SSA-200

ISA Security Compliance Institute — System Security Assurance –

ISASecure SSA chartered laboratory operations and accreditation

Version 1.2

February 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, INFORMATON, 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

Contents

List of requirements from other ISASecure SSA specifications

List of tables

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 systems and ISASecure Security Development Lifecycle Assurance (SDLA) which addresses control system supplier development processes. This specification is one of the series of documents that describes requirements for ISASecure SSA certification. The current list of documents related to ISASecure certification programs can be found on the web site http://www.ISASecure.org.

1 Scope

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). An organization that performs evaluations and grants certifications under the ISASecure SSA (System Security Assurance) program for control systems is referred to as an *ISASecure SSA chartered laboratory*, or (more briefly) a *chartered laboratory*. This document specifies the criteria and processes that define:

- Requirements on the operations of a chartered laboratory (Section 6); and
- How a chartered laboratory may begin and continue ISASecure SSA system certification operations (Section 7).

ISCI has based its certification program approach on:

- International standards for conformity assessment programs
- General specifications for operation of ISA compliance programs
- Specifications developed for the ISASecure SSA program.

This document provides a complete reference to these sources, and details ISASecure SSA program-specific requirements for compliance with applicable general specifications and standards.

ISCI also has developed certification programs for:

- embedded devices, the ISASecure EDSA program (Embedded Device Security Assurance)
- supplier development process for control systems and components, the ISASecure SDLA program (Security Development Lifecycle Assurance).

The separate documents EDSA-200 *ISASecure EDSA chartered laboratory operations and accreditation* and SDLA-200 *ISASecure SDLA chartered laboratory operations and accreditation* address these same topics as they relate to chartered laboratories that perform ISASecure EDSA and SDLA certifications, respectively.

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

2 Normative references

2.1 General

NOTE The following is the highest level document that describes the ISASecure SSA certification program for control systems.

[SSA-100]] ISCI System Security Assurance – ISASecure Certification Scheme, as specified at http://www.ISASecure.org

2.2 Accreditation/recognition

2.2.1 Chartered and CRT laboratory operations and accreditation

NOTE The following document can be tailored for chartered laboratories performing EDSA, SSA or SDLA certifications, or any combination of these.

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

[EDSA-206] *ISCI Embedded Device Security Assurance – ISASecure EDSA CRT laboratory operations and accreditation,* as specified at http://www.ISASecure.org

2.2.2 CRT tool recognition program

NOTE The following documents describe how to attain ISASecure recognition for a tool used to carry out communication robustness testing (CRT) and network stress testing (NST), which are two aspects of the system robustness testing performed for an SSA evaluation. CRT is also a requirement for ISASecure EDSA certification for an embedded device. The same tool recognition process applies for all of these applications of the tool.

[EDSA-201] *ISCI Embedded Device Security Assurance –Recognition process for communication robustness testing tools,* as specified at http://www.ISASecure.org

[EDSA-203] *ISCI Embedded Device Security Assurance - Application and Contract for CRT Tool Recognition,* internal ISCI document

2.3 ISASecure symbol and certificates

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

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

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

2.4 Technical specifications

NOTE This section includes the specifications that define technical criteria for evaluating a system for ISASecure SSA certification.

2.4.1 General technical specifications

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

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

[SSA-301] *ISCI System Security Assurance – Maintenance of ISASecure Certification,* as specified at http://www.ISASecure.org

[SSA-303] *ISASecure SSA Sample Report*, available on request to ISCI

2.4.2 Specifications for certification elements

NOTE 1 The following document provides the technical evaluation criteria for the System Robustness Testing element of an SSA evaluation.

[SSA-310] *ISCI System Security Assurance – Requirements for system robustness testing,* as specified at http://www.ISASecure.org

NOTE 2 The following document provides the technical evaluation criteria for the Functional Security Assessment element of an SSA evaluation.

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

NOTE 3 The following document provides the overall technical evaluation criteria for the Security Development Artifacts element of an SSA product evaluation. [SDLA-312] is referenced by [SSA-312] and also provides the technical evaluation criteria for an ISASecure assessment of a supplier's security development lifecycle process.

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

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

NOTE 4 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier security development lifecycle processes. [SDLA-100] also lists all other documentation for the SDLA program.

