SDLA-300

ISA Security Compliance Institute – Security Development Lifecycle Assurance –

ISASecure certification and maintenance of certification requirements

Version 1.9

June 2020

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
1.3	2014.06.02	Initial version published to http://www.ISASecure.org
1.6	2018.02.01	Align with ANSI/ISA 62443-4-1: ANSI/ISA and IEC 62443-4-1 made normative references and cited as source for requirements, remove references to and requirements involving security levels, update Appendix minimum requirements list
1.9	2020.06.19	Require documented process accessible to certified development organization (R1), add option for shorter certification expiration if not all artifacts available using SDLA readiness evaluation (R5,8,12), modify certifier action for major nonconformity in Table 1, permit year grace period for audit of common supplier SDL process (R10), remove recognition for certification pending, replace EDSA by CSA

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). Certifications available include ISASecure Component Security Assurance (CSA) for industrial control system components, ISASecure System Security Assurance (SSA) for control systems and ISASecure Security Development Lifecycle Assessment (SDLA) which addresses control system supplier development processes. This specification is the overarching document in the series that describes technical requirements for ISASecure SDLA certification of secure product development lifecycle processes. It references all other documents that contain these requirements and places them in context. The current list of documents related to ISASecure certification programs can be found on the web site http://www.ISASecure.org.

1 Scope

1.1 Scope of this document

This document defines the types of development organizations (as defined in 3.1.7) that fall within the scope of the ISASecure SDLA (Security Development Lifecycle Assurance) certification program. It specifies the criteria for granting an initial certification and for an organization to maintain this certification.

1.2 Scope for SDLA certification

Development organizations for critical systems that specify compliance to the ANSI/ISA/IEC 62443 standards may apply for ISASecure SDLA certification.

1.3 Overview of criteria for certification

Section 5 of the present document defines the criteria for ISASecure SDLA certification. To specify the criteria for achieving certification, this document references the SDLA technical specification document [SDLA-312] listed in Section 2 that covers detailed requirements for the certification.

An SDLA evaluation examines the processes that a specific development organization uses to develop systems or components. This includes examining documentation for the process, as well as evidence that shows that the process has been followed for products that fall within the defined scope of that process.

An organization meeting SDLA requirements achieves certified status until a specific expiration date. A recertification process is then required to extend the certification. If during an initial certification assessment, some aspects of the development organization's process are fully documented but have not yet been executed, the certifier can grant certification for a limited time period based upon evidence of the organization's readiness to execute them.

2 Normative references

[SDLA-100] *ISA Security Compliance Institute Security Development Lifecycle Assurance - ISASecure certification scheme*, 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

[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*

3 Definitions and abbreviations

3.1 Definitions

3.1.1
application
<information technology> software program(s) executing on the infrastructure that are used to interface with the process or the control system itself (e.g. configuration software, historian)

3.1.2
application
<administrative process> form used or set of requirements met in order to make a request

3.1.3
certifier
chartered laboratory

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

3.1.5
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.6
control system 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
development organization
part of a supplier's organization that develops products, components, and systems, and defines and employs a secure development process that encompasses all IEC 62443-4-1 practices

NOTE Some suppliers have a separate organization that defines and maintains their development process. The above definition implies that for the purposes of the present document, such an organization is considered to be a part of all development organizations which employ that process.

3.1.8
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.

3.1.9
host device
general purpose device running a general purpose operating system (e.g. Windows OS, Linux) capable of hosting one or more applications, data stores or functions

NOTE Typical attributes: rotating media, no real time scheduler, 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
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 and identified by a 3-place number such as ISASecure SDLA 3.0.0

3.1.13
major nonconformity
instance for any requirement, in which no evidence exists that the requirement has been met, or instance for an SDLA minimum requirement, in which evidence does not show that the requirement is consistently met

3.1.14
minimum requirements
subset of the numbered SDLA certification requirements from [SDLA-312] which are considered of high relative importance

NOTE Minimum requirements are listed in the Appendix. The minimum requirements concept is used in defining the concept of major nonconformity.

3.1.15
minor nonconformity
instance for any requirement that the requirement has not been met, but the failure is not classified as a major non-conformity

3.1.16
network device
device which facilitates data flow between devices, or restricts the flow of data, but does not directly interact with a control process

NOTE Typical attributes: Embedded OS or firmware, no HMI, no real-time scheduler, configured through an external interface.

3.1.17
product
system, subsystem or component that is manufactured, developed or refined for use by other products

NOTE The processes required by the practices defined in [IEC 62443-4-1] apply iteratively to all levels of product design (for example, from the system level to the component level).

