SSA-301
ISA Security Compliance Institute — System Security Assurance –
Maintenance of ISASecure® certification

Version 3.1

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
1.4	2014.02.09	Initial version published to http://www.ISASecure.org
1.6	2015.03.20	Use acronym SDLPA, update EDSA-310 reference, update ISASecure certification version numbering format, clarify wording regarding VIT by supplier in R5 and CRT criteria for no-repeat in R7
2.2	2018.02.05	Align with ANSI/ISA-62443-4-1 and IEC 62443-4-1: SDLA certification no longer has an associated certification level, although some SDLPA and SDA-S validations depend upon certification level; address scalable systems: mention scalable systems in overview clause 1, add terms scalable system, layout, reference layout, reference system, call out changes to certified layouts in 4.2, R4, R9
2.4	2018.10.02	Modify pass criteria for VIT to correspond to DM-4 in SDLA-312; Align with ANSI/ISA-62443-4-2: in clause 1 update discussion of FSA-E; provide reference to ISASecure-116; update normative references; delete term allocatable in clause 3 and revise definition of supported; change EDSA-311 to CSA-311 in R4 and R10; use updated FSA-E assessment outcome terminology and add validation for integration into particular system in R17
3.1	2019.08.18	Clarify definition of certification level; change device to component in definitions for layout, reference layout, and scalable control system; remove certifier CRT and NST; remove FSA-E; make SDLA prerequisite, incorporate maintenance of cert policy for updates and upgrades introduced in ISASecure-115

Contents

Foreword

This is one of a series of documents that defines ISASecure® certification for control systems, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This specification is one of the series of documents that describes requirements for ISASecure System Security Assurance (SSA) certification of systems. A description of the ISASecure program and the current list of documents related to ISASecure SSA as well as other ISASecure certification programs, can be found on the web site http://www.ISASecure.org.

1 Scope

This document specifies the criteria for maintaining ISASecure® SSA (System Security Assurance) certification for a control system, as the system and the ISASecure SSA criteria evolve over time. This document covers certification situations where:

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

In these cases, an evidence impact assessment may be performed in order to determine whether, and in what manner, evidence from a previous certification may be used as evidence toward a new certification. The requirements in this document address these topics.

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

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

ISASecure SSA certification of systems has three additional elements:

- Security development artifacts for systems (SDA-S);
- Functional security assessment for systems (FSA-S); and
- Vulnerability identification testing for systems (VIT-S).

Both the SDLA certification evaluation and SDA-S 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-S examines the artifacts that are the outputs of the supplier's secure product development lifecycle processes as they apply to the system to be certified. FSA-S examines the security capabilities of the system. VIT-S scans all components of a system for the presence of known vulnerabilities.

A system submitted for SSA certification is comprised of security zones, and an associated certification level designated by the supplier for each zone, which may be capability security level 1, 2, 3, or 4. The required SDLA certification does not have an associated level. The SDA-S and VIT-S assessments are the same for all certification levels with the exception of allowable residual risk for known security issues. FSA-S incorporates more requirements at higher levels, aligned with the requirements assigned to each capability security level in [IEC 62443-3-3].

For scalable systems, which are systems which support replication of components and/or zones in order to scale for small and large installations, tests performed by the certifier as part of FSA-S or VIT-S will be performed on a reference system, whose layout meets criteria specified in [SSA-300]. Analyses performed by the certifier will consider all layouts to be evaluated under the certification.

This document specifies when and how the results of a previous certification may be used for certification of a modified system, for a certification to a later version of the ISASecure criteria, or for a certification to a higher capability security level for one or more security zones. 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 SSA certification listed above.

2 Normative references

NOTE 1 The following document is the overarching technical specification for ISASecure SSA certification.

[SSA-300] *ISCI System Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

NOTE 2 The following document provides the technical evaluation criteria for the Vulnerability Identification Testing element of an SSA evaluation.

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

NOTE 3 The following document provides the technical evaluation criteria for the Functional Security Assessment element of an SSA evaluation.

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

NOTE 4 The following two documents provide the overall technical evaluation criteria for the Security Development Artifacts element of an SSA product evaluation. [SDLA-312] also provides the technical evaluation criteria for an ISASecure SDLA certification of a supplier's development lifecycle process.