[SDLA-100] ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme, as specified at http://www.ISASecure.org

NOTE 5 The following document describes evaluation of a modified embedded device under ISASecure EDSA certification criteria, where a prior version of the device was certified. These requirements apply when certification evidence for a prior version of an embedded device component of a system is available toward an SSA certification.

[EDSA-301] *ISCI Embedded Device Security Assurance – Maintenance of ISASecure Certification,* as specified at http://www.ISASecure.org

2.4.3 Vulnerability identification testing specifications

NOTE The following document describes the policy parameter values used to perform Vulnerability Identification Testing (VIT) for a specific system. VIT is a sub element of System Robustness Testing.

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

2.4.4 CRT Specifications

NOTE The first document in this list is the overarching technical specification that defines how tests are carried out for both ISASecure EDSA and for several aspects of SSA SRT (System Robustness Testing). It applies for ISASecure SSA to the extent described in [SSA-312]. The list of protocol-specific ISASecure EDSA technical test specifications that follow, refer to [EDSA-310] for requirements that are common across all protocols.

[EDSA-310] *ISCI Embedded Device Security Assurance – Common requirements for communication robustness testing of IP based protocol implementations,* as specified at http://www.ISASecure.org

[EDSA-401] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols,* as specified at http://www.ISASecure.org

[EDSA-402] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4,* as specified at http://www.ISASecure.org

[EDSA-403] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-404] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-405] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

[EDSA-406] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

2.5 External references

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

2.5.1 IACS security standards

NOTE [SSA-100] describes the relationship of ISASecure to these approved standards as well as to ISA 62443 series standards under development.

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

[ISA 62443-3-3] ANSI/ISA−62443−3−3, *Security for industrial automation and control system: Part 3-3, System security requirements and security levels*

2.5.2 International standards for certification programs

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

[ISO/IEC Guide 65] ISO/IEC Guide 65, "*General Requirements for Bodies Operating Product Certification Systems*", 1996

[IAF Guide 65 Guidance] IAF Guidance on the Application of ISO/IEC Guide 65:1996**,** "*General Requirements for Bodies operating Product Certification Systems"**,** IAF GD 5:2006 Issue 2, Application date: 8 December 2007

[ISO/IEC 17025] ISO/IEC 17025, "*General requirements for the competence of testing and calibration laboratories"**,** 15 December 1999

2.5.3 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

2.5.4 ASCI operations

NOTE Some evaluation criteria in the following document are used for ISASecure chartered laboratory accreditation.

[ASCI Lab] *ASCI Chartered Testing Laboratory 2009 Approval Process*, as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accreditation
third party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks

NOTE For ISASecure certification programs, accreditation is an assessment and recognition process via which an organization is granted chartered laboratory status 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 specific conformity assessment

3.1.3
applicant
organization that has submitted a product or process to a chartered laboratory for evaluation for ISASecure certification

3.1.4
capability security level
security level that a component or system can provide when properly configured

NOTE This type of security level states that a particular component or system is capable of meeting a target security level natively without additional compensating countermeasures when properly configured and integrated.

3.1.5
certifier
chartered laboratory, which is an organization that is qualified to certify products or supplier devellopment 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.

3.1.6
chartered laboratory
organization chartered by ASCI to evaluate products and/or 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.

3.1.7
conformity assessment body
body that performs conformity assessment services and that can be the object of accreditation

NOTE Examples are a laboratory, inspection body, product certification body, management system certification body and personnel certification body. This is an ISO/IEC term and concept.

3.1.8
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.9
CRT evidence submission
set of test evidence for an embedded device submitted by a CRT laboratory to a chartered laboratory on behalf of an applicant for ISASecure EDSA or SSA certification

3.1.10
CRT laboratory
organization authorized by ASCI to perform communication robustness testing for embedded devices and submit results to a chartered laboratory toward an ISASecure EDSA or SSA certification

3.1.11
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.

3.1.12
evidence impact assessment
identification of that portion of the evidence from the certification evaluation of a product, which may be applied toward the certification of a modified version of the product, and of those aspects of the evaluation which must be performed on the modified product and new evidence created

3.1.13
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

3.1.14
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.

3.1.15
security zone
grouping of logical or physical assets that share common security requirements

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

3.1.16
symbol
graphic affixed or displayed to designate that ISASecure certification has been achieved

NOTE An earlier term for symbol is “mark.”

