, and the rationale if no such content is identified. Any content not identified as unique to one or more family members covered, is termed "generic content." The certifier MAY then accept the generic content in the artifact document together with any unique content identified for a family member, as evidence for conformance to the requirement of each family member covered by the artifact.

NOTE 1 Examples of documents about a product are a documented security context, a threat model, a design document, or user security guidelines. Section 3.1 provides a definition for *document about product*.

NOTE 2 Examples of unique content for a member of a product family are: due to added interfaces, additional threats in threat model (IEC 62443-4-1 SR-2i), additional design information (SM-1C, SD-1), DFD (SR-2a), and additional security guidelines (SG-3H).

NOTE 3 This intent of this requirement is to allow the process of verifying a certification requirement across a product family to be more efficient, by incorporating a supplier pre-analysis of documentation evidence.

**Requirement FAM.R7 – Scope of written artifacts for a product family** For any written artifacts used to support a product family certification:

- If an artifact does not identify within its content, those family members to which the artifact applies, the certifier SHALL maintain for its records, separate evidence that identifies those family members covered by the artifact.

- User documentation SHALL include content that identifies those family members to which the documentation applies.

### 5.5 Process evidence and supplier verification evidence other than direct testing

Figure 4 illustrates requirement FAM.R8 below regarding how to efficiently reuse either process evidence, or supplier verification evidence other than direct testing, to show conformance of a product family with a requirement under SDA or FSA.

