SDLA-100

ISA Security Compliance Institute – Security Development Lifecycle Assurance –

ISASecure certification scheme

Version 2.1

June 2020

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
1.2	2014.02.09	Initial version published to http://www.ISASecure.org
1.5	2014.05.27	Change from three to four certification levels, change scope statement of certification program from control systems to systems compliant with ISA 62443, replace ISO/IEC Guide 65 by ISO/IEC 17065, remove reference to ANSI Chartered Test Lab Approval Process 2009, remove event-driven audits, add possibility of recognition for progress before achievement of certification, remove technical readiness assessment
1.8	2018.01.31	Align with approved ANSI/ISA-62443-4-1: revise references, remove discussion of levels of SDLA certification
2.1	2020.06.19	Add option for shorter certification expiration if not all artifacts available, remove recognition for certification pending, change term end users to asset owners and add roles for integration and maintenance service providers, replace EDSA by CSA

Contents

FOREWORD

This is one of a series of documents that defines ISASecure certification for supplier control systems development lifecycle processes, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). This is the highest level document that describes the overall certification scheme and the scope for all other related documents. A description of the ISASecure program and the current list of documents related to ISASecure SDLA (Security Development Lifecycle Assurance), as well as other ISASecure certification programs, can be found on the web site http://www.ISASecure.org.

1 Scope

This document provides an overview of the operation of the ISASecure SDLA (Security Development Lifecycle Assurance) certification program, the roles of all organizations that participate in carrying out the program, and the documents that define these roles as well as the technical aspects of the program. This document provides an overview of the requirements for SDLA certification of a supplier's development lifecycle process; the detailed reference for that topic is the document [SDLA-300] listed in Section 2.

The ISASecure certification 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 supports this goal by offering a common industry-recognized set of development process requirements that drive product security based on the IEC 62443-4-1 standard [IEC 62443-4-1], simplifying product assurance for product suppliers. A supplier can display the ISASecure symbol in association with one or more development organizations within the supplier organization that are certified to meet these requirements. In addition to ISASecure SDLA, ISCI also operates a product certification program for IACS components, called ISASecure CSA (Component Security Assurance) and a product certification program for control systems, called ISASecure SSA (System Security Assurance). The ISASecure CSA and SSA certification schemes (CSA-100 and SSA-100) and other documentation can be found on the web site http://www.ISASecure.org. The present document describes the relationships between ISASecure SDLA and these other certification programs.

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

2 Normative references

NOTE Section 4.6 provides a diagrammatic and expository overview of the ISASecure SDLA documents and their relationships.

2.1 General

NOTE The following lists all document titles and versions that define SDLA 3.0.0. It is reissued to list any errata subsequently issued for the baseline documents.

[SDLA-102] *SDLA-102 ISCI Security Development Lifecycle Assurance – Baseline document versions and errata for SDLA 3.0.0 specifications,* as specified at http://www.ISASecure.org

2.2 Accreditation

2.2.1 Chartered laboratory operations and accreditation

NOTE The following documents describe how to achieve chartered laboratory status and operate as an ISASecure SDLA certifier.

[SDLA-200] *ISCI Security Development Lifecycle Assurance – ISASecure SDLA Chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[ISASecure-202] *ISCI ISASecure Certification Programs – Application and Contract for Chartered Laboratories*, internal ISCI document

[ISASecure-118] *ISASecure-118 ISCI ISASecure Certification Programs - Policy for transition to SDLA 3.0.0*, as specified at http://www.ISASecure.org

2.3 ISASecure symbol and certificates

NOTE The following document describes the ISASecure symbol and certificates and how they are used for the ISASecure SDLA program.

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

[SDLA-205] *ISCI Security Development Lifecycle Assurance – Certificate Document Format,* as specified at http://www.ISASecure.org

2.4 Technical specifications

NOTE 1 This section includes the specifications that define technical criteria for evaluating a supplier's development lifecycle process for ISASecure SDLA certification.