3.1.17
system
control system

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

3.1.18
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
ARP	address resolution protocol
BS	Bachelor of Science
CE	computer engineering
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CRT	communication robustness testing
CS	computer science
DCS	distributed control system
EDSA	embedded device security assurance
FSA-E	functional security assessment for embedded devices
FSA-S	functional security assessment for systems
IACS	industrial automation and control system(s)
IAF	International Accreditation Forum
ICMP	Internet control message protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet engineering task force
ILAC	International Laboratory Accreditation Cooperation
IP	Internet protocol
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
NA	not applicable
NST	network stress testing
OS	operating system
PLC	programmable logic controller
SDA-S	security development artifacts for systems
SDLA	security development lifecycle assurance, security development lifecycle assessment
SIS	safety instrumented system
SRT	system robustness testing
SSA	system security assurance
SY	system
SUT	system under test
TCP	transmission control protocol
TD	test device
UDP	user datagram protocol
VIT	vulnerability identification testing

4 Background

4.1 Technical ISASecure SSA certification elements

ISASecure SSA is a certification program for control systems, where a control system product is considered to be within the scope of this program if it satisfies all of the following criteria:

- The control system consists of an integrated set of components and includes more than one device.
- The control system is available from and supported as a whole by a single supplier, although it may include hardware and software components from several manufacturers.
- The supplier has assigned a unique product identifier to the control system which the supplier uses in the marketplace to refer to the integrated set of components as a whole.
- The system product is under configuration control and version management.

In order to obtain ISASecure SSA certification, a supplier must pass a security development lifecycle process evaluation equivalent to that defined under the ISASecure SDLA development process certification described in the reference [SDLA-100]. Specifically, in order for a system product from a supplier to achieve ISASecure SSA certification, either:

- The supplier must hold an ISASecure SDLA certification; or
- The supplier passes an equivalent SDLA evaluation of their development process as part of the SSA evaluation itself.

A supplier may apply for ISASecure SSA and SDLA certifications in parallel.

ISASecure SSA certification for systems has four additional elements:

- Security Development Artifacts for systems (SDA-S);
- Functional Security Assessment for systems (FSA-S);
- Functional Security Assessment for embedded devices (FSA-E); and
- System Robustness Testing (SRT).

SDA-S examines the artifacts that are the outputs of the supplier's security development processes as they apply to the system to be certified. FSA-S examines the security capabilities of the system. FSA-E examines the security capabilities of any embedded devices that are components of the system, recognizing that in some cases security functionality is provided by other system components. SRT has three major elements - Vulnerability Identification Testing (VIT), Communication Robustness Testing (CRT) and Network Stress Testing (NST). VIT scans all components of a system for the presence of known vulnerabilities. CRT and NST verify that the system adequately maintains essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions) at its network interfaces.

A system submitted for certification is comprised of one or more security zones. The supplier identifies a desired capability security level for each zone. The FSA-S evaluation is applied to each zone; required security capabilities will differ based upon the level identified for a zone. Similarly, requirements for development process artifacts evaluated under SDS-S are more stringent for components in higher security level zones of the system. The ISASecure SSA certificate for a system will name the security zones and security levels to which they have been certified.

If the system has a component embedded device that is ISASecure EDSA certified, that certification may be leveraged to meet CRT and FSA requirements for SSA certification of the overall system, to the extent specified in [SSA-300].

In addition to requirements for initial certification, ISASecure SSA specifies requirements for maintaining certification when a certified system and/or ISASecure criteria are modified, as described in [SSA-301].

4.2 ISASecure SSA certification program implementation

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

ASCI ISASecure SSA chartered laboratories are organizations that are accredited to evaluate systems under the ISASecure SSA program. ASCI grants accredited laboratories the right to process ISASecure SSA certifications for systems on its behalf and issue certificates for systems meeting the SSA certification requirements. System certification is determined based upon tests, functional audits and process audits, which measure adherence to the ISASecure SSA requirements.

Evaluations for all SSA certification elements described in 4.1 are conducted directly by the chartered laboratory or its subcontractors, with the possible exception of the CRT element of SRT for embedded devices. The chartered laboratory shall directly conduct CRT for all types of system components with the possible exception for embedded device components of the system presented for certification. CRT test for such embedded device components may be conducted by a separate accredited organization called a CRT laboratory, which submits test evidence to the chartered laboratory for evaluation. However, a chartered laboratory must be qualified and prepared to conduct CRT for all types of components, including embedded devices.