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
DCS	distributed control system
HMI	human machine interface
IACS	industrial automation and control system
ISCI	ISA Security Compliance Institute
OS	operating system
PLC	programmable logic controller
SCADA	supervisory control and data acquisition
SDL	security development lifecycle
SDLA	security development lifecycle assessment or security development lifecycle assurance
SDLPA	security development lifecycle process assessment
SIS	safety instrumented system
SSA	System Security Assurance

4 Background

The ISASecure program has been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for Industrial Automation and Control Systems (IACS). ISASecure SDLA certification achieves this goal by offering a common industry-recognized set of security development lifecycle process requirements that drive product

security based on the IEC 62443-4-1 standard [IEC 62443-4-1], simplifying procurement for asset owners, and development assurance for control system product suppliers.

ISCI has developed product certification programs for:

- IACS components, the ISASecure CSA program (Component Security Assurance)
- Control systems, the ISASecure SSA program (System Security Assurance).

NOTE The separate documents CSA-300 *ISASecure CSA certification requirements* and SDLA-300 *ISASecure SSA certification requirements* define criteria for CSA and SSA product certifications, respectively.

The ISASecure SDLA program complements these ISASecure certification programs that certify specific products. It simplifies the process for suppliers that wish to certify multiple products. For example, a supplier development organization that holds an SDLA certification, thereby satisfies the SDLPA (Security Development Lifecycle Process Assessment) element of an ISASecure CSA or SSA certification evaluation for one or any number of the supplier's control system products under that development organization. Therefore, the required examination of the development process to achieve a specific product certification is limited to the SDA element (Security Development Artifacts) of CSA or SSA, in which the secure product development artifacts for the specific product to be certified are examined. A reexamination of the process documentation itself is not required.

The ISASecure programs support and align with the ANSI/ISA/IEC 62443 series of standards for IACS security. [SDLA-100] discusses the relationship between ISASecure SDLA and the 62443 effort. ISASecure SDLA validates conformance of an organization with the standard [IEC 62443-4-1]. ANSI/ISA has published this standard as [ANSI/ISA-62443-4-1]. [SDLA-312] defines criteria for validating conformance to that standard.

ASCI (Automation Standards Compliance Institute) will accredit private organizations to perform ISASecure SDLA certification evaluations as “certifiers.” ASCI grants accredited certifiers the right to grant and maintain ISASecure SDLA certifications for supplier development organizations based upon the certifier’s assessments conforming to the ISASecure SDLA specifications in [SDLA-312]. ISCI will publish on its website a list of SDLA certified development organizations.

NOTE ISCI is organized under the umbrella structure provided by ASCI.

5 Certification requirements

5.1 Certification scope and definition

Requirement ISASecure_SDL.R1 – Definition of SDLA certification

An SDLA certification SHALL apply to:

- a named development organization or organizations
- a named, documented security development lifecycle (SDL) process under version control that is made accessible to and used by that organization(s).

Requirement ISASecure_SDL.R2 – Publication of SDL certification status

If ISCI, the certifier, or a supplier publishes certification status information for a supplier's SDL in a public venue, information provided SHALL identify the development organization(s) and process for which the certification was granted, and the ISASecure version and expiration date for the SDLA certification.

NOTE Expiration for certification is defined in Section 5.3.

5.2 Certification application and criteria

Requirement ISASecure_SDL.R3 – Deleted

Requirement ISASecure_SDL.R4 – Application requirements for certification

Items specified as follows SHALL be submitted to the ISASecure SDLA certification process by an applicant for an initial certification or recertification:

a) the development organization's documented SDL, which itself SHALL specify:
   i. whether it applies to development of components, systems or both; and
   ii. the scope of products to which the organization applies the process (which may be all products); and

b) process artifacts and other evidence that allows the certifier to validate that the organization is following the SDL in accordance with the column labeled "Development Organization and SDL Validation Activity" in [SDLA-312] and Requirement ISASecure_SDL.R5 in the present document. The organization SHALL submit evidence as selected by the certifier from among those products that fall under the scope of the SDL.

NOTE 1 The requirement for recertification is defined in Section 5.3.