[SSA-312] *ISCI System Security Assurance – Security development artifacts for systems,* as specified at http://www.ISASecure.org

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

[ISASecure-117] *ISCI ISASecure Certification Programs - Policy for transition to CSA 1.0.0 and SSA 4.0.0,* as specified at http://www.ISASecure.org

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
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.

3.1.3
certification level
capability security level for which conformance is demonstrated by a certification

NOTE An SSA certification for a particular security zone may be for capability security level 1, 2, 3, or 4. A zone certified under SSA to capability security level *n* meets requirements for capability security level *n* as defined in the standard IEC 62443-3-3:2013 *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*.

3.1.4
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.

3.1.5
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.6
essential function
function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control

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

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

3.1.8
industrial automation and control system
collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process

3.1.9
initial certification
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of a product under evaluation or of any of its prior versions

NOTE The first ISASecure SSA certification for a system is considered an initial certification *of that system*, regardless of whether some components of the system are ISASecure certified.

3.1.10
ISASecure version
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 SSA 4.0.0

NOTE An ISASecure version will map to document versions of the ISASecure technical specifications that define the technical criteria for certification.

3.1.11
layout
description of a specific instance of a scalable control system, that lists quantities of zones and resident components, and internal and external interfaces

3.1.12
reference layout
specific layout for scalable control system, that represents security characteristics found in any layout to be SSA certified, in a manner suitable to support testing that provides assurance for all such layouts

NOTE A reference layout may be neither the minimum nor the maximum layout for a scalable system. Its properties are specified in a requirement in [SSA-300]. In overview, the reference layout for a control system includes all zones, resident components in these zones, interfaces and protocols present in any layout in scope for a certification.

3.1.13
reference system
physical instance of a control system, that adheres to a reference layout

NOTE Use of a reference system may be specified for testing, when a system has many layouts.

3.1.14
scalable control system
control system which supports replication of zones and/or components to support small and large installations

3.1.15
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.

3.1.16
security zone
grouping of logical or physical assets that share common security requirements

NOTE 1 A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

NOTE 2 This definition and NOTE 1 are from the standard IEC 62443-3-3:2013. A zone configuration is part of the system architecture diagram submitted by applicants for ISASecure SSA certification, as required per [SSA-300].

3.1.17
supported
provided by the entity under evaluation itself

NOTE This term is used when referring to security functionality.

3.1.18
system
control system

NOTE In the ISASecure SSA documentation, this shorter term is used for convenience to refer to a control system product that may fall under the scope of ISASecure SSA certification. Per the definition above, control systems include safety systems.

3.1.19
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.20
upgrade
incremental hardware or software change in order to add new features

3.1.21
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CSA	Component Security Assurance
CVE	Common Vulnerabilities and Exposures
DCS	distributed control system
FSA-S	functional security assessment for systems
IACS	industrial automation and control system
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
PLC	programmable logic controller
SDA-S	security development artifacts for systems
SDL	security development lifecycle
SDLA	security development lifecycle assurance
SIF	safety instrumented function
SIS	safety instrumented system
SSA	system security assurance
SYM	system – maintenance (of certification)
VIT-S	vulnerability identification testing for systems

4 Overview

In this section we summarize the approach to maintenance of ISASecure SSA certification as a system and the ISASecure SSA 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 - 10 provide more detailed requirements for various certification maintenance scenarios.

4.1 SDLA Certification Prerequisite

In order to achieve any ISASecure SSA 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 systems

Different approaches are used for certification of system updates (bug fixes) and system upgrades (new system functionality). The terms *update* and *upgrade* are formally defined in [IEC 62443-4-2] and in the present document in 3.1.19 and 3.1.20.

The intent of the SSA 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 system. Certification evaluations for system upgrades will leverage prior certification evidence as described in this document.

4.2.1 System updates

Certification applies to a specific system version together with its updates. Once a supplier earns an SSA certification, that certificate remains valid for all system updates per the definition in 3.1.19 as long as:

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

4.2.2 System upgrades

A system supplier is not *required* to obtain a system certification for every system upgrade (including layout updates for scalable systems) that creates a new version of the system. The decision to certify a later system version is ultimately an optimization of end customer opinion and cost to the supplier. However, the supplier is required to clearly communicate to the marketplace which version(s) of their system fall under an ISASecure SSA certificate, and which version of the criteria is met, as stated in Requirement ISASecure_SY.R5 of [SSA-300].