NOTE 2 The following document is the overarching technical specification for ISASecure SDLA certification.

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

[SDLA-303] *ISCI Security Development Lifecycle Assurance - Sample Report*, available on request to ISCI

NOTE 3 The following document provides the detailed technical evaluation criteria for an ISASecure SDLA certification of a supplier organization's security development lifecycle process against the standard [IEC 62443-4-1] .The document also provides the technical evaluation criteria for the Security Development Artifacts element (SDA) of an ISASecure CSA or SSA product certification.

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

2.5 External references

External references are documents that are used by the ISASecure SDLA program but maintained outside of the ISASecure program.

2.5.1 IACS security standards

NOTE 1 Section 4.4 describes the relationship of ISASecure SDLA to the 62443 series standards.

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

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

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

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

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

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

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

2.5.2 International standards for certification programs

NOTE The following international standards apply to the ISASecure SDLA certification processes.

[ISO/IEC 17065] ISO/IEC 17065, "*Conformity assessment - Requirements for bodies certifying products, processes, and services*", September 15, 2012

2.5.3 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure chartered laboratory accreditation process. The transition timeline to the later 2017 version of ISO/IEC 17011 below is defined by ISO/ILAC policy.

[ISO/IEC 17011 2004] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", 01 September 2004

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", November 2017

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
for ISASecure certification programs, assessment and recognition process via which an organization is granted chartered laboratory status

3.1.2
accreditation body
third party that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out a specific conformity assessment

3.1.3
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.

3.1.4
asset owner
individual or company responsible for one or more IACS

NOTE 1 Used in place of the generic term end user to provide differentiation.

NOTE 2 This includes the components that are part of the IACS.

NOTE 3 In the context of this document, an asset owner also includes the operator of the IACS.

3.1.5
certificate
document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

NOTE For ISASecure SDLA, there are certificates for certified development organizations and chartered laboratories.

3.1.6
certification
third party attestation related to products, processes, or persons that conveys assurance that specified requirements have been demonstrated.

NOTE Here, this refers to either a successful authorized evaluation of a product or a process to ISASecure criteria. This outcome permits the product supplier or organization performing the process to advertise this achievement in accordance with certification program guidelines.

3.1.7
certification scheme
overall definition of and process for operating a certification program

3.1.8
certified development process
well-defined supplier development process that has undergone an evaluation by a chartered laboratory, has met the ISASecure SDLA criteria, has been granted certified status by the chartered laboratory, and has maintained this status

3.1.9
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.

3.1.10
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

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

3.1.11
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

3.1.12
conformity assessment
demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

3.1.13
conformity assessment body
body that performs conformity assessment services and that can be the object of accreditation

NOTE This is an ISO/IEC term and concept. For ISASecure certification programs, the conformity assessment body is a chartered laboratory.

3.1.14
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.15
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.

3.1.16
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.

3.1.17
host device
general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

3.1.18
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

3.1.19
network device
device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

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

3.1.20
pass
meet the criteria for passing an ISASecure evaluation as defined within the technical ISASecure specifications

3.1.21
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).

3.1.22
provisional chartered status
interim, temporary recognition status granted by ISCI during which a chartered laboratory is authorized to perform evaluations and grant ISASecure certifications

NOTE ISCI grants provisional chartered status for ISASecure SDLA when an SDLA accreditation body has assessed all requirements as passing, but has not yet formalized the accreditation of the chartered laboratory.

3.1.23
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.