In accordance with the next requirement ISASecure_SDL.R5, for an initial certification, a supplier can request either a *full SDLA evaluation* or an *SDLA readiness evaluation,* for individual requirements in [SDLA-312]. A supplier that has passed validation of each requirement in [SDLA-312], under their choice of these two evaluation methods, may obtain certification. The option to evaluate requirements using an SDLA readiness evaluation means that the supplier may obtain certification before the SDL is fully practiced. Examination of artifacts from execution of the development process for specific products is not required for a readiness evaluation. Certification based upon a full SDLA evaluation requires such artifacts for many requirements, and has a longer expiration period than for a certification partially based upon readiness evaluation. Expiration is determined as described in requirement ISASecure_SDL.R8.

Requirement ISASecure_SDL.R5 – Criteria for granting initial certification

An initial ISASecure SDLA certification SHALL be granted to a development organization if all SDLA requirements in [SDLA-312] applicable to the scope of the SDL (systems, components or both), are assessed as pass. The certifier SHALL validate these requirements using one of the following evaluation methods. The evaluation method used for validation to determine passing status SHALL be agreed between the certifier and the supplier for each individual SDLA requirement.

- *SDLA full evaluation:* evaluation as described in the column labeled “Development Organization and SDL Validation Activity” in [SDLA-312].
- *SDLA Readiness evaluation:* evaluation as described in the column labeled “Development Organization and SDL Validation Activity” in [SDLA-312], with the following modifications. These modifications are applied to all requirements for which the validation activity states that examination of artifacts from execution of the development process for specific products is mandatory, except for requirements in Appendix A of [SDLA-312].
  - Omit from the existing validation activity, review of actual output (proof of execution) artifacts from execution of the development process for specific products
  - Verify that evidence of readiness to execute the process exists (such as training, tools, templates).

NOTE 2 If the validation activity for a requirement in [SDLA-312] does not include mandatory examination of artifacts from execution of the development process, then the SDLA full evaluation and the SDLA readiness evaluation for that requirement are the same. Both are fully described by the validation activity defined in [SDLA-312].

NOTE 3 Listed below are the twenty-one requirements in [SDLA-312], outside of Appendix A of [SDLA-312], for which the validation activity states that examination of artifacts from execution of the development process for specific products is mandatory. For requirements not on this list, [SDLA-312] states in some cases that such artifacts *may* be examined as part of the validation activity, but are not mandatory. (For example, this is the case for all SDLA-SG requirements.)

SDLA-SM-3
SDLA-SM-5
SDLA-SM-8
SDLA-SM-9
SDLA-SR-2i
SDLA-SD-3
SDLA-SD-4E
SDLA-SI-1
SDLA-SI-1C-1
SDLA-SI-2
SDLA-SVV-1A1
SDLA-SVV-1A3
SDLA-SVV-2-2
SDLA-SVV-3A1
SDLA-SVV-3A3
SDLA-SVV-3A5
SDLA-SVV-3C1
SDLA-SVV-3C2
SDLA-SVV-3D
SDLA-SVV-3E
SDLA-DM-3A

Requirement ISASecure_SDL.R6 – Deleted

Requirement ISASecure_SDL.R7– Deleted

5.3 Certification expiration and recertification

Requirement ISASecure_SDL.R8 – Initial certification expiration

The terms *SDLA full evaluation* and *SDLA readiness evaluation* used in this requirement are as defined in prior requirement ISASecure_SDL.R5.

An initial ISASecure SDLA certification for which an SDLA full evaluation has passed for all SDLA requirements in [SDLA-312], SHALL remain valid until the end of the 36th month from when it is granted.

An initial ISASecure SDLA certification for which an SDLA readiness evaluation has passed for all requirements in [SDLA-312], but one or more SDLA requirements has not passed an SDLA full evaluation, SHALL remain valid until the end of the 12th month from when it is granted.

Requirement ISASecure_SDL.R9 – Extension of 36-month certification

An organization MAY extend the expiration date for their existing 36-month certification by undergoing a recertification audit as described in ISASecure_SDL.R10. In particular, the certifier SHALL take actions as indicated in Table 1. *Major conformity* and *minor nonconformity* are defined based upon the concept of *minimum requirements*, where these terms are defined in Section 3. Minimum requirements are listed in the appendix to this document.

Table 1 - Actions following recertification audit for existing 36-month certification

Recertification Audit Findings	Action
No nonconformities found	• Extend certification expiration 36 months from expiration date of prior certification

Minor nonconformities found	• If a specific minor nonconformity is open since last recertification, existing certification expires on its expiration date
	• Otherwise:
	  ○ Re-audit related requirements at next recertification, or earlier if requested by client, and clear nonconformity if re-audit passes
	  ○ If no major nonconformities, extend certification 36 months from prior certification

Major nonconformities found	• Identify root cause, and that nonconformities are corrected in both supplier process and in supplier audit function. Verify conformance after correction, for one instance of process execution • If above conditions are met by expiration date of existing certificate, and no minor nonconformities are open since last recertification, extend certification 36 months from prior certification • Otherwise, existing certificate expires on its expiration date

NOTE 2 If an organization's certification expires, then to regain certification the organization must begin again with the process of initial certification as described in Requirement ISASecure_SDL.R5.

