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

Version 3.2

August 2019

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.0	2010.08.04	Initial version published to http://www.ISASecure.org
2.1	2014.12.11	replace SDSA by SDLA and use SDLPA terminology, incorporate VIT in EDSA, add concept of confidence in evidence impact assessment
2.6	2018.02.05	Align with ANSI/ISA-62443-4-1 and IEC 62443-4-1: SDLA certification no longer has an associated security level, although some SDLPA and SDA-E validations differ by level (changes to clause 1, 4.4 and requirements R3 and R14)
2.8	2018.10.01	Align with ANSI/ISA-62443-4-2: In clause 1, modify discussion of allocation of requirements, remove statement that VIT depends upon FSA-E, and add pointer to ISASecure-116; in body of document, change EDSA-311 to CSA-311; in R15, modify criteria for passing FSA-E line item
3.2	2019.08.03	Title changed from EDSA-301 to CSA-301; clarify definition of term certification level; update for all 4-2 component types; remove certifier CRT; make SDLA prerequisite; incorporate maintenance of certification policy for updates and upgrades introduced in ISASecure-115

Contents

FOREWORD

This is one of a series of documents that defines ISASecure® CSA (Component Security Assurance) certification for software applications, embedded devices, host devices and network devices. These are the component types defined by the standard IEC 62443-4-2 that are used to build control systems. ISASecure CSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of documents related to ISASecure CSA can be found on the ISCI web site http://www.ISASecure.org.

1 Scope

This document specifies the criteria for maintaining ISASecure® CSA (Component Security Assurance) certification for an IACS (Industrial Automation and Control System) component, as the component and the ISASecure CSA criteria evolve over time. 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 [IEC 62443-4-2] and in 3.1 of the present document. This document covers certification situations where:

- a certified component has subsequently been modified; or
- the ISASecure certification criteria have changed; or
- both the component and the certification criteria have changed.

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

In overview, in order to obtain an initial ISASecure CSA certification, a supplier must hold an ISASecure SDLA (Security Development Lifecycle Assurance) development process certification such that the component to be evaluated is in the scope of that process. A supplier may apply for CSA and SDLA certification in parallel.

ISASecure CSA certification of components has three additional elements:

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

Both the SDLA certification evaluation and SDA-C assess development process. SDLA certification demonstrates that the supplier has a documented secure product development lifecycle process, that is compliant with [IEC 62443-4-1], and that there is evidence the process is followed. SDA-C examines the artifacts that are the outputs of the supplier's development processes as they apply specifically to the component to be CSA certified. FSA-C examines the security capabilities of the component, recognizing in accordance with [IEC 62443-4-2] that requirements for security functionality differ by component type. The certifier determines all component types applicable to a product; FSA-C then incorporates requirements for all component types applicable to the product.

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

A CSA certification has an associated certification level, which may be Capability Security Level 1, Capability Security Level 2, Capability Security Level 3, or Capability Security Level 4. The required SDLA certification does not have an associated level. SDA-C and VIT-C are the same for all certification levels with the exception of allowable residual risk for known security issues. FSA-C incorporates more requirements at higher levels, aligned with the requirements assigned to each capability security level in [IEC 62443-4-2].

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

2 Normative references

2.1.1 ISASecure Specifications

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

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

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

[CSA-300] *ISA Security Compliance Institute Component Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

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

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

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

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

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

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

2.1.2 IACS security standards

NOTE 1 [CSA-100] describes the relationship of ISASecure CSA to the ANSI/ISA/IEC 62443 series of standards.

NOTE 2 The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

[ANSI/ISA-62443-1-1] ANSI/ISA-62443-1-1 *(99.01.01)-2007 Security for industrial automation and control systems Part 1-1: Terminology, concepts and models*

[IEC 62443-1-1] IEC TS 62443-1-1:2009 *Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models*

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

.

