

SDLA-100

ISA Security Compliance Institute — Security Development Lifecycle Assurance — ISASecure certification scheme

Version 1.5

May 2014

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.

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

Contents

1	Scope	6
2	Normative references	6
2.1	Accreditation	6
2.2	ISASecure symbol and certificates	6
2.3	Technical specifications	6
2.4	External references	7
3	Definitions and abbreviations	7
3.1	Definitions	7
3.2	Abbreviations	10
4	ISASecure SDLA certification program	10
4.1	Scope of evaluation	10
4.2	Certified development lifecycle processes	11
4.3	Relationship of the SDLA program to ISASecure product certification programs	11
4.4	Relationship of the SDLA program to ISA 62443	11
4.5	Organizational roles	11
4.6	Certification program documentation	12

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, simplifying product assurance for product suppliers. A supplier can display the ISASecure symbol in association with one or more development groups within the supplier organization that are certified to meet these requirements. In addition to ISASecure SDLA, ISCI also operates a product certification program for embedded devices, called ISASecure EDSA (Embedded Device Security Assurance) and a product certification program for control systems, called ISASecure SSA (System Security Assurance). The ISASecure EDSA and SSA certification schemes (EDSA-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 ISA 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 Accreditation

2.1.1 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

2.2 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>

2.3 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. The document also provides the technical evaluation criteria for the Security Development Artifacts element (SDA) of an ISASecure SSA product certification. The bibliography for [SDLA-300] provides a list of the sources from which these requirements were derived

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

2.4 External references

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

2.4.1 IACS security standards

NOTE Section 4.4 describes the relationship of ISASecure SDLA to this approved standard as well as to ISA 62443 series standard under development, listed in the bibliography.

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

2.4.2 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

2.4.3 International standards for accreditation programs

NOTE The following international standard applies to the ISASecure chartered laboratory accreditation process.

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

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 or CRT 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 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.

3.1.5 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.

3.1.6 certification level (for SDLA certification)

number associated with an ISASecure SDLA certification, where a higher number indicates that a more rigorous set of security development lifecycle process evaluation criteria has been met by the supplier

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 conformity assessment

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

3.1.12 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.

3.1.13 control system

hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.14 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.

3.1.15

end user

organization that purchases, uses or is impacted by the security of control system products

3.1.16

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

3.1.17

pass

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

3.1.18

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.

3.1.19

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.

3.1.20

supplier

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

3.1.21

symbol

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

NOTE An earlier term for symbol is "mark."

3.1.22

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

3.1.23

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.

ASCI	Automation Standards Compliance Institute
CRT	communication robustness testing
DCS	distributed control system
EDSA	embedded device security assurance
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
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)
- a certification level of 1, 2, 3, or 4.

The four certification levels for a process offer increasing levels of development lifecycle security assurance. These certifications are called ISASecure SDLA Level 1, ISASecure SDLA Level 2, ISASecure SDLA Level 3, and ISASecure SDLA Level 4.

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 to a particular certification level, 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.

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, Level 2.

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. The program also defines procedures for certified organizations to obtain certification to higher certification levels. In addition, the program offers formal recognition for organizations that have made significant progress toward certification.

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

4.3 Relationship of the SDLA program to ISASecure product certification programs

A supplier that holds an ISASecure SDLA process certification at an appropriate certification level thereby meets the SDLA evaluation element required to achieve ISASecure certification for their products. A supplier applying for a product certification that does not hold an SDLA process certification at the appropriate level, will undergo an SDLA evaluation at this level as a part of the ISASecure product evaluation itself. Thus the SDLA certification program provides a method for a supplier to undergo an SDLA 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 ISA 62443

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

In the future, the ISASecure SDLA process certification requirements and certification levels will be revised as necessary to align with the requirements and level concepts in the planned standard ISA 62443-4-1 "Security for industrial automation and control systems – Product development requirements." This standard is under development.

The approved standard ISA 62443-1-1 establishes terminology and concepts that apply for the overall series of standards.

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 Guide 65].

- **End users** define procurement criteria for control system products, and may require an ISASecure certification for a product or supplier development lifecycle process, at a particular certification level
- **Suppliers** apply for certification of their development lifecycle processes
- **Chartered SDLA laboratories** accept applications from suppliers for process certification, evaluate processes, and are authorized to grant SDLA certifications and formal pre-certification recognition to supplier development organizations (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 application form [ISASecure-202] and certificate form [SDLA-205].