If a system has achieved certification, and a system upgrade is submitted for certification to the same ISASecure version and zone capability security levels, the supplier may at their option request consideration for the prior certification evidence for either or both of the certification elements SDA-S and FSA-S. 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 system. Given the scope of changes to the system, if such an assessment is determined not to support revision of the evaluation with confidence, the certifier may elect to perform either or both of the evaluation elements in full for the modified system.

If an evidence impact assessment is performed and shows that the modifications to the system and its documentation would not affect the certification results for these elements, then no certification tests or evaluations will be necessary in order for the modified system 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 system upgrade. However, by policy, VIT-S is always run in its entirety on the upgraded system.

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

Sections 5-7 discuss requirements for certification of system upgrades.

4.3 Updated ISASecure criteria

As in the case of system upgrades, a system supplier is not required to revise a system certification to the latest ISASecure version. Hence, for example, a system certified to ISASecure SSA 3.0.0 is not required to obtain a certification to ISASecure SSA 4.0.0. However, all systems going through an initial certification or certification of an upgrade after ISASecure SSA 4.0.0 becomes available will be certified to that ISASecure SSA version, in accordance with the ISASecure published transition policy.

Consider the case where a system achieved certification under ISASecure SSA 3.0.0, and the system supplier decides to submit this same system version for certification to the new certification version ISASecure SSA 4.0.0. This certification process will consist of carrying out the defined delta between the two certification versions. Since the prior certificate for SSA 3.0.0 may apply to several updates of a system, the

supplier will determine one of these update versions to be used as the first certified version to be listed on a new SSA 4.0.0 certificate. That system version will be used for examining the delta certification requirements between SSA 3.0.0 and SSA 4.0.0. All system updates of this first version will fall under the new certificate.

An upgraded system may be submitted for certification to an ISASecure SSA certification version that also has changed. Consider the case where a system achieved certification under ISASecure SSA 3.0.0, and a system upgrade is submitted for certification to ISASecure SSA 4.0.0. This certification process will be logically equivalent to first certifying the system upgrade to ISASecure SSA 3.0.0 using the approach described in 4.2, and then carrying out the defined delta between the two certification versions SSA 3.0.0 and SSA 4.0.0 on the upgraded system.

Section 8 provides requirements for certification to modified ISASecure SSA certification criteria. Section 9 provides requirements for certifications when both the system and the certification criteria have been changed.

4.4 Certification to a higher level

Once a system has achieved certification with each of its security zones at a specified capability security level, the system supplier may modify the system or available process evidence as deemed necessary, and then apply for a system certification specifying a higher level certification for one or more zones. As noted in 4.1, the supplier must hold an ISASecure SDLA certification that applies to the system going forward, to achieve SSA certification to a higher level (or any SSA certification). Any system upgrades are assessed to the original certification levels following the approaches outlined in 4.2.2.

The validations for SDA-S and VIT-S evaluation criteria related to residual risk due to known security issues will differ by certification level. Requirements under FSA-S also increase by capability security level. Therefore, the certifier will evaluate the FSA-S and SDA-S certification criteria by zone that differ from those at the original zone capability security level. Finally, the certifier will rerun VIT-S and apply the pass/fail criterion for the new level. Since the prior certificate issued for a lower level for one of more zones, may apply to several updates of a system, 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 system version will be used for examining the delta certification requirements between the two certification levels.

Section 10 provides requirements for this case.

5 Requirements for certification of system updates

This section addresses maintenance of certification for updates of a system, which are defined in 3.1.19.

Requirement ISASecure_SYM.R1 – Identification of updates and upgrades

A chartered laboratory SHALL reach agreement with an applicant for SSA certification, on a policy that can be applied based upon examining system 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 system (see 3.1.20) SHALL require a new certification, and updates (see 3.1.19) SHALL NOT.

NOTE A new certificate would be issued when:

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

Requirement ISASecure_SYM.R2 – System update certification and withdrawal

An SSA certification applies to any update of a certified system (as identified under ISASecure_SYM.R1), for as long as:

- the supplier of the system maintains an ISASecure SDLA certification; and
- the scope of the SDLA certified process includes the system; and
- the system 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 an SSA certified system, then after a one year grace period, the SSA certification for that system SHALL be withdrawn. A supplier SHALL inform the certifying chartered lab when a certified system 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 system upgrades

The requirements in this section cover certifying an upgraded system, when a previous version of the system has already been certified to the same ISASecure version and zone capability security levels. The requirements are structured to address each of the certification elements (SDA-S, FSA-S, VIT-S) separately. In Section 7, a summary requirement is stated that incorporates these requirements together with the requirement for an SDLA certification.