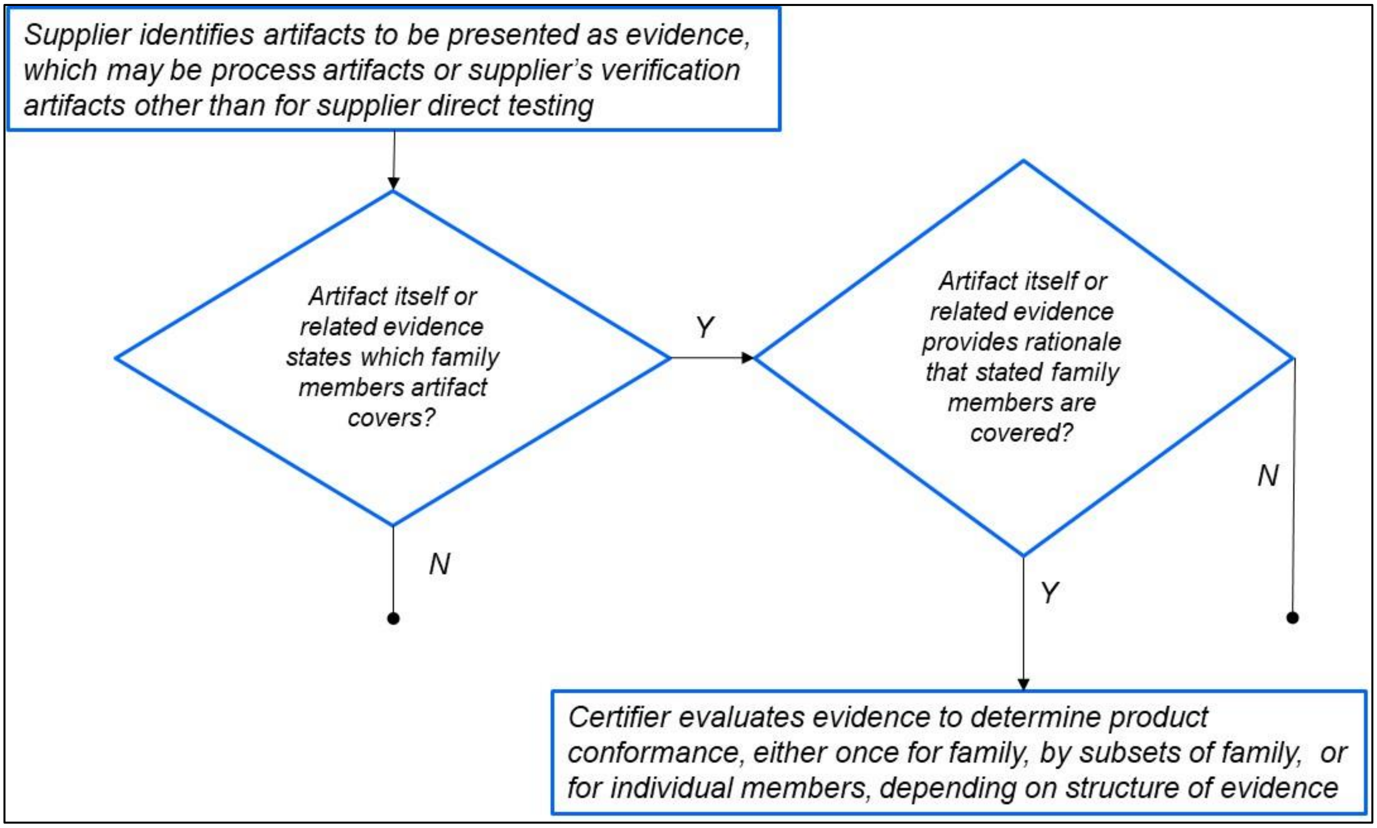

Supplier identifies artifacts to be presented as evidence, which may be process artifacts or supplier's verification artifacts other than for supplier direct testing
Artifact itself or related evidence states which family members artifact covers?
Y
N
Artifact itself or related evidence provides rationale that stated family members are covered?
N
Y
Certifier evaluates evidence to determine product conformance, either once for family, by subsets of family, or for individual members, depending on structure of evidence

**Figure 4. Process evidence or supplier verification evidence other than direct testing for product family certification**

**Requirement FAM.R8 – Applying process evidence or supplier verification evidence other than direct testing for a product family certification** This requirement applies in the event that (1) an artifact presented to demonstrate conformance to a requirement under the SDA or FSA element of an ISASecure product family certification, is either process evidence or supplier verification plans and results, other than for supplier direct testing of the product, and (2) the artifact itself, or other related evidence, states that the artifact covers all or some subset of a product family and provides rationale where needed to demonstrate this coverage. In this case the certifier MAY then accept the artifact as evidence for conformance with the requirement of each product family member covered by the artifact. Otherwise, evidence of conformance SHALL be provided for each individual product family member.

NOTE 1 Section 3.1 provides definitions for these types of evidence. Examples of process evidence (and related requirements) are design review or code review minutes (IEC 62443-4-1 SD-3 and SI-1d). Examples of supplier verification evidence other than direct testing are: traceability analyses (IEC 62443-4-1 SM-1b) and an analysis of sufficiency for storage space provided for audit (IEC 62443-4-2 CR 2.9a).

NOTE 2 The intent of this requirement is that the types of evidence named in the requirement must be present for all product family members; it is not sufficient to sample this evidence over a subset of product family members. For example, code review minutes for one member of a product family would be sufficient to satisfy the code review requirements for all family members, only if other evidence was presented showing that no further code unique to other family members required review under the supplier code review policy.

### 5.6 Supplier direct testing plans and results

Figure 5 illustrates requirement FAM.R9 below regarding how to efficiently reuse supplier test plans and results of direct testing by the supplier, to show conformance of a product family with a requirement under SDA or FSA.