The lists of ASCI ISASecure SSA chartered laboratories and CRT laboratories are posted on the ISCI website at http://www.ISASecure.org. At the request of system suppliers, systems that are issued certifications are registered on this same ISCI website.

The ISASecure EDSA and SSA certification programs require the use of a test tool for CRT and NST. A tool is used by chartered laboratories for CRT and NST, by CRT laboratories to perform CRT and by device and system suppliers in preparation for certification. CRT/NST test tools must be evaluated for consistency and fairness to ensure that they are appropriate for use by ISASecure test laboratories. ISCI operates a test tool recognition program to support these objectives. The program is described in document [EDSA-201].

In addition, the ISASecure SSA program requires the use of the Nessus® tool (http://www.tenable.com/products/nessus) for performing the VIT element of SRT. Nessus may also be used by suppliers in preparation for certification.

5 Summary of operations and accreditation requirements

ISASecure SSA will operate as an internationally recognized certification program. To meet this standard, the chartered laboratory operations and accreditation requirements are designed to comply with accepted international standards applicable to product certification and testing.

The operations of ISASecure SSA chartered test laboratories shall be in compliance with the applicable requirements in:

- ASCI Chartered Testing Laboratory 2009 Approval Process [ASCI Lab]
- ISO/IEC Guide 65 [ISO/IEC Guide 65]
- IAF Guidance on the Application of Guide 65 [IAF Guide 65 Guidance]
- ISO/IEC 17025 [ISO/IEC 17025]

The first document in this list applies to ISCI (and all interest area groups that are organized under ASCI). The last three documents are international standards that apply generally to organizations that carry out tests and audits in support of product certification.

This document organizes the requirements from the above documents into a unified set of categories. Where required, it interprets those requirements for ISASecure SSA and adds additional requirements. Of particular note are interpretations for:

- qualifications for chartered laboratory personnel (6.3.2);
- requirements on the certification application process (6.6.2);
- technical criteria for the certification decision (6.10.2);
- complaint appeals (6.5.2);
- publication of certification status (6.6.2); and
- monitoring use of the ISASecure symbol (6.12.2).

Accreditation of a chartered laboratory consists of an assessment of the organization against the general requirements in the above documents and the specific requirements in Section 6 of this document, together with an assessment of technical readiness for performing ISASecure SSA evaluations. Technical readiness assessment is based upon review of laboratory processes and procedures as well as review of artifacts from evaluation activities. To be recognized as a chartered laboratory for the ISASecure SSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC accreditation body:

- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure SSA SRT specifications; and
- accredited to IAF ISO/IEC 65, with technology scope of accreditation covering ISASecure SSA certification.

The laboratory accreditation process consists of two steps. In the first step, an assessor who is qualified with respect to the above two accreditations will complete an evaluation of all accreditation requirements. Provisional chartered status is granted if ISCI's analysis of the assessor's report following this evaluation, shows that the laboratory meets the requirements for formal accreditation defined in 7.1, including those technical readiness criteria in 7.3 that may be verified based upon process and procedure documentation evidence. At this point the accreditation body has not yet formally granted accreditation, which requires a review and approval process internal to the accreditation body.

Once a laboratory has attained provisional chartered status, ASCI grants that laboratory the right to perform system evaluations and grant ISASecure SSA certifications. These rights continue as long as the laboratory receives formal accreditation from an SSA accreditation body in a timely manner (the second step), and maintains this status.

6 Requirements on operations of chartered laboratories

6.1 Overview

This section specifies all requirements on the operation of SSA chartered laboratories. It provides specific interpretations for some of the general requirements in the four source references listed in Section 5, and defines additional requirements that are specific to the ISASecure SSA program. It should be noted that there are duplicate requirements as well as unique requirement contributions in the four source documents listed above.

The requirements on chartered laboratory operations listed in [ASCI Lab] apply to ISASecure SSA as specified in this document. However, the application process described in [ASCI Lab] is not used for

ISASecure SSA chartered laboratories. A candidate organization for chartered laboratory status shall follow the application process in [ISASecure-202] in order to apply to ASCI for chartered laboratory status, and in addition shall follow the application process specified by the accreditation body.