3.1.1
artifact
tangible output from the application of a specified method that provides evidence of its application

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

3.1.2
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.3
certifier
chartered laboratory, which is an organization that is qualified to certify products or supplier development processes as ISASecure

NOTE This term is used when a simpler term that indicates the role of a “chartered laboratory” is clearer in a particular context.

3.1.4
chartered laboratory
organization chartered by ASCI to evaluate products and/or processes under one or more ISASecure certification programs and to grant certifications under one or more of these programs

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

3.1.5
certification level
capability security level for which conformance is demonstrated by a certification

NOTE 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*.

3.1.6
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

3.1.7
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.

3.1.8
evidence impact assessment
identification of that portion of the evidence from the certification evaluation of a product, which may be applied toward the certification of a modified version of the product, and of those aspects of the evaluation which must be performed on the modified product and new evidence created

3.1.9
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.).

3.1.10
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

3.1.11
initial certification

certification where the ISASecure certification process does not take into account any prior ISASecure certifications of the entity under evaluation or of any prior versions of the entity

3.1.12
ISASecure version

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

3.1.13
network device

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

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

3.1.14
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.

3.1.15
software application

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

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

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

3.1.16
update

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

3.1.17
upgrade

incremental hardware or software change in order to add new features

3.2 Abbreviations

The following abbreviations are used in this document

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CM	component maintenance of certification
CSA	component security assurance
CVE	common vulnerabilities and exposures
FSA-C	functional security assessment for components
HMI	human-machine interface
IACS	industrial automation and control system
ISA	International Society of Automation
IEC	International Electrotechnical Commission
ID	identifier
ISCI	ISA Security Compliance Institute
OS	operating system
PLC	programmable logic controller
SDA-C	security development artifacts for components
SDL	security development lifecycle
SDLA	security development lifecycle assurance
SIS	safety instrumented system
SSA	system security assurance
TS	technical specification
VIT-C	vulnerability identification testing for components

4 Overview

In this section we summarize the approach to maintenance of ISASecure CSA certification as a component and the ISASecure CSA certification requirements evolve over time. The intent of the overall approach is to leverage previous certification results wherever possible to achieve cost effectiveness, while maintaining the integrity of the certification result. Sections 5 - 9 provide formal detailed requirements for various certification maintenance scenarios.

4.1 SDLA certification prerequisite

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

4.2 Modified components

Different approaches are used for certification of component updates (bug fixes) and component upgrades (new component functionality). The terms *update* and *upgrade* are formally defined in [IEC 62443-4-2] and in the present document in 3.1.16 and 3.1.17.

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

4.2.1 Component updates

Certification applies to a specific component version together with its updates. Once a supplier earns a CSA certification, that certificate remains valid for all component updates per the definition in 3.1.16 as long as:

- the component remains in a support status such that an SDLA certified SDL process for security management still applies; and

- the supplier retains their SDLA certification.

Once issued, a CSA certificate is amended to list version numbers for currently supported updates of the component, at the time of each SDLA recertification, which occurs every three years (as required by [CSA-200]). [CSA-204] provides the format for a certificate including these amendments.

4.2.2 Component upgrades

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

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

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

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

Section 6 provides requirements for certification of component upgrades.

4.3 Updated ISASecure criteria

As in the case of component upgrades, a component supplier is not required to revise a component certification for the latest ISASecure version. Hence, for example, a component certified to ISASecure CSA 1.0.0 is not required to obtain a certification to ISASecure CSA 2.0.0. However, all components going through an initial certification or certification of an upgrade after ISASecure CSA 2.0.0 becomes available, will be certified to that ISASecure CSA version in accordance with the ISASecure published transition policy.

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

An upgraded component may be submitted for certification to an ISASecure CSA certification version that also has changed. Consider the case where a component achieved certification under ISASecure CSA 1.0.0, and a component upgrade is submitted for certification to ISASecure CSA 2.0.0. This certification process will be logically equivalent to first certifying the component upgrade to ISASecure CSA 1.0.0 using the approach described in 4.2, and then carrying out the defined evaluation delta between the two certification versions CSA 1.0.0 and CSA 2.0.0 on the upgraded component.