6.1 Criteria for applying prior certification evidence to system upgrade

The following requirements provide the general criteria under which evidence from prior certifications is considered applicable toward earning certification for an upgraded system. Specific requirements on how these criteria are evaluated follow in Section 6.2.

Requirement ISASecure_SYM.R3 – SDA-S certification element for an upgraded system

If a system has been certified, then an upgraded version of the system SHALL on the basis of that prior evidence pass the SDA-S element of certification for the same ISASecure version and zone capability security levels, if:

- the certifier determines that an evidence impact assessment to determine whether the system modifications may have impacted each line item of the SDA-S can be performed with confidence (where a line item is a cell in the [SDLA-312] matrix), in the column applicable to product certifications; 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-S line items, and given them pass status.

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

Requirement ISASecure_SYM.R4 – FSA-S element for an upgraded system

If a system has been certified, then an upgraded version of the system SHALL on the basis of that prior evidence pass the FSA-S element of certification for the system, for the same ISASecure version and zone capability security levels, if:

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

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

- No system architecture change, change to the set of layouts to be certified, functionality change or significant new code has been incorporated related to a security feature referenced by the line item of the FSA-S.

In this case the certification report covering FSA-S MAY consist of only a summary of the FSA-S evidence impact assessment, results for those line items that were evaluated, and a reference to the prior certification report for the system. If the certifier determines that an FSA-S evidence impact assessment cannot be performed with confidence for the system, or that system changes related to the FSA-S are widespread for the system, then the certifier SHALL perform the full FSA-S as indicated for the system 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 system or device. Therefore, if there are sufficient changes to security functionality for the system which it appears may interact, then the full FSA-S is likely to be performed on the modified system. This is because an evidence impact assessment attempting to isolate the line items affected by the modifications, will likely need to examine all FSA-S line items to gain confidence, which will make this assessment essentially equivalent to simply performing a full FSA-S.

Requirement ISASecure_SYM.R5 – Performance of VIT-S certification element for an upgraded system

If a system has been certified, and an upgraded system later presented for certification, VIT-S SHALL be executed on the upgraded system such that the test meets the same requirements as for an initial certification, as described in [SSA-420]. In some cases, it MAY be run by the supplier instead of the chartered laboratory. In particular, if any FSA-S validations by independent tests are required for the certification of the upgraded system per Requirement ISASecure_SYM.R4, then VIT-S SHALL be performed by the chartered laboratory. If no FSA-S validations by independent tests are required, the chartered laboratory MAY permit the supplier to perform VIT-S 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_SYM.R6 – Requirements on supplier-executed VIT for modified system

If a supplier executes VIT-S toward certification of a revised system under the conditions in Requirement ISASecure_SYM.R5, this process SHALL meet the following requirements:

- supplier personnel responsible for the VIT-S 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-S 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-S:
    - documentation of the tested system 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
- the VIT-S evidence submitted to the chartered laboratory SHALL be signed by a responsible representative of the supplier.

Requirement ISASecure_SYM.R7 – Deleted

Requirement ISASecure_SYM.R8 – Deleted

6.2 Evidence and assessment for criteria

If based upon the criteria in Section 6.1, a system supplier believes that some or all of the evidence used to certify a previous version of a system is applicable toward certification of an upgraded system, they may request consideration for this evidence. In this case, their submission of data toward certification of the modified system will include supporting evidence to demonstrate that the criteria stated in the requirements of 6.1 are met. This sub 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 system changes.

Requirement ISASecure_SYM.R9 – Submission of modification data for system upgrade

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

- a high level description of modifications to the system since the previous certification (which may have been for an initial certification or a prior upgrade), including bug fixes, new functions, network or firewall configuration changes - for example, release notes from the supplier and from component suppliers, and any changes to the scope of SSA certification document that describes layouts covered by the certification; and
- a high level analysis of the impacts of these changes by system component.