6.2 Management system elements

6.2.1 General requirements

The following requirements shall be implemented by an SSA chartered laboratory. The chartered laboratory may subcontract as defined in these requirements. The subcontracting of the certification decision by the laboratory to another organization is not allowed per ISO/IEC requirements.

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process I. Capability E. Quality Assurance and F. Records, also III Independence*
- ✓ ISO/IEC Guide 65 Section 4
- ✓ IAF Guidance on ISO/IEC Guide 65 Section 4
- ✓ ISO/IEC 17025 Section 4

6.2.2 ISASecure SSA specific requirements

A chartered laboratory shall accept CRT evidence for embedded devices that are components of a system, from a recognized CRT laboratory, toward certification of the system. The chartered laboratory shall define processes for appropriate due diligence on the compliance of this evidence with ISASecure SSA requirements. Before accepting a CRT evidence submission from a CRT laboratory, the chartered laboratory shall verify that this organization is currently recognized as such by ISCI.

The general confidentiality requirement in 4.10.2 of ISO/IEC Guide 65 states that information gained from an evaluation may not be available to a third party without consent of the supplier applying for the certification. This means in particular that neither ASCI nor ISCI shall have access to information generated during ISASecure SSA evaluations, except by permission of the system supplier. ISCI as a matter of course publishes the names of products that have been certified on its web site. This shall be done with permission of the system supplier. An SSA chartered laboratory likewise shall have no rights to information about test status or results from CRT laboratories, except with permission of the system supplier.

The requirement in 4.2.1 of ISO/IEC 17025 for adequate documentation of procedures instructions, etc. shall be interpreted as follows for SRT: Laboratory documentation that provides guidance for SRT shall provide sufficient detail to ensure compliance with the requirements of [SSA-310], when used in conjunction with a recognized CRT tool and the Nessus tool, which are used for the CRT/NST and VIT sub elements of SRT, respectively.

6.3 Personnel

6.3.1 General requirements

Chartered laboratory procedures shall address the general requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I. Capability G. Personnel*
- ✓ ISO/IEC Guide 65 Section 5
- ✓ IAF Guidance on ISO/IEC Guide 65 Section 5
- ✓ ISO/IEC 17025 Section 5.2

6.3.2 ISASecure SSA specific requirements

6.3.2.1 FSA-S/SDA-S auditors

The above general requirements include written descriptions of personnel qualifications for positions related to evaluation of systems. The minimum qualifications that a chartered laboratory sets for auditors that carry out FSA-S and SDA-S shall include those specified in Table 1.

An SDLA development lifecycle process evaluation may be carried out as part of the SSA evaluation. In this case the qualifications for performing that SDLA evaluation SHALL be the same as that for SDA-S below.

Table 1 – FSA-S and SDA-S auditor qualifications

Category of qualification / experience	FSA –S auditor	SDA –S auditor
Formal education	• BS Electrical Engineering OR • BS Computer Engineering (CE) OR • BS Computer Science (CS) OR • BS Chemical Engineering with CE or CS minor OR • Equivalent science or engineering degree	• BS Electrical Engineering OR • BS Computer Engineering OR • BS Computer Science OR • BS Chemical Engineering with CE or CS minor OR • Equivalent science or engineering degree
Professional certification*	• CISA, CISSP or equivalent	• CISA, CISSP or equivalent
Work experience post BS degree	• Min 8 years experience	• Min 8 years experience
Relevant development work experience	• Min 4 year detailed system level product development involvement for IACS OR • Min 4 years of systems integration experience for IACS OR • Min 6 years system level product Test of IACS • Experience includes 2 years with software security-related responsibilities	• Min 4 year software integration experience for IACS AND • Min 2 year involvement with software process improvement activities • Experience includes 2 years with software security-related responsibilities • Experience includes 2 years with technical management responsibilities at the system level
Relevant auditing work experience	• Min 1 year experience performing technical product audit OR 2 years in position in which has been audited on 3 or more products	• Min 1 year experience performing software process audit OR 2 years in position in which software process has been audited on 3 or more products
Relevant industry specific knowledge	• General knowledge of at least two different IACS AND • General knowledge of application of IACS and roles and duties of employees at sites using	• General knowledge of end-end software development life cycle AND • General knowledge of IACS

Category of qualification / experience	FSA –S auditor	SDA –S auditor
	IACS AND • Moderate level knowledge of networking and communication protocols AND • Able to independently read and interpret requirement specifications for IACS products AND • Able to independently read and understand user installation and configuration documents for IACS products AND • Knowledge of methods used to protect communications and detect / prevent communication attacks	architectures
Knowledge of security standards	ISA 62443 Standard plus at least one of: • Common Criteria • ISO/IEC 27001 • IEC 61508	ISA 62443 Standard plus at least one of: • Common Criteria • ISO/IEC 27001 • IEC 61508

*Requirement applies 6 months after ISCI launch of the SSA certification program.