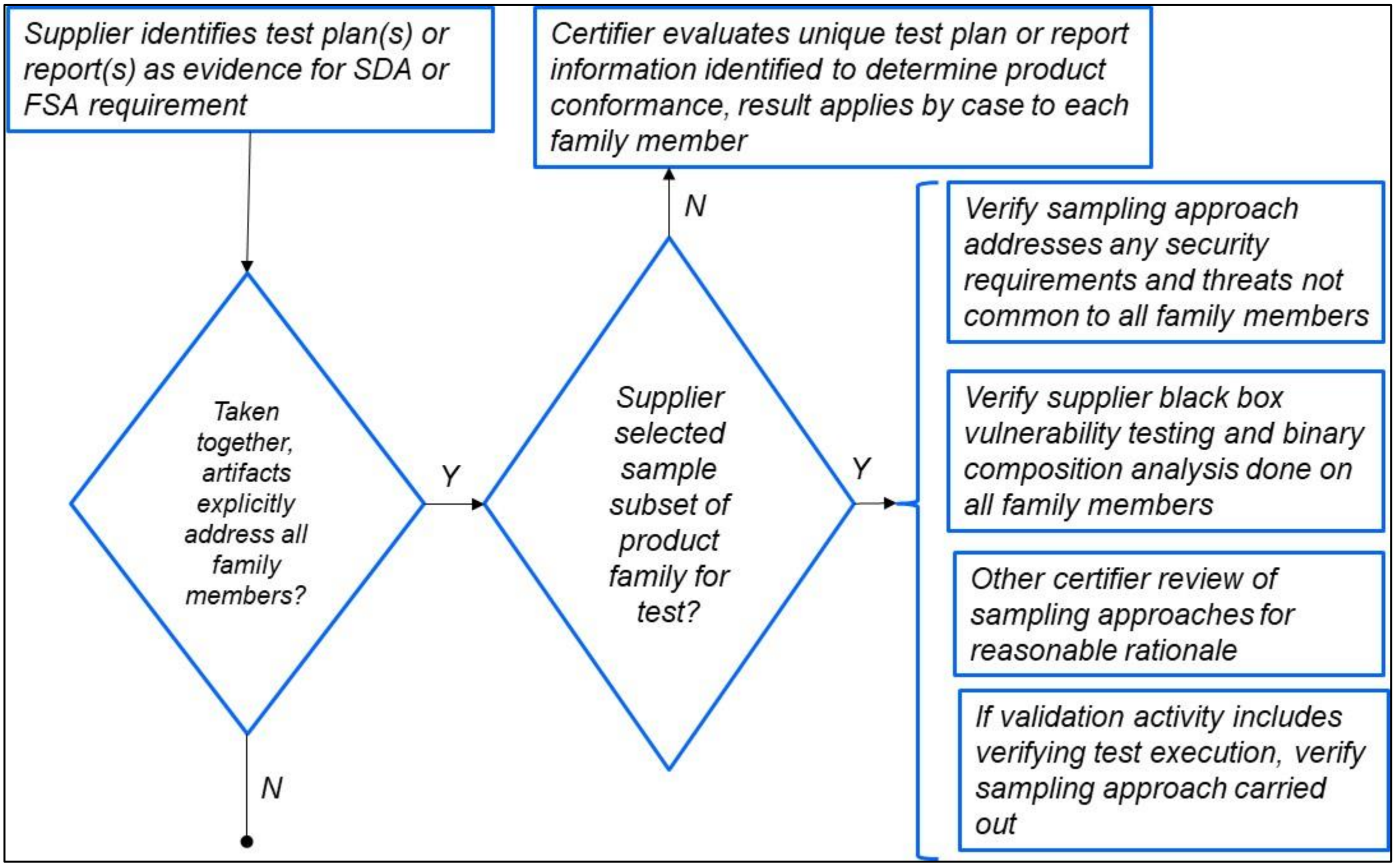

Supplier identifies test plan(s) or report(s) as evidence for SDA or FSA requirement
Taken together, artifacts explicitly address all family members?
N
Y
Supplier selected sample subset of product family for test?
N
Certifier evaluates unique test plan or report information identified to determine product conformance, result applies by case to each family member
Y
Verify sampling approach addresses any security requirements and threats not common to all family members
Verify supplier black box vulnerability testing and binary composition analysis done on all family members
Other certifier review of sampling approaches for reasonable rationale
If validation activity includes verifying test execution, verify sampling approach carried out

**Figure 5. Supplier test plans or reports as evidence for product family certification**

**Requirement FAM.R9 – Applying supplier direct testing as evidence for a product family certification**
This requirement applies in the event that a supplier test plan or results from direct testing are presented to demonstrate conformance to a requirement under the SDA or FSA element of an ISASecure product family certification. The certifier SHALL verify that artifacts from this testing explicitly address coverage of all family members for all areas of testing required by IEC 62443-4-1, whether or not the supplier has employed a sample testing strategy under which not all family members are individually tested. The remainder of this requirement applies when a supplier has employed such sample testing. In this case the certifier SHALL verify the supplier's sampling approach as follows, in addition to reviewing test content as required by other ISASecure validation activities under the SDLA-312 or ISDLA-312 SVV practice. In particular, the certifier SHALL verify that:

- Where a sample testing strategy has been employed, the supplier has documented rationale that supports the strategy.
- Threat mitigation testing and security requirement test plans include tests for all threats and security requirements identified as unique to some family members under requirement FAM.R6.
- Black box vulnerability testing and binary composition analysis are executed by the supplier on all family members.

- For all validation activities in which the certifier is to verify the execution of test plans, the supplier has carried out the plans as written to address all family members to be certified, employing any sampling of family members as the supplier planned.

### 5.7 Hardware visual inspection

**Requirement FAM.R10 – Hardware visual inspection for a product family** If a validation activity as carried out by a certifier for a product family certification incorporates visual examination of product hardware, then one member or a subset of the product family members SHALL be directly examined by the certifier. At the discretion of the certifier, remaining family members MAY be evaluated based upon photographic evidence provided by the supplier.