This analysis shall describe:

- any new accessible interfaces on prior or new components; and
- any third party component that had new CVE reports against it since the prior certification; whether or not addressed by the time of application for certification; and
- any component with a change in third-party supplied sub components such as:
    - An OS service pack update; or
    - A new database version; and

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

Requirement ISASecure_SYM.R10 – Submission of analysis of modifications for system upgrade

If a system supplier has submitted evidence per Requirement ISASecure_SYM.R9 – Submission of modification data for system upgrade, then they SHALL in addition submit the following to the certification process:

- If consideration is requested for prior SDA-S evidence,
    - an analysis of the SDA-S 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 certifications, which were carried out to meet this validation requirement for this certification.
- If consideration is requested for prior FSA-S evidence:
    - an analysis of the FSA-S matrix, that notes for each numbered line item in [SSA-311] that applies to the capability security level for some zone in the system, whether there is any change to the configuration, functionality, or code supporting such zones and described by this requirement line item, among the system modifications since the previous certification. If so, the applicant SHALL provide a mapping to the related system modifications reported under Requirement ISASecure_SYM.R9.

The following requirements describe how the certifier renders a judgment that no certification-relevant changes to a system have occurred. In particular, these requirements enumerate for each element of an ISASecure SSA evaluation, how the certifier makes the decision in an evidence impact assessment, that results of that evaluation element would not be impacted due to the system modifications since a prior certification of the system.

NOTE No requirement is listed below regarding assessment of system modifications impacting VIT-S. Such an assessment would be inappropriate, since known vulnerabilities change over time even if there is no change to the system. Hence in accordance with Requirement_ISASecure_SYM.R5, full VIT-S is always run on an upgraded system.

Requirement ISASecure_SYM.R11 – Determination of no evidence impact for SDA-S line item

When performing an evidence impact assessment for an upgraded system 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-S evaluation have occurred if:

- the analysis submitted of the SDA-S matrix as described under Requirement ISASecure_SYM.R10 reports no impact; and
- a certifier review of evidence submitted per Requirement ISASecure_SYM.R9 and Requirement ISASecure_SYM.R10 finds no indication of such an impact after consultation with the system supplier.

Requirement ISASecure_SYM.R12 – Determination of no evidence impact for FSA-S line item

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

- the analysis submitted of the FSA-S matrix as described under Requirement ISASecure_SYM.R10 reports no changes to functionality covered by this line item since the last certification; and

- a certifier review of evidence submitted per Requirement ISASecure_SYM.R9 and Requirement ISASecure_SYM.R10 finds no indication of such changes after consultation with the system supplier.

Requirement ISASecure_SYM.R13 – Deleted

7 Criteria for granting certification to a system upgrade

The following requirement provides a summary statement of the criteria for granting a certification to an upgraded system based upon the previously stated requirements in Section 6.

Requirement ISASecure_SYM.R14 – Criteria for granting a certification to a system upgrade

If system has been certified with security zones $\{z_i\}$ to capability security levels $\{n_i\}$, then an upgraded version of the system SHALL be granted certification to the same zone capability security levels and ISASecure SSA version if:

- the organization that will develop the system 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 system upgrade, and the scope of the process certified SHALL include that system; and

- criteria for passing the SDA-S element of the certification are met per Requirement ISASecure_SYM.R3 and Requirement ISASecure_SYM.R11; and

- criteria for passing the FSA-S element of the certification are met per Requirement ISASecure_SYM.R4 and Requirement ISASecure_SYM.12; and

- criteria for passing the VIT-S element of the certification are met per Requirement ISASecure_SYM.R5 and Requirement ISASecure_SYM.R6.

Alternatively, for each of the evaluation elements SDA-S or FSA-S for which the supplier did not request consideration for the prior certification per Requirement ISASecure_SYM.R9, the certifier SHALL evaluate that element under the criteria for initial certification found in [SSA-300].

8 Certification to updated ISASecure criteria

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

The intent of these requirements is that an evaluation of the delta between versions of the ISASecure criteria is sufficient to support certification to a later version of the criteria.

Requirement ISASecure_SYM.R15 – SDA-S element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the SDA-S element of a certification to a later ISASecure SSA version if:

- any new SDLA requirements added in this ISASecure SSA version are assessed as pass under SDA-S for the system; and

- any changed SDLA requirements in this ISASecure SSA version are assessed as pass under SDA-S for the system.

NOTE It is possible that this requirement may be met for a system, 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 system is developed. The requirement may therefore be met for this system, but not met (yet) for all systems or components under that process. The requirement for maintenance of the development process itself for new ISASecure requirements, is described in [SDLA-300].