6.3.2.2 CRT/NST Testers

The minimum qualifications that a chartered laboratory sets for individuals that oversee the technical aspects of SSA CRT or NST testing and interpretation of results (including interpretation of CRT evidence submissions from CRT laboratories) shall include those specified in Table 2:

Table 2 – CRT or NST test lead qualifications

Category of qualification / experience	CRT or NST lead
Formal education	• BS Electrical Engineering OR • BS Computer Engineering OR • BS Computer Science OR • BS Chemical Engineering with CE or CS minor OR • Equivalent science or engineering degree OR • 4 years work experience in testing of IACS may be substituted for degree
Work experience post BS degree	• Min 5 years experience
Relevant development work experience	• Min 4 year detailed system level product development involvement for IACS OR • Min 4 years of Systems Integration experience for IACS OR • Min 3 years System Level Product Test for IACS • Experience includes 1 year with software security-related responsibilities • Experience includes 2 years involvement with networking technologies
Relevant test work experience	• Min 1 year experience performing testing on IACS

Category of qualification / experience	CRT or NST lead
Relevant industry specific knowledge	• Successful completion of training class or 1 year experience in job demonstrating proficiency with CRT/NST tool to be used AND • General knowledge of at least two different IACS OR detailed knowledge of one IACS AND • Moderate level knowledge of networking and communication protocols AND • Able to independently read and understand user installation and configuration documents for IACS Products AND • Knowledge of methods used to protect communications and detect / prevent communication attacks
Knowledge of security standards	ISA 62443 Standard plus at least one of: • Common Criteria • ISO/IEC 27001 • IEC 61508

6.3.2.3 VIT testers

The qualifications for individuals who oversee the technical aspects of VIT are the same as those for CRT/NST testers as shown in Table 2, with the following modifications (where the asterisk (*) refers to the note following Table 1):

- The following qualification is added:
  - Professional certification: CISA, CISSP or equivalent*
- The following qualification is revised as shown:
  - Successful completion of training class or 1 year experience in job demonstrating proficiency with ~~CRT~~ VIT tool to be used
- The following qualification is deleted:
  - Knowledge of methods used to protect communications and detect / prevent communication attacks.

6.4 Changes to certification requirements

6.4.1 General requirements

The chartered laboratory procedures shall address the requirements as specified in:

- ✓ ISO/IEC Guide 65 Section 6

6.4.2 ISASecure SSA specific requirements

For ISASecure, changes in technical certification requirements are initiated by ISCI, not the laboratory. Hence ISCI keeps the chartered laboratories informed of upcoming changes to technical certification criteria. The chartered laboratory in turn shall have processes to keep interested parties informed of these changes and other types of changes to certification requirements (such as changes to legal agreements associated with the certification process). This shall include keeping the chartered laboratory's ISASecure SSA certification clients informed of changes to CRT requirements, whether or not the chartered laboratory directly performed CRT on any embedded devices for a client's system or whether it was performed by a CRT laboratory.

When technical changes in certification criteria occur, existing certifications to the previous criteria remain in place, since the certification applies to a particular product and ISASecure certification version. Hence no products can lose certification due to lack of communication of new technical requirements. However, suppliers can do more effective planning related to future systems based upon timely information about upcoming changes (of all types) to the certification program requirements.

6.5 Appeals, complaints and disputes

6.5.1 General requirements

Chartered laboratory procedures shall address the requirements as specified in

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section IV. Report and Complaint Procedures B. Complaints*
- ✓ ISO/IEC Guide 65 Section 7
- ✓ IAF Guidance on ISO/IEC Guide 65 Section 7
- ✓ ISO/IEC 17025 Section 4.8

6.5.2 ISASecure SSA specific requirements

The published chartered laboratory procedure for handling complaints shall include the provision that complaints may be appealed to ISCI by the party bringing the complaint, if the internal laboratory resolution procedure does not offer a resolution satisfactory to them. Appealed complaints first go to the ISCI Technical Steering Committee. They may be further appealed to the ISCI governing board, then to ASCI board of directors.