Section 7 provides requirements for certification to modified ISASecure CSA certification criteria. Section 8 provides requirements for certifications when both the component and the certification criteria have changed.

4.4 Certification to a higher level

Once a component has achieved ISASecure CSA certification at a specified certification level, the component supplier may modify the component and/or available process evidence as deemed necessary, and then apply for a higher level certification. As noted in 4.1, the supplier must hold an ISASecure SDLA certification for an SDL process that applies to the component going forward to achieve a CSA certification to a higher level (or any CSA certification). Any component modifications are first assessed to the original certification level following the approaches outlined in 4.2.

The validations for SDA-C evaluation criteria related to residual risk due to known security issues will differ by certification level, as will FSA-C requirements. The certifier will therefore evaluate the SDA-C and FSA-C certification criteria, where different from those at the original level. Finally, the certifier will rerun VIT-C and apply the pass/fail criterion for the new level. Since the prior certificate issued for a lower level may apply to several updates of a component, the supplier will determine which one of these update versions will be used as the first certified version to be listed on the new higher level certificate. That component version will be used for examining the delta certification requirements between the two certification levels.

Section 9 provides requirements for this case.

NOTE In SDLA-312 v5.5, the treatment of residual risk related to known security issues is found in SDLA requirement SDLA-DM-4.

5 Requirements for certification of component updates

This section addresses maintenance of certification for updates of a component, which are defined in 3.1.16.

Requirement ISASecure_CM.R1 – Identification of updates and upgrades

A chartered laboratory SHALL reach agreement with an applicant for CSA certification, on a policy that can be applied based upon examining component version numbers, that determines whether a new version falls under an existing certificate, or would require a new certification. The intent of the policy is that upgrades of a certified component (see 3.1.17) SHALL require a new certification, and updates (see 3.1.16) SHALL NOT.

NOTE A new certificate would be issued when:

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

Requirement ISASecure_CM.R2 – Component update certification and withdrawal

A CSA certification applies to any update of a certified component (as identified under ISASecure_CM.R1), for as long as:

- the supplier of the component maintains an ISASecure SDLA certification; and
- the scope of the SDLA certified process includes the component; and

- the component remains in a support status such that the certified SDL process for security management still applies.

If a supplier does not maintain an SDLA certification with scope that includes a CSA certified component, then after a one year grace period, the CSA certification for that component SHALL be withdrawn. A supplier SHALL inform the certifying chartered lab when a certified component has transitioned to a minimal or no support status, such that the certified SDL process for security management no longer applies. The chartered laboratory SHALL withdraw the certificate upon receiving this notification.

6 Requirements for certification of component upgrades

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

6.1 Criteria for applying prior certification evidence to component upgrade

The following requirements provide the general criteria under which evidence from prior certifications of a component is considered applicable toward earning certification for a component upgrade. Specific requirements on how these criteria are evaluated follow in Section 6.3.

Requirement ISASecure_CM.R3 – SDA-C certification element for component upgrade

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

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

- the certifier carries out this assessment; and

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

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

Requirement ISASecure_CM.R4 – FSA-C certification element for component upgrade

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

- the certifier determines that an evidence impact assessment for the prior FSA-C results for the component can be performed with confidence; and

- the certifier carries out this assessment and shows that component modifications have either not impacted these results, or may have impacted few FSA-C line items in [CSA-311] in a manner isolated from other line items; and

- the certifier has evaluated any potentially impacted FSA-C line items and given them pass status.