3.1.24
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

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

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

3.1.25
supplier
organization that is responsible for compliance of a product or development process with ISASecure requirements

3.1.26
symbol
graphic or text affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.27
version (of a development lifecycle process)
well defined documented release of a development lifecycle process, typically identified by a release number that identifies the document release that describes that process

3.1.28
version (of ISASecure certification)
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 SDLA 2.6.1

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(s)
IAF	International Accreditation Forum
IEC	International Electrotechnical Commission
ILAC	International Laboratory Accreditation Cooperation
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
PLC	programmable logic controller
SCADA	supervisory control and data acquisition
SDA	security development artifacts
SDL	security development lifecycle
SDLA	security development lifecycle assurance
SIS	safety instrumented system
SSA	system security assurance

4 ISASecure SDLA certification program

4.1 Scope of evaluation

ISASecure SDLA is a certification program that applies to the development lifecycle processes of suppliers for control system products. An SDLA certification is granted for:

- a named development organization or organizations
- a specific version of a named, documented development lifecycle process under version control that is used by that organization(s).

The documented process itself shall specify:

- whether it applies to development of components, systems or both; and
- the scope of products to which the organization applies the process (which may be all products).

In order to carry out an ISASecure SDLA certification, a certifier:

1. evaluates the specific documented version of the organization's process to assess whether it meets the requirements stated in the SDLA specification; and
2. reviews representative artifacts to verify that each ISASecure SDLA requirement is being followed for products under the scope of the process.

The supplier provides a list of products for which such artifacts are available, for the various requirements. The certifier may select from among these to review.

If some aspects of the process are fully in place but have not yet been executed, the certifier can grant certification for a limited time period based upon a review of the development organization's readiness to execute them, as specified in [SDLA-300].

4.2 Certified development lifecycle processes

A supplier whose development lifecycle process has been evaluated under the ISASecure SDLA certification program and shown to meet these technical criteria may display the ISASecure symbol and a certificate granting certification, in accordance with program procedures. A certification references a 3-digit certification version that identifies the set of ISASecure specifications used for the certification. For example, the ABC Company development process might be certified to ISASecure SDLA 2.6.1.

The program defines an expiration period for ISASecure SDLA certification, as well as actions required to maintain the certification beyond this period, i.e. extend the expiration date.

Subject to permission of each organization, ISCI will post on its web site http://www.ISASecure.org, the names of organizations that hold an SDLA certification for their development lifecycle process.

4.3 Relationship of the SDLA program to ISASecure product certification programs

A development organization that holds an ISASecure SDLA process certification thereby meets the SDLPA (Security Development Lifecycle Process Assessment) evaluation element required to achieve ISASecure certification for their products. Thus, the SDLA certification program provides a method for a supplier to undergo an SDLPA evaluation once, such that it can apply toward all product certifications.

The supplier may at their option apply concurrently for both ISASecure SDLA process certification and ISASecure certification for a specific product, in which case product security artifacts may serve as evidence toward both certifications.

These topics are covered in greater detail in the documentation for ISASecure product certification programs.

4.4 Relationship of the SDLA program to ANSI/ISA/IEC 62443

A goal for the ISASecure certification programs is to offer a compliance program for the ANSI/ISA/IEC 62443 series of standards, which address security for IACS.

The ISASecure SDLA process certification is a conformance program for the approved standard "IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements.” ANSI/ISA has published this standard as [ANSI/ISA- 62443-4-1].

The standard [IEC 62443-1-1] establishes terminology and concepts that apply for the overall 62443 series of standards. Definitions for terms will be published in the technical report currently under development: “ISA TR 62443-1-2 Security for industrial automation and control systems - Master glossary of terms and abbreviations."

4.5 Organizational roles

The following organizations participate in the ISASecure SDLA program. A term in parentheses following a description indicates the term used for this role in [ISO/IEC 17065].

- **Asset owners** define procurement criteria and acceptable risk tolerance for control system solutions, and approve the system integrator’s defense in depth model (technical and organizational capabilities) and rationale, which may rely upon certified components and systems. Certified components and systems in turn are developed and maintained under an SDLA-certified process. An entity may assume the role of an asset owner and a service provider (for integration and/or maintenance).

- **Integration service providers** may use component and system certification information as a method for identifying components and systems to be procured as part of an IACS solution. SDLA certification is among the prerequisites to component and system certification; application of [IEC 62443-4-1] practices as verified by SDLA certification is intended to provide confidence that the component or system has security commensurate with its expected level of risk throughout the product’s life-cycle.