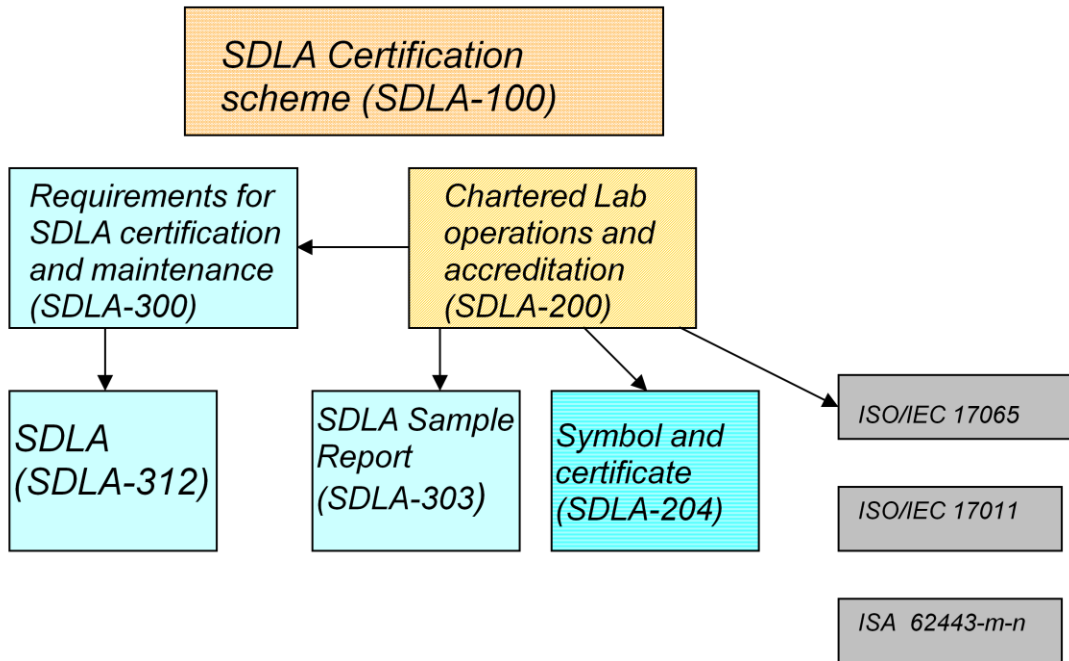


Figure 1 - ISASecure SDLA Documents

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/recognition**, 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.

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. This document also defines the criteria for formal recognition by ISCI of an organization that has achieved significant progress toward certification. The SDLA specification [SDLA-312] defines the technical evaluation criteria required for a process to pass SDLA, for each certification level. (This same document includes requirements on the artifacts generated by these methods which are used for ISASecure product certifications.)

These documents are used by:

- end users, to understand the meaning of various levels of ISASecure SDLA certification
- 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 end users 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/recognition

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. It also provides a transition time line permitted from Guide 65 to 17065, for organizations applying to be SDLA chartered laboratories, that have previously been accredited to Guide 65 as chartered laboratories under another ISASecure certification 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
- end users, 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.

In Figure 1, the notation ISA 62443-*m-n* refers to the series of ISA 62443 standards. One of these standards related to SDLA process certification is currently approved, which is ISA 62443-1-1 covering terminology and concepts for the 62443 series. Although the ISASecure specifications are self-contained, the ISASecure program intent is to provide a conformance program for ISA 62443, as described in 4.4. Therefore the ISASecure specifications are closely related to the ISA 62443 standards. For example, ISA 62443-1-1 defines the concepts of zones and security levels used to determine appropriate SDLA certification levels as described in 4.4.

The approved standard ISA 62443-1-1 is listed in the normative references section. The standard ISA 62443-4-1 "*Security for industrial automation and control systems – Product development requirements*" is under development as of the publication of this document. Therefore it is listed in this document as a bibliographic reference rather than a normative reference. It is the intent going forward to align ISASecure SDLA certification with the approved version of [ISA 62443-4-1].

BIBLIOGRAPHY

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