NOTE Examples of FSA requirements for which ISASecure explicitly specifies visual examination of hardware are IEC 62443-4-2 EDR|HDR|NDR 2.13 *Use of physical diagnostic and test interfaces*. Examples where a certifier is likely to use visual examination of hardware are EDR|HDR|NDR 3.11 *Physical tamper resistance and detection*.

### 5.8 Other evidence types

**Requirement FAM.R11 – Identification of evidence type** The certifier SHALL identify the evidence type or types they have used to verify a requirement when applying this specification. If the type of evidence is uncertain, or not judged to be one of the types listed in Table 1, then the certifier SHALL apply this evidence to evaluate conformance across the product family in a manner consistent with the approaches used in this specification.

NOTE The paragraph preceding Table 1 describes the general approaches used for the evidence types listed in that table.

### 5.9 Other use of sampling

**Requirement FAM.R12 – Selection of data samples for a product family certification** If a validation activity as carried out by a certifier for a product family certification incorporates selection of a sample from a set of supplier data, then the sample SHALL include data associated with all product family members in common and data unique to individual family members or to subsets of the family, where such data exists. This requirement SHALL apply if sampling is used, whether or not ISASecure specifications explicitly specified the use of sampling to verify the requirement.

NOTE Examples of SDA requirements in SDLA-312 for which ISASecure explicitly specifies use of data sampling are SDLA-SM-11 *Assessing and addressing security-related issues* and SDLA-SI-1C-2 *Security implementation review – static code analysis on code changes*.

### 5.10 Certification reports, certificates, modifications to product, family and certification criteria

**Requirement FAM.R13 – Certification report for a product family** Documentation of certification evaluation results for a product family SHALL at a minimum include an assessment report following the content and format of the ISASecure assessment report sample for the certification program. This sample is the specification CSA-303, ICSA-303, and SSA-303 for the CSA, ICSA, and SSA programs, respectively. The certification report for a product family SHALL also include the following information.

- *Product differences:* Product description for all family members, including description of differences among family members, as listed in requirement FAM.R3, and any other differences (e.g., for CSA-303, add to Section 3)

- *FSA differences:* Any differences between product family members, in evaluation results for the Functional Security Assessment. For example, for some requirements, one family member might be evaluated as *Not relevant*, and another member as *Met* (e.g., for CSA-303, add to Section 4)

- *Certifier use of sample testing:* If the certifier elects to use sample testing for some tests as described under requirement FAM.R2, where product differences related to the FSA requirement under test are listed in FAM.R3, then the subset of products tested for each such test SHALL be documented in the certification report. If testing on samples has been performed under requirement FAM.R2, where product differences related to the test are not listed in FAM.R3, in addition the rationale for the selection of samples SHALL be included in the certification report (e.g., for CSA-303, add to Section 4)

- *Fuzz and Network Traffic Load Testing scope differences:* Any differences in scope of these tests carried out by the supplier for different family members (e.g., for CSA-303, add to Section 5.4)

- *VIT for family:* Results from VIT run on all family members (e.g., for CSA-303, add to Section 6)

- *Supplier use of sample testing:* If the supplier used sample testing focused on specific members of the product family, include a high-level description of the nature and rationale for the strategy if used for security requirements testing, threat mitigation testing, vulnerability testing, or penetration testing (e.g., for CSA-303, add to Section 5).

NOTE 1 The format of the information listed in this requirement is not specified here. The evaluator will determine the most useful way to integrate this information in the existing sample report format, depending upon the nature and extent of differences among the product family members.

**Requirement FAM.R14 – Certificate for a product family** A certificate for a product family SHALL contain the same information that would be required under the ISASecure product certification specifications on a certificate for each individual family member. This includes (but is not limited to) product identifier, validity status, and product versions current at the time of SDLA or Security Maintenance Audit (SMA) assessments that take place after initial product family certification.

NOTE 2 For CSA, ICSA, and SSA certifications, certificate content is specified in the documents CSA-204, ICSA-204, and SSA-204 respectively.

**Requirement FAM.R15 – Adding a product family member** The certifier that issued a product family certificate SHALL grant certification to an additional family member and add it to that certificate, under the following conditions: (1) The supplier has requested this addition, (2) the certifier has verified that the additional product meets the same eligibility requirements and certification criteria described in this specification (which were required for products listed on the existing certificate), and (3) the certifier has updated the product family certification report to include the additional family member.