A chartered laboratory shall be responsible for managing the resolution of complaints related to any aspect of compliance for a system it evaluated or certified, including complaints related to compliance with CRT where these tests were performed by a CRT lab and results submitted to the chartered laboratory. If the chartered laboratory receives a complaint related to CRT where these tests were performed by a CRT laboratory, the chartered laboratory shall inform the CRT laboratory and engage their assistance toward resolution where appropriate.

An appealed complaint may request a ruling on whether the ISASecure specifications were correctly applied in a specific instance. Such a complaint shall not be escalated to the ASCI board of directors, but is resolved within ISCI. This ruling could impact:

- Whether the certification process is applicable to a particular product that has applied for certification
- Whether or not a certification was granted
- Adequacy of the system evaluation process by the chartered laboratory or CRT laboratory.

ISCI or ASCI shall not accept certification applications, nor process, grant, or revoke certifications. This is the role of a chartered laboratory. ISCI can assist in interpretation of the ISASecure SSA specifications.

6.6 Application for certification

6.6.1 General requirements

The procedures shall address the requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I. Capability 8. Testing, evaluation and processing, items C7-C8.*

- ✓ ISO/IEC Guide 65 Section 8
- ✓ ISO/IEC 17025 Section 4.4, Contract Review of Testing Services

6.6.2 ISASecure SSA specific requirements

The ISASecure specification [SSA-300] contains requirements that system suppliers must meet in order to achieve ISASecure SSA certification for a system. That document is intended as a reference for suppliers applying for certification of a system.

These requirements are numbered R1, R2, and R3, and are repeated here so that this document may describe their impact on chartered laboratory operations.

A chartered laboratory shall incorporate the R1 and R3 requirements into their certification application process for system suppliers:

Requirement ISASecure_SY.R1 – Application for security zone certification levels

When a system supplier applies for certification of a system, the certification applicant SHALL specify the maximum capability security level for which they would like to achieve certification for each security zone. The levels possible are 1, 2, or 3, or 4. The certifier SHALL award certification designating each security zone at the highest level less than or equal to this maximum level for which the security zone qualifies, without requiring the system supplier to reapply for certification.

NOTE The SRT specification [SSA-310] requires that a security zone breakdown for the system be submitted with an application for system certification.

An application is either for an initial certification, or requests consideration for evidence from prior certifications of an earlier system version. As discussed in [SSA-301], the chartered laboratory may perform an SSA evidence impact assessment to determine the extent to which the evidence offered from any prior certification is applicable to the new certification. The chartered laboratory shall have the option to require that the evaluation process defined for an initial certification be performed, if in its judgment an evidence impact assessment could not be performed with confidence. This process includes analysis of CRT evidence, regardless of whether CRT was previously or shall in the future be performed by the chartered laboratory or a CRT laboratory.

Requirement ISASecure_SY.R3 – ISASecure application requirements for certification

Items specified as follows SHALL be submitted to the SSA certification process by an applicant for an initial certification:

a) technical items as required by the specifications listed in Clause 2 of [SSA-300];

b) for any ISASecure EDSA certified embedded devices that are components of the system, the FSA section of the EDSA certification report; and

c) administrative and potentially additional technical items defined by the certifier.

Note that if a CRT laboratory performs CRT, the items under a) above that apply for CRT would be submitted to the CRT laboratory and then included in the CRT evidence submission from the CRT laboratory to the chartered laboratory.

A chartered laboratory shall include the following in its signed agreement with a certification applicant:

Requirement ISASecure_SY.R2 – Publication of system certification status

If ISCI, the certifier, or the system supplier publishes certification status information for certified systems in a public venue, information provided SHALL include the most granular version identifier of the system to which

the ISASecure SSA certification applies, and the version of the certification achieved, designated by the year and release, such as ISASecure SSA 2014.1.