- **Maintenance service providers** may use product certification information, which implies an underlying SDLA certification, to evaluate how a product developer’s SDL and user documentation required by the SDL, will support their site hardening, event management, and decommissioning processes.

- **Product suppliers** apply for certification of their secure product development lifecycle processes.

- **Chartered SDLA laboratories** accept applications from suppliers for process certification, evaluate processes, and are authorized to grant SDLA certifications (conformity assessment body).

- **ISCI** defines, maintains and manages the overall ISASecure SDLA certification program, interprets the ISASecure specifications and maintains a web site for publishing program documentation, as well as a list of chartered SDLA laboratories, ISASecure certified supplier development lifecycle processes and ISASecure certified products.

- **ASCI** (Automation Standards Compliance Institute)**,** as the legal entity representing ISCI, grants chartered SDLA laboratory status to applicant organizations based on successful accreditation to criteria defined by ISCI.

- **SDLA accreditation bodies** evaluate candidates for chartered SDLA laboratory status and determine if they meet program accreditation criteria (accreditation body).

ISCI is organized as an interest area within ASCI, a not-for-profit 503 (c) (6) corporation owned by ISA (International Society of Automation). Descriptions of the governance and organizational structure for ASCI are found on the ISASecure website: http://www.ISASecure.org.

An SDLA accreditation body will be an organization recognized by IAF/ILAC.

Information related to ISASecure evaluations is private to chartered laboratories performing these evaluations, and is not disclosed to ASCI/ISCI, except as explicitly permitted by the supplier under evaluation or for cause in ASCI/ISCI’s role as manager of the certification program.

4.6 Certification program documentation

4.6.1 Overview of documentation

Figure 1 shows the documents that define the ISASecure SDLA certification program. An arrowhead represents a referential dependency of a document on the contents of another document. Refer to Section 2 for the detailed listing of these documents.

NOTE The figure depicts all documents in Section 2 with the exception of the policy document [ISASecure-118], application form [ISASecure-202], document version and errata list [SDLA-102], and certificate form [SDLA-205].