**Requirement FAM.R16 – Certified product as first family member** This requirement applies in the event that a product has been certified, and the supplier would like to obtain a product family certification including that original product together with additional variants. In this case, if the requirements of the present specification are met, a separate product family certificate SHALL be created for these products. The evidence that supported the original certification MAY be used where applicable to meet these requirements.

**Requirement FAM.R17 – Certification of product family upgrades.** The process used by a certifier to determine whether to grant a new family certification for a set of upgrades of products found on a prior product family certificate, SHALL be the same as that required by the ISASecure specifications for granting a new certificate for each upgraded family member, assuming the products in the family had been certified individually and not under a product family certification, with the addition of requirement FAM.R19 regarding pattern vulnerabilities. However, the supplier MAY provide evidence that a product change they have identified as part of the upgrade, and its impact on SDA or FSA evidence that supported the prior certification of the product family, is identical for all or a subset of the product family members. In this case the evaluation of that change and related evidence for an upgrade certification MAY be performed once by the certifier and applied for the upgrades of all of these product family members.

NOTE 3 For CSA, ICSA, and SSA certifications, the process for certifying upgrades of products previously certified, is specified in the documents CSA-301, ICSA-301, and SSA-301 respectively.

NOTE 4 As described in the 301 series ISASecure specifications, the certification process for upgrades first requires that the supplier list high level changes present in an upgraded product, and a mapping from these changes to detailed changes shown in their CM system change log. The supplier then submits an analysis of these changes, for impact on prior evidence of conformance to SDA process requirements, and to FSA functional requirements. In the case of a product family, FAM.R17 implies these analyses are therefore to be done for each family member. However, if there is a product change that impacts evidence of conformance with either of these certification elements for some member of a previously certified product family, it is likely that there is impact to all members of the family, due to the hardware/software used in common among members of the product family. It is also likely that the updated evidence required for certification of the upgrade will also apply to all product family members. The supplier can identify these common cases so that the certifier can examine them once instead of repeating the analysis for each family member. However, there may be exceptions. These may be cases in which a change affected only one or some family members, or where the impact on certification evidence may be different among family members. To address such cases, the certifier must consider each family member individually.

**Requirement FAM.R18 – Certification of product family updates** A product family remains certified as its members undergo updates, under the same conditions as specified for individual certified products.

NOTE 5 These conditions are specified for CSA, ICSA, and SSA in CSA-301, ICSA-301, and SSA-301, respectively.

NOTE 6 The requirement FAM.R19 in this specification provides a verification that similar security updates are applied to all family members that need them.

**Requirement FAM.R19 – Pattern vulnerabilities in a product family** For an upgrade certification for a product family, the certifier SHALL verify that any security issue reported against any member of the product family previously certified under the product family certificate, since the time when that certification was granted, is reported and addressed for all family members, or the supplier has provided rationale for why it does not apply to all members.

NOTE 7 In accordance with IEC 62443-4-1 DM-3, the supplier security development lifecycle is to include the more general requirement "identifying all other products/product versions containing the security-related issue (if any)." The requirement FAM.R19 verification of conformance with this requirement across an upgraded product family is a special case.

In the following requirement, "a certification criterion defined by an ISASecure scheme" refers to capability security level for CSA, tier for ICSA, and capability security level by zone for SSA, as defined under a specific release of a certification program such as CSA 1.0.0. A certification criterion determines the detailed certification criteria to be applied.

**Requirement FAM.R20 – Certification of product families to different ISASecure criteria** If a product family has been certified to a certification criterion defined by an ISASecure scheme, it SHALL be granted a new product family certification to a different certification criterion defined by the same ISASecure scheme, under these conditions:

- each family member meets the conditions for certification to the new criterion as defined in the 301 series specification for the scheme
- validation activities carried out by the certifier to verify conformance to the new certification criterion conform to the requirements of the present specification.

NOTE 8. Once a product has been certified under some certification criterion, a different criterion could be a higher level(s), a higher tier, a certification to an updated version of the ISASecure scheme at the same level(s) or tier, or a combination of these. These scenarios are described in the specifications CSA-301, ICSA-301, SSA-301.

NOTE 9 Briefly, the 301 documents specify that to certify to a higher level or tier, or to an updated ISASecure certification program version, it suffices to carry out a delta evaluation of new or changed requirements and changed validation activities, and to rerun VIT.

## 6 Annex – Examples of candidate product families

The following table provides examples of sets of products that might be presented as candidates for product family certification, to illustrate the eligibility criteria shown in Figure 1.