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

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

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

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

Requirement ISASecure_EDM.R5 – Deleted

6.2 VIT-C assessment for a component upgrade

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

Requirement ISASecure_ CM.R6 – VIT-C certification element for component upgrade

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

Requirement ISASecure_ CM.R7 – Requirements on supplier-executed VIT-C for component upgrade

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

- supplier personnel responsible for the VIT-C SHALL have successfully completed a training class or 1 year of job experience demonstrating proficiency with the VIT tool to be used;
- the supplier SHALL run the test with a policy file provided by the chartered laboratory;
- the chartered laboratory SHALL witness execution of the VIT-C by the supplier, including starting the test, saving the report file, and signing of the report. This witnessing MAY be achieved remotely.
- the supplier SHALL submit as evidence of VIT-C:
    - documentation of the tested component configuration, that contains the same information the chartered laboratory would record if they performed the test;
    - the policy file used to run the test;
    - the command line that was executed to run the test; and
    - the full report from the VIT tool; and
- the VIT-C evidence submitted to the chartered laboratory SHALL be signed by a responsible representative of the supplier.

6.3 Evidence and assessment for criteria

If based upon the criteria in Section 6.1, a component supplier believes that some of the evidence used to certify a previous version of a component is applicable toward certification of a component upgrade, they may request consideration for this evidence. In this case, their submission of data toward certification of the modified component will include supporting evidence to demonstrate that the criteria stated in the requirements of 6.1 are met. This section specifies the nature of that supporting evidence and how the certifier carries out an evidence impact assessment relative to the evidence from the prior certification evaluation, based upon the suppliers' supporting evidence regarding component changes.

Requirement ISASecure_CM.R8– Submission of component modification data

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

- a high level description of modifications to the component since the prior CSA evaluation of the component (which may have been for an initial certification or a prior upgrade);
- a mapping from the elements of this description to a detailed change log extracted from the change management system for the component software; and
- evidence that this extraction from the change management system constitutes all changes in the modified component; and
- a list of any third party sub components that had new CVE reports against them since the prior certification; whether or not addressed by the time of application for certification; and
- a list of any changes in third-party supplied sub components such as an OS service pack update; and
- a high level summary of any changes to user documentation related to component security.

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

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

- if consideration is requested for prior SDA-C evidence:
    - an analysis of the SDA-C matrix, that for each numbered requirement and SDLA ID, considering the validation activity in the column labeled “Applies for Component or System Certification” in [SDLA-312], either:
        - States that no additional actions beyond those previously carried out to meet this requirement for the prior certification are required to meet this validation requirement for this certification, or
        - Briefly describes additional actions beyond those previously carried out to meet this requirement for the prior certification, which were carried out to meet this validation requirement for this certification.
- if consideration is requested for FSA-C: an analysis of the FSA-C matrix, that notes for each numbered line item in [CSA-311] that applies to the capability security level for the CSA certification, whether there is any change to the functionality or code described by this requirement, among the component modifications since the previous certification. If so, the applicant SHALL provide a mapping to the related code modifications at the CM level of detail (as reported under Requirement ISASecure_CM.R8).

Requirement ISASecure_CM.R10 – Determination of no evidence impact for SDA-C line item

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

- the analysis submitted of the SDA-C matrix as described under Requirement ISASecure_CM.R9 reports no impact; and
- a certifier review of evidence submitted per Requirement ISASecure_CM.R8 and Requirement ISASecure_CM.R9 finds no indication of such an impact after consultation with the component supplier.

Requirement ISASecure_CM.R11 – Determination of no evidence impact for FSA-C line item

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

- the analysis submitted of the FSA-C matrix as described under Requirement ISASecure_CM.R9 reports no changes to functionality covered by this line item of the FSA-C since the last certification; and
- a certifier review of evidence submitted per Requirement ISASecure_CM.R8 and Requirement ISASecure_CM.R9 finds no indication of such changes after consultation with the component supplier.