Requirement ISASecure_SDL.R10 – Recertification audit for 36-month certification

For a recertification audit of an SDLA certification that had been granted with 36 months to expiration, the certifier SHALL verify for the previously certified development organization that:

- Changes and updates to the previously certified process, as recorded via the version control system in place under ISASecure_SDL.R1, comply with the current version of the ISASecure SDLA requirements. In particular:
  - There may be elements of the documented SDL process used by a development organization, that are employed in common with other SDLA certified development organizations for the same supplier. The check of compliance of changes and updates to these SDL elements against the current SDLA, toward recertification of any one of these development organizations, MAY be reused toward recertification of any other, if the check has taken place at most one year before a recertification is issued.
  - For any other elements of the SDL process for a development organization, this verification SHALL take place when granting the new certification.

- The development organization is following all elements of its current SDL for products within the defined scope of the SDL.

NOTE 3 The first sub bullet under the first major bullet in this requirement, is intended to efficiently support the case in which a supplier maintains one SDL that applies across many or all of its certified development organizations. An annual audit of a supplier's common SDL process would ensure the first sub bullet is always met. However, neither a common supplier-wide process nor such an annual audit is required by these specifications. The second sub bullet acknowledges that even in the case of a common supplier SDL, there may also be some detailed SDL elements that are specific to particular development organizations and impact compliance with SDLA requirements. They are therefore subject to evaluation when recertifying that development organization. Examples are work instructions and tool configurations.

NOTE 4 An audit of *all* elements of an SDL when granting any extension to a 36-month certification, would meet and exceed the criterion defined in the first major bullet of this requirement.

Requirement ISASecure_SDL.R11 – Deleted

Requirement ISASecure_SDL.R12 – Extension of 12-month certification to 36 months

A certifier SHALL grant an extension to an initial SDLA certification that had been granted with 12 months to expiration, if the following criterion is met. The new certification SHALL expire at the end of the month, 36 months after the granting of the prior 12-month certification.

- All SDLA requirements that initially passed based upon an SDLA readiness evaluation have passed an SDLA full evaluation, where these evaluation types are defined in requirement ISASecure_SDL.R5 of this document.

If this criterion has not been met as of the expiration date of the 12-month certification, SDLA certification SHALL expire. In this case, to regain SDLA certification, a development organization SHALL pass all requirements based upon an SDLA evaluation as defined in requirement ISASecure_SDL.R5.

APPENDIX *- SDLA Minimum Requirements*

The following is the list of "minimum requirements" from [SDLA-312]. The requirements in this list are referred to as a group, within the text of some requirements of this document, SDLA-300.

- SDLA-SM-3 Identification of applicability
- SDLA-SM-4 Security expertise
- SDLA-SM-6 File integrity
- SDLA-SM-9 Security requirements for externally provided components
- SDLA-SR-2 Threat model
- SDLA-SR-3 Product security requirements
- SDLA-SD-4E Secure design best practices - attack surface reduction
- SDLA-SVV-1A1 Security requirements testing (plan)
- SDLA-SVV-2-1 Threat mitigation testing (abuse testing for mitigated threats)
- SDLA-SVV-3A1 Vulnerability testing - fuzz testing (plan)
- SDLA-SVV-3A3 Vulnerability testing - fuzz testing (results)
- SDLA-SVV-3B Vulnerability Testing - attack surface analysis
- SDLA-SVV-3C1, 3C2 Vulnerability testing - black box known vulnerability testing
- SDLA-SVV-3D Vulnerability Testing - binary composition analysis
- SDLA-DM-1A Receiving notifications of security-related issues
- SDLA-DM-3 Assessing security-related issues (track and assign criticality)
- SDLA-DM-3A Assessing security-related issues (impact analysis)
- SDLA-DM-3D Assessing security-related issues (root cause)
- SDLA-DM-5 Disclosing security related issues
- SDLA-SUM-1 Security update qualification
- SDLA-SG-1A, 1B, 1C Product defence in depth
- SDLA-SG-3 Security hardening guidelines (all parts)