**Table 2. Example eligibility evaluations for ISASecure product family certification**

| Description of set of products | Disposition | Rationale per Figure 1 criteria |
|---|---|---|
| Product offered with Modbus interface only, or supporting Modbus and BACnet | Could be eligible | Likely eligible criterion: *Offer different combinations of features and/or protocols, all compatible, and including a fully featured family member, without changes to the hw/sw implementation of common security functionality* |
| Product offered with either Modbus interface only, or BACnet interface only, and with varying quantity of interfaces | Could be eligible | Likely eligible criteria: *Offer different mutually exclusive features or protocols, without changes to the hw/sw implementation of common security functionality, and family has significant common security functionality* and *Different quantity of analog or digital I/O interfaces using the same protocol* |
| Product offered with between 1 and 8 serial I/O ports | Could be eligible | Likely eligible criterion: *Additional serial interfaces* |
| IP camera offered with optional zoom and/or tilt modules | Could be eligible | Likely eligible criterion: *Offer different combinations of features and/or protocols, all compatible, and including a fully featured family member, without changes to the hw/sw implementation of common security functionality* |
| Sensor offered with different sensing functions such as temperature, pressure | Could be eligible | Likely eligible criterion: *Offer different mutually exclusive features or protocols, without changes to the hw/sw implementation of common security functionality, and family has significant common security functionality* |
| Product offered with AC or DC power | Could be eligible | Likely eligible criterion: *Power supply differences* |

| Description of set of products | Disposition | Rationale per Figure 1 criteria |
|---|---|---|
| Product to be certified to SL-C=2 offered with additional capability for password generation and lifetime restrictions which is required at SL-C = 3 (IEC 62443-4-2 CR 1.7 RE(1)) | Could be eligible | Likely eligible criterion: *Offer different combinations of features and/or protocols, all compatible, and including a fully featured family member, without changes to the hw/sw implementation of common security functionality.* However in this case, could become ineligible if the changes made to add the capability described, entail changes to authentication itself (likely common security functionality), and are not limited to adding this management functionality |
| Product offered as Internet-connected device and as device without Internet connection | Likely ineligible | Likely ineligible criterion: *Internet connected and not Internet connected*. Also, if *security context* is different, ineligible by that mandatory criterion |
| Product offered with choice of software or hardware security module supporting most security functions | Likely ineligible | Likely ineligible criterion: *Differences in hardware used for common security functionality in several cases* |
| Product offered with an additional quantity of I/O interfaces where for higher quantities, the generally used software security module is replaced by hardware to achieve required performance | Likely ineligible | Likely ineligible criteria: *Differences in hardware used for common security functionality in several cases*, even though products with a different quantity of interfaces could be eligible, if they did not also replace common security functionality |
| Product offered with several different non-security relevant features, and in some cases also a different cryptography module | Likely ineligible | Likely ineligible criterion: *Differences in software/firmware for common security functionality in several cases,* since the cryptography module usually broadly supports security functionality for the product. However, if the two modules have minor differences, and especially if they have no differences in their interfaces, the certifier may consider such product variants eligible for family certification as described by example in 4.2.1 of this document: "For example, the differences in software/firmware may be judged isolated and minor." FAM.R1 also states formally that the certifier will consider in this decision "whether this expected impact on certification evidence is limited." |
| Software application offered using choice of different major releases of containerization platform, at time of purchase | Likely ineligible | Likely ineligible criterion: *Different major release of some underlying platform component (other than operating system…)* |

| Description of set of products | Disposition | Rationale per Figure 1 criteria |
|---|---|---|
| Product models offered with selection of several security features that define product models: e.g., PKI or password authentication, optional SIEM interface | Likely ineligible | Likely ineligible criterion: *Offer different mutually exclusive features or protocols such that there is little common security functionality…* |
| Product offered on real time OS and non-real-time OS | Ineligible | Does not meet mandatory criterion: *Same operating system and major release* |
| Controller offered with and without gateway function | Ineligible | Does not meet mandatory criterion for same *Component type*, since product with gateway function is both embedded device and network device |
| Product acquired from another organization, considered together with a set of related products created by its new owner, with features/interface offerings made more flexible | Ineligible | Original product does not meet mandatory criterion *Product family members were developed and are within the stated scope for development going forward, of the same lifecycle process, certified under the same SDLA certification or an associated SDLA recertification.* Newly created products could be eligible as a family, without the original product. |
| Product offered with security features to obtain level 1 certification, and with added features to obtain level 2 certification | Ineligible | Does not meet mandatory criterion for shared *Capability security level or ICSA tier for certification* |