Requirement ISASecure_SYM.R16 – FSA-S element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the FSA-S element of a certification to a later ISASecure SSA version if:

- any new FSA-S requirements added in this ISASecure SSA version are assessed for the system as either supported or NA; and
- any changed FSA-S requirements in this ISASecure SSA version are assessed for the system as either supported or NA.

Requirement ISASecure_SYM.R17 – Deleted

Requirement ISASecure_SYM.R18 – VIT-S element for certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified SHALL pass the VIT-S element of a certification to a later ISASecure SSA version if VIT-S is executed in full against the system and passes per the later ISASecure SSA version.

Requirement ISASecure_SYM.R19 – Deleted

The following requirement provides a summary statement of the criteria for granting a certification to a later ISASecure SSA version, for a system which previously achieved ISASecure SSA certification to an earlier ISASecure SSA version. It is based upon the previously stated requirements.

Requirement ISASecure_SYM.R20 – Criteria for granting a certification to a later ISASecure SSA version

A system that has been ISASecure SSA certified with zones $\{z_i\}$ to capability security levels $\{n_i\}$ SHALL be granted a certification to a later ISASecure SSA version at these same zone capability security levels if:

- the organization that will develop the system 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 system, and the scope of the process certified SHALL include that system; and
- certification criteria for passing SDA-S are met per Requirement ISASecure_SYM.R15; and
- certification criteria for passing the FSA-S are met per ISASecure_SYM.R16; and
- certification criteria for passing the VIT-S are met per Requirement ISASecure_SYM.R18.

Since the prior certificate may apply to several updates of the system, the supplier will determine which one of these update versions will be evaluated under the new SSA version. This system update version and any existing later system updates will be initially listed on the new certificate.

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

9 Certification for both system upgrade and new ISASecure SSA version

It will be a common scenario that a system will have been upgraded by the time a new version of the ISASecure SSA certification criteria is released. Thus, it will be useful to be able to certify a system upgrade

to a newer version of ISASecure SSA, 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 upgraded systems and certification to later ISASecure SSA versions. These have been defined in previous sections.

Requirement ISASecure_SYM.R21 – Certification of a system upgrade to a later ISASecure SSA version

For a system that previously received an ISASecure certification, a certifier SHALL grant a certification to a later ISASecure SSA version for an upgraded system if the criteria in both Requirement ISASecure_SYM.R14 and Requirement ISASecure_SYM.R20 are met.

10 Certification to higher level for a security zone

Once a system has achieved ISASecure SSA certification with security zones $\{z_i\}$, to capability security levels $\{n_i\}$, the vendor may modify the system or available evidence as deemed necessary, and then apply to change one or more of the levels $\{n_i\}$ to a higher value. The following requirement applies in this situation.

Requirement ISASecure_SYM.R22 – Certification of a system incorporating a higher level security zone

For a system that previously received an ISASecure SSA certification with zones $\{z_i\}$ to capability security levels $\{n_i\}$, a certifier SHALL grant a certification where one of more of the $n_{i,}$ is changed to a higher level, for this same system or an upgraded system if:

- the criteria for granting a certification at the original levels $\{n_i\}$ for an upgraded system are met per Requirement ISASecure_SYM.R14; and
- VIT-S pass criteria are met for those zones where certified capability security level has increased, at their new higher level; and
- the additional FSA-S requirements that apply to the higher capability security level for any security zone, that did not apply to its previously certified capability security level, have been assessed as pass; and
- the supplier passes an SDA-S evaluation for those SDLA-312 requirements whose validation depends upon capability security level, for those zones where certified capability security level has increased; and
- the supplier holds an ISASecure SDLA certification at the time of granting of the higher level certification, that applies to the system going forward.

The prior certificate may apply to several updates of the system. If the system presented for higher level certification does not include upgrades, the supplier will determine which one of these update versions covered by the prior certificate will be evaluated for the new level(s). This system update version and any existing later system updates will be initially listed on the new certificate.

The certification report SHALL provide content per Requirement ISASecure_SYM.R14 if this is a upgraded system, as well as report on the new requirements assessed or validations applied for all new zone certification level(s).

NOTE In SDLA-312 v5.5, the one requirement SDLA-DM-4 regarding the treatment of residual risk related to known security issues, depends upon capability security level.