SDLA-300

ISA Security Compliance Institute — Security Development Lifecycle Assurance –

ISASecure certification and maintenance of certification requirements

Version 1.3

June 2014

Revision history

version	date	changes
1.3	2014.06.02	Initial version published to http://www.ISASecure.org

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 Embedded Device Security Assurance (EDSA) for embedded devices, ISASecure System Security Assurance (SSA) for control systems and ISASecure Security Development Lifecycle Assessment (SDLA) which addresses control system supplier security development processes. This specification is the overarching document in the series that describes technical requirements for ISASecure SDLA certification of security 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 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 ISA 62443 standards may apply for ISASecure SDLA certification.

1.3 Overview of criteria for certification

To specify the criteria for achieving ISASecure SDLA certification, this document references the SDLA technical specification document [SDLA-312] listed in Clause 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 all [SDLA-312] requirements for a particular security level achieves certified status at that level until a specific expiration date, A recertification process is then required to extend the certification. The program also defines a process via which an organization meeting most of these requirements receives formal recognition for their progress. An organization that receives this recognition may meet the remaining requirements within a specified time period to achieve certification.

2 Normative references

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

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

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

software or hardware/software element that may be used as part of a control system

NOTE Embedded devices, host devices, network devices and applications are control system components.

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
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.).

3.1.9
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

3.1.10
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

3.1.11
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 2.6.1

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

3.1.12
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 criteria for SDLA certification pending, and the concept of major nonconformity.

3.1.13
minor nonconformity

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

3.1.14
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 Attributes Typical attributes: Embedded OS or firmware, no HMI, no real-time scheduler, configured through an external interface.

3.1.15
SDLA certification pending
formal status of a candidate for SDLA certification, via which ISCI confirms that the organization has made significant progress toward meeting SDLA requirements

3.2 Abbreviations

The following abbreviations are used in this document

ASCI	Automation Standards Compliance Institute
DCS	distributed control system
EDSA	embedded device security assurance
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
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, simplifying procurement for asset owners, and development assurance for control system product suppliers.

ISCI has developed product certification programs for:

- embedded devices, the ISASecure EDSA program (Embedded Device Security Assurance)
- control systems, the ISASecure SSA program (System Security Assurance).

NOTE The separate documents EDSA-300 *ISASecure EDSA certification requirements* and SDLA-300 *ISASecure SSA certification requirements* define criteria for EDSA 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 at an applicable level, thereby satisfies the SDLA component of an ISASecure EDSA or SSA certification evaluation for one or any number of the supplier's control system products. Therefore the required examination of the development process to achieve a specific product certification is limited to the SDA component (Security Development Artifacts), in which the security development artifacts for the product to be certified are examined. A reexamination of the process documentation itself is not required. Further, suppliers that develop types of control system products for which ISASecure product certification is not available at this time, may nevertheless apply for ISASecure SDLA certification.

The ISASecure SDLA program offers four certification levels for a process, offering increasing levels of security assurance. These certifications are called ISASecure SDLA Level 1, ISASecure SDLA Level 2, ISASecure SDLA Level 3, and ISASecure SDLA Level 4. SDLA requirements increase in rigor from Level 1 to Levels 2, 3, and 4.

The evaluation criteria in [SDLA-312] were developed from a variety of industry sources. The source for each criterion is listed in [SDLA-312]. A bibliography for these sources is found at the end of the present document.

It is a goal for the ISASecure programs to support and align with the developing standards ISA 62443 for IACS security. [SDLA-100] discusses the relationship between ISASecure SDLA and the ISA 62443 effort.

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 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, as well as those organizations progressing toward this certification, that have achieved a specified level of compliance.

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 used by that organization(s)
- a certification level of 1, 2, 3, or 4.

Requirement ISASecure_SDL.R2 – Publication of SDL certification status

If ISCI, the certifier, or a supplier publishes certification status information for the supplier's SDL in a public venue, information provided SHALL include the name of the development organization(s) and process for which the certification was granted, the certification level, and the ISASecure version and expiration date for the SDLA certification. This information SHALL also be provided when publishing the status of ISASecure SDLA certification pending.

NOTE Expiration for pending status is defined in Section 5.2. Expiration for certification is defined in Section 5.3.

5.2 Certification application and criteria

Requirement ISASecure_SDL.R3 – Application for a certification level

When an organization applies for certification of an SDL, the certification applicant SHALL specify the maximum level for which they would like SDL certification. The levels possible are 1, 2, 3, or 4. The certifier

SHALL award certification to an organization at the highest level for which the SDL qualifies, up to this maximum level.

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 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]. The organization SHALL submit evidence as selected by the certifier from among those products that fall under the scope of the SDL.

NOTE The requirement for recertification is defined in Section 5.3.

Requirement ISASecure_SDL.R5 – Criteria for granting initial certification

An initial ISASecure SDLA certification SHALL be granted to a organization for the security level requested in ISASecure_SDL.R3 if all SDLA requirements in [SDLA-312] applicable to the scope of the SDL (systems, components or both) for this level, are assessed as pass. A certification to a lower security level SHALL be granted if all of the requirements for that level have been assessed as pass. Validation of these requirements SHALL take place as described in the column labeled “Development Organization and SDL Validation Activity” in [SDLA-312].

ISCI grants formal recognition to organizations progressing toward SDLA certification, that meet a significant portion of the requirements for this certification, as described in the following requirement.

Requirement ISASecure_SDL.R6 – Criteria for granting ISASecure SDLA certification pending

The status of "ISASecure SDLA certification pending" SHALL be granted to an organization that is progressing toward initial SDLA certification if:

- all minimum requirements in [SDLA-312] applicable to the scope of the SDL (systems, components or both), are assessed as pass. The minimum requirements are listed in the Appendix; and

- 80% of the remaining applicable requirements for security level 1, are assessed as pass.