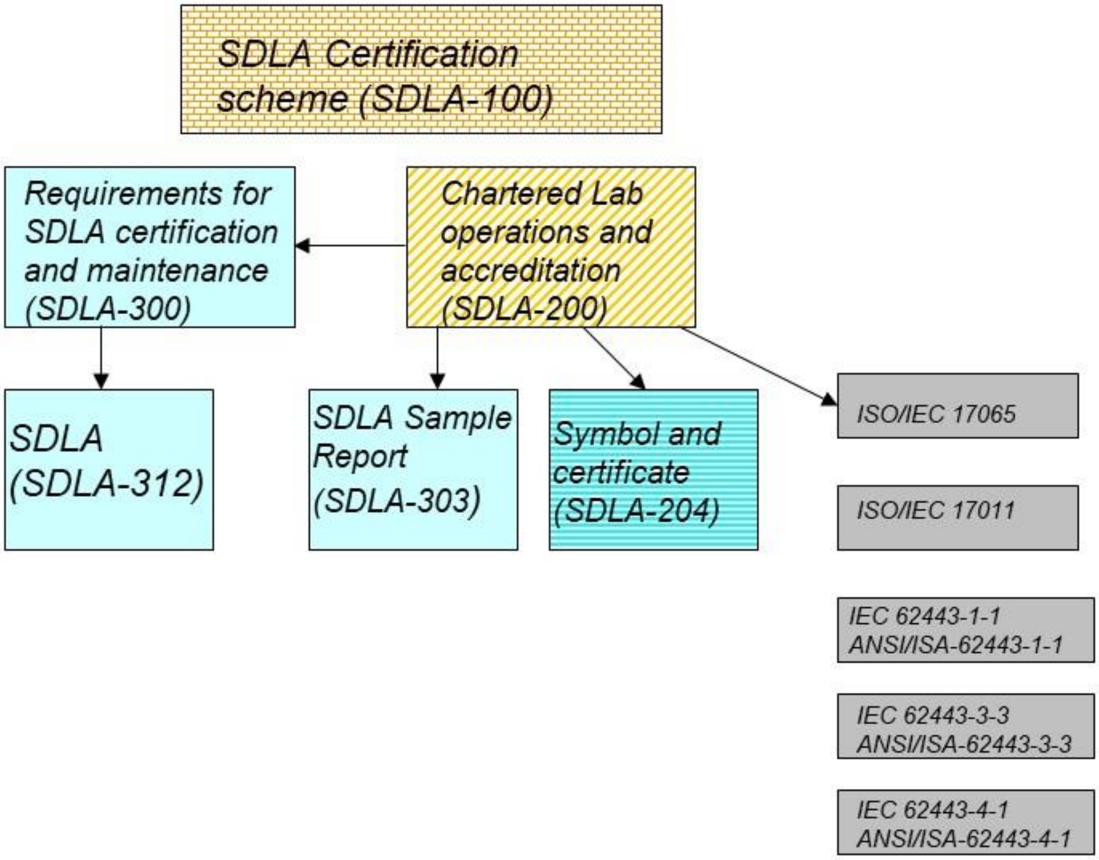
SDLA Certification scheme (SDLA-100)
Requirements for SDLA certification and maintenance (SDLA-300)
Chartered Lab operations and accreditation (SDLA-200)
SDLA (SDLA-312)
SDLA Sample Report (SDLA-303)
Symbol and certificate (SDLA-204)
ISO/IEC 17065
ISO/IEC 17011
IEC 62443-1-1 ANSI/ISA-62443-1-1
IEC 62443-3-3 ANSI/ISA-62443-3-3
IEC 62443-4-1 ANSI/ISA-62443-4-1

Figure 1 - ISASecure SDLA Documents

There are five major categories of ISASecure SDLA program documents:

- **Technical specifications**, shown with no pattern in light blue, that describe the technical criteria applied to determine whether a process will be certified
- **Accreditation**, shown in gold diagonal stripe, that describes how an organization can become a chartered SDLA laboratory
- **Symbol and certificate**, shown in blue horizontal stripe, covers the topic of proper usage of the ISASecure symbol and certificate

- **Structure,** shown in an orange brick pattern, used to describe an overall certification program. The present document falls in this category.

- **External references**, shown with no pattern in dark grey, are documents that apply to the ISASecure program but are maintained outside of the program.

The following sections describe all documents in each category in further detail.

4.6.2 Technical specifications

The brief document [SDLA-300] *ISCI SDLA - Requirements for ISASecure certification and maintenance of certification,* defines at a high level the criteria for supplier development lifecycle process certification. Simply stated, the criteria are for the supplier to pass an SDLA evaluation as defined in [SDLA-312], and to maintain this certification over time. [SDLA-300] also specifies certification criteria and procedures for the case in which some aspects of a development organization's SDL process are fully in place but have not yet been executed on a specific product.

The SDLA specification [SDLA-312] defines the technical evaluation criteria required for a process to pass SDLA. (This same document includes requirements on the artifacts generated by these methods which are used for ISASecure product certifications.)

These documents are used by:

- asset owners and service providers (for integration or maintenance), for the general understanding that SDLA certification provides assurance that components or systems subject to a supplier's SDLA certified process, are developed and maintained in accordance with IEC 62443-4-1 requirements, as stated in 4.4 of the present document

- suppliers, to understand the criteria against which their processes will be evaluated and how to maintain certification

- chartered laboratories, to define evaluation processes and criteria

- SDLA accreditation bodies, as the end reference for technical readiness assessment requirements when evaluating candidate organizations for chartered laboratory status.