Requirement ISASecure_EDM.R12 – Deleted

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

If a component has been certified, then a component upgrade SHALL be granted certification to the same capability security level and ISASecure CSA certification version if:

- the organization that will develop the component going forward holds an ISASecure SDLA certification. In particular, the supplier SHALL hold an SDLA certification at the time of application for the certification of the component upgrade, and the scope of the process certified SHALL include that component; and
- criteria for passing the SDA-C element of certification are met per ISASecure_CM.R3 and Requirement ISASecure_CM.R10 ; and
- criteria for passing the FSA-C element of the certification are met per ISASecure_CM.R4 and Requirement ISASecure_CM.R11; and
- criteria for passing the VIT-C element of certification are met per ISASecure_CM.R6 and R7.

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

7 Certification to updated ISASecure criteria

The requirements in this section cover certification of a component that holds a prior certification, to a later version of the ISASecure certification criteria. These requirements suffice in the case that the component itself has not undergone upgrade modifications as well. If it has, see Section 8.

Requirement ISASecure_CM.R14 – SDA-C element for certification to a later ISASecure CSA version

A component that has been ISASecure CSA certified to capability security level *n* SHALL pass the SDA-C element of a certification to a later ISASecure CSA version at this same level, if any changed SDA-C requirements or changed validations in this ISASecure CSA version for capability security level *n*, are assessed as pass for the component.

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

Requirement ISASecure_CM.R15 – FSA-C element for certification to a later ISASecure CSA version

A component that has been ISASecure CSA certified to capability security level *n* SHALL pass the FSA-C element of a certification to a later ISASecure version at this same level if:

- any new FSA-C requirements added in this ISASecure version that are applicable to capability security level *n,* are assessed for the component as either *Met, Met by component, Met by integration into system, or Not Relevant,* per the criteria specified in the validation activity in [CSA-311]; and

- any changed FSA-C requirements or changed validations in this ISASecure version that are applicable to capability security level *n*, are likewise assessed for the component as either *Met, Met by component, Met by integration into system, or Not Relevant*.

Requirement ISASecure_CM.R16 – VIT-C element for certification to a later ISASecure version

A component that has been ISASecure CSA certified SHALL pass the VIT-C element of a certification to a later ISASecure version if the component passes VIT-C under the requirements in 6.2.

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

A component that has been ISASecure CSA certified to capability security level *n* SHALL be granted a new certification to a later ISASecure version at this same level if:

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

- certification criteria for passing SDA-C for capability security level *n* are met per ISASecure_CM.R14; and

- certification criteria for passing the FSA-C for capability security level *n* are met per Requirement ISASecure_CM.R15 ; and

- certification criteria for passing the VIT-C for capability security level *n* are met per Requirement ISASecure_CM.R16.

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

8 Certification for both component upgrade and new ISASecure version

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

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

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

9 Certification to a higher ISASecure CSA level

Once a component has achieved certification at ISASecure CSA capability security level *n*, the supplier may modify the component or available process evidence as deemed necessary, and then apply for a higher level certification. The following requirement applies in this situation.

Requirement ISASecure_CM.R19 – Certification of a component to a higher level

For a component, that previously received an ISASecure CSA certification to capability security level *n*, a certifier SHALL grant a certification to a higher ISASecure certification level for a (possibly upgraded) component if:

- if the component has been upgraded since the capability security level *n* certification was received, the criteria for granting a certification at the original level *n* for the modified component are met per Requirement ISASecure_CM.R13; and
- the additional FSA-C requirements present at the desired new level certification that are not present at capability security level *n* have been assessed as pass; and
- the SDA-C requirements for which validation criteria differ between capability security level *n* and the new higher certification level, have been assessed as pass; and
- the supplier holds an ISASecure SDLA certification at the time of granting of the certification that applies to the component going forward; and
- VIT-C has passed for the new capability security level, per ISASecure_CM.R6 and R7.

In this case the certification report SHALL provide content per Requirement ISASecure_CM.R13 as well as report on the new requirements assessed for the new certification level.

NOTE In accordance with [CSA-300] and [CSA-312], SDA-C requirements for which validation differs by CSA security capability level, are those requirements with validation activities explicitly defined as dependent upon the capability security level of the component. In SDLA-312 version 5.5, this is true for the one requirement SDLA-DM-4.