Validation of these requirements SHALL take place as described in the column labeled “Development Organization and SDL Validation Activity” in [SDLA-312].

NOTE ISASecure SDLA certification pending status recognizes progress in meeting SDLA level 1 requirements. At this time, there are no similar pre-certification designations that recognize progress beyond level 1 to a higher levels of certification.

Requirement ISASecure_ SDL.R7– Transition to certification following SDLA certification pending status

Within 12 months after the status of SDLA certification pending is granted, the certifier SHALL perform an audit which SHALL consist of:

- validation of the remaining requirements not previously passed

- validation of available artifacts demonstrating compliance with requirements previously passed, where artifacts were not previously evaluated for those requirements.

If all requirements for a security level pass, and the artifacts evaluated demonstrate compliance with requirements previously passed, then the certifier SHALL grant SDLA certification at that level. If all requirements for some security level do not pass within 12 months, then SDLA certification pending status expires. The audit of remaining requirements and new artifacts described in this requirement MAY be performed as part of an evaluation toward an ISASecure product certification.

5.3 Certification expiration and recertification

Requirement ISASecure_SDL.R8 – Certification expiration

An initial ISASecure SDLA certification or recertification SHALL remain valid until the end of the 36th month from when it is granted.

Requirement ISASecure_SDL.R9 – Extension of certification

An organization MAY extend the expiration date for their existing certification by undergoing a recertification audit as described in ISASecure_SDL.R10. In particular, the certifier SHALL take actions as indicated in Table 1:

Table 1 - Actions following recertification audit

Certification Level	Recertification Audit Findings	Action
Any	No nonconformities found	• Extend certification 36 months from prior certification
1	Minor nonconformities found	• If a specific minor nonconformity is open since last recertification, withdraw certification when prior certificate expires • 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
1	Major nonconformities found	• If not compliant by the later of: 60 days after the nonconformity was reported to the supplier, or the expiration date of the prior certificate, then withdraw the certification • The organization retains its certification during the 60 day grace period
2, 3, 4	Minor nonconformities found	• If a specific nonconformity required for level 1 is open since last recertification, withdraw the

Certification Level	Recertification Audit Findings	Action
		certification when prior certificate expires • If a specific nonconformity required for any level n>1 is open since last recertification, then n-1 is the maximum level that can be achieved upon recertification • If certificate is not withdrawn: ○ 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 at the prior certification level, unless this is higher than the maximum level that can be achieved as described above, in which case the level is set to this maximum
2, 3, 4	Major nonconformities found	• If not compliant by the later of: 60 days after the nonconformity was reported to the supplier, or the expiration date of the prior certificate, take one of the following actions as supported by the recertification audit results: ○ grant a lower level of certification with expiration 36 months beyond the expiration date of the prior certification ○ withdraw the certification • The organization retains its certification during the 60 day grace period

NOTE 1 If an organization is granted a lower level certification after a recertification audit, they may regain their previous level as described in Requirement ISASecure_SDL.R11.

NOTE 2 If an organization's certification expires or is withdrawn, then to regain certification the organization must begin again with the process of initial certification as described in Requirements ISASecure_SDL.R5 and R6.

Requirement ISASecure_SDL.R10 – Recertification audit

For a recertification audit, the certifier SHALL verify 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.
- The current SDL is being followed for all products within its defined scope.

Requirement ISASecure_SDL.R11 – Certification to a higher level

Any organization that holds an SDLA certification MAY at any time apply for an audit to obtain a certification to a higher level. The audit SHALL cover only the requirements for the new level that are not requirements at the organization's present certification level. The expiration of the new certification SHALL be the same as for the prior certification.

BIBLIOGRAPHY

NOTE The following documents are sources for the requirements in [SDLA-312]. The notation in bold is used in that document.

[CLASP] Comprehensive Lightweight Application Security Process v1.2 https://www.owasp.org/index.php/Category:OWASP_CLASP_Project#CLASP_v1.2

[DO-178B] RTCA Inc., RTCA/DO-178B: Software considerations in airborne systems and equipment certification, 1992

[IEC-61508-1] IEC Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, 2010

[IEC-61508-3] IEC Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 2010

[ISO/IEC 15408-3] ISO/IEC 15408 Information technology - security techniques - evaluation criteria for IT security - Part 3: Security assurance components, 2008

[Microsoft] Microsoft Security Development Lifecycle http://www.microsoft.com/security/sdl/default.aspx

NOTE The SDLA certification requirements will be aligned with the following standard when approved.

ISA 62443-4-1 Security for industrial automation and control systems – Product development requirements (under development as of publication of this document)

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, in some requirements of this document, SDLA-300.

- SMP 1.5 Competence
- SRS-1 Security Requirements Specification
- SAD-6 Attack Surface Reduction
- SDLA-SRA-3 Threat Modeling
- SRA-3.2 Threat Model Updates
- DSG-1.1.2 Installation Requirements
- DSG-1.1.5 Known Security Risks
- SIT-1.1 Fuzz Test Plan
- SIT-1.3 Fuzz Test Results
- SIT-2.1 Threat Exploitation
- SIT-3.2 Known Vulnerability Detection Test Results
- SRP-1 Vulnerability Reporting
- SRP-2.2 Vulnerability Bug Tracking
- SRP-2.6 Root Cause Analysis
- SRP-2.7 Lessons Learned
- SRP-4 Impact Analysis
- SRP-4.3 Return to Appropriate Phase
- SVT-1 Validation Planning
- SRE-3 Report Vulnerabilities
- SRE-5 Patches