The SDLA evaluation report requirements embodied in the sample evaluation report [SDLA-303] will be followed by chartered laboratories. This document provides asset owners, system integrators, and system suppliers with an understanding of the type of information that will be provided to suppliers following all ISASecure SDLA evaluations.

4.6.3 Accreditation

ISASecure SDLA chartered laboratories implement the technical aspects of the certification program. The accreditation document defines how they obtain this role.

[SDLA-200] *ISCI SDLA – ISASecure SDLA chartered laboratory operations and accreditation* describes the accreditation criteria and process that an organization will follow to become a chartered laboratory. To be granted full status as a chartered laboratory for the ISASecure SDLA program, a laboratory shall attain the following internationally recognized accreditation, performed by an SDLA accreditation body:

- accredited to ISO/IEC 17065, with technology scope of accreditation covering ISASecure SDLA certification.

ACSI grants provisional recognition to a chartered laboratory when an accreditation body informally reports to ISCI that the candidate organization has met all requirements for accreditation. Full chartered laboratory status is granted when the accreditation body formally grants the above accreditation to the candidate organization.

[SDLA-200] details the requirements for both provisional and full chartered laboratory status, including compliance with the above international standard for the ISASecure SDLA program. This document is used by:

- organizations that are candidate chartered laboratories, to understand the accreditation requirements and process, as well as ongoing requirements on their operations
- SDLA accreditation bodies, as the source for program specific requirements for the 17065 accreditation described above.

4.6.4 Symbol and certificate

The document [SDLA-204] *ISCI SDLA – Instructions and Policies for Use of the ISASecure Symbol and Certificate* describes the format and correct usage for the ISASecure symbol and certificate under the SDLA program. The ISASecure symbol is used by a supplier to indicate a certified development process. It is also used by a chartered laboratory to indicate its authorized participation in the ISASecure SDLA program.

Two types of ISASecure certificates are issued under the SDLA program: for certified processes and chartered laboratories.

The documents in this category as they apply to certified supplier processes are used by:

- suppliers that are candidates for SDLA certification, to understand requirements for symbol and certificate usage
- asset owners and service providers, to understand the meaning of a symbol or certificate displayed by a supplier
- chartered laboratories, to create certificates for certified processes
- chartered laboratories, to monitor for correct use of the symbol and SDLA certificates by client suppliers as required by [SDLA-200].

These documents as they apply to chartered laboratories are used by:

- chartered laboratories to understand requirements for symbol and certificate usage
- suppliers that are candidates for SDLA certification, to understand the meaning of the symbol or certificate displayed by a chartered laboratory
- ASCI/ISCI, to create certificates for chartered laboratories
- ISCI, to monitor for correct use of the symbol and certificates for chartered laboratories.

4.6.5 Structure

The present document [SDLA-100] is in the Structure category. [SDLA-100] is a publicly available reference to the structure of the overall ISASecure SDLA certification program.

4.6.6 External references

[ISO/IEC 17065] is an international standard that contains requirements for operating a product, process, or service certification program.

[ISO/IEC 17011] is an international standard that applies to the accreditation process itself. Thus, this document is used by SDLA accreditation bodies and ASCI to define their accreditation operations for the ISASecure SDLA certification program.

Figure 1 includes three approved standards from the 62443 series. The standard [IEC 62443-1-1] covers terminology and concepts for the 62443 series of standards.

The standard "IEC 62443-4-1*Security for industrial automation and control systems: Part 4-1: Secure product development lifecycle requirements*" provides the list of requirements to which SDLA certification assesses conformance. The document [SDLA-312] lists these requirements and defines methods for assessing conformance toward ISASecure SDLA certification.

The standard "IEC 62443-3-3 *Security for industrial automation and control systems Part 3-3: System security requirements and security levels"* defines capability security levels for industrial control systems. [SDLA-312] specifies that validation of conformance to the IEC 62443-4-1 requirement DM-4 "Addressing security-related issues," depends upon the capability security level of products under development.