6.7 Preparation for evaluation/testing

6.7.1 General requirements

Chartered laboratory procedures shall address the requirements as specified in:

- ✓ ISO/IEC Guide 65 Section 9
- ✓ IAF Guidance on ISO/IEC Guide 65 Section 9
- ✓ ISO/IEC 17025 Section 4.4

6.7.2 ISASecure SSA specific requirements

Individuals assigned responsibility for an FSA-S audit, SDA-S audit, SDLA audit and oversight of CRT/NST and VIT shall have at a minimum the associated qualifications listed in 6.3.2. These criteria for oversight of CRT/NST shall also apply to individuals that interpret CRT evidence submitted by a CRT laboratory on behalf of a certification applicant.

6.8 Evaluation

6.8.1 General requirements

Chartered laboratory procedures shall address the requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I. Capability A. Testing facilities, B. Testing equipment and C. Testing, evaluation and processing procedures*
- ✓ ISO/IEC Guide 65 Section 10
- ✓ ISO/IEC 17025 Section 5 – Technical Requirements

6.8.2 ISASecure SSA specific requirements

6.8.2.1 General

An evaluation of a control system for an initial certification shall be carried out in accordance with all technical specifications for SDLA, SDA-S, FSA-S, FSA-E, and SRT as referenced in Requirement ISASecure_SY.R4 of [SSA-300].

For cases other than an initial certification, [SSA-301] specifies the method for carrying out a system evaluation when evidence from a prior certification is accepted toward a new certification for a newer system version. [SSA-301] also specifies criteria that the certifier shall apply to determine whether or not to accept such evidence when performing an evidence impact assessment.

The chartered laboratory shall always perform the asset discovery test that precedes the major elements of SRT (VIT, CRT, NST). The chartered laboratory also shall always perform VIT and NST. The chartered laboratory or a CRT laboratory may perform CRT for embedded devices that are components of the system to be certified. The chartered laboratory shall always perform CRT for any other types of devices that are components of the system.

6.8.2.2 defines requirements that apply to testing performed by a chartered laboratory. 6.8.2.3 describes additional requirements to be met by the chartered laboratory when a CRT laboratory performs CRT for an embedded device. [EDSA-206] defines complementary requirements allocated to the CRT laboratory.

6.8.2.2 Chartered laboratory testing requirements

The evaluation and testing process for CRT and NST shall use an ISCI recognized test tool. The process for recognition of these test tools is defined in [EDSA-201]. The chartered laboratory shall verify that the software version and hash of the tool software is as specified for the recognized tool on the ISASecure web site at http://www.ISASecure.org.

The VIT process shall use a test tool specified by ISCI in [SSA-310].

ISO/IEC 17025 5.4.2 on selection of test methods specifies using the latest version of the standards upon which tests are based. The latest versions of ISASecure specifications shall be identified on the ISASecure web site.

ISO/IEC 17025 5.4.4 and 5.4.5 discuss the definition of procedures for and validation of non-standard test methods. The test methods and criteria for monitoring upward essential functions for CRT, NST and VIT are non-standard test methods that are agreed with each certification applicant before the start of SRT. They are subject to the requirements in these ISO/IEC 17025 sub clauses.

ISO/IEC 17025 5.5 on the topic of accuracy, appropriate use, maintenance and calibration specifically applies to the CRT/NST test tool, in particular the functional component of this tool that measures jitter.

6.8.2.3 Chartered laboratory requirements when CRT laboratory performs CRT

When a CRT laboratory performs CRT for a device that is a component of a candidate system for SSA certification, then at the request of the client that originally engaged the CRT laboratory (whether the system supplier or the device supplier), the CRT laboratory shall provide a CRT evidence submission to a chartered laboratory selected by the system supplier. Such submissions shall be accepted from a recognized CRT laboratory only and not from the system or device supplier.

The chartered laboratory shall verify that a CRT evidence submission from a CRT laboratory meets the requirements laid out in [EDSA-206]. The same requirements apply whether the testing supports an initial or subsequent certification of the embedded device. The chartered laboratory shall also verify that:

- the CRT tool version reported by the CRT laboratory is recognized for CRT by ISCI
- the CRT specification versions reported by the CRT laboratory match the latest versions on the ISASecure web site
- the device version in the CRT evidence submission is the same version of the device that has been submitted by the supplier as a component of the system for performance of the other elements of the SSA evaluation.

If the device version in the CRT evidence submission differs from the version submitted to the chartered laboratory as a component of the system for certification, the chartered laboratory may perform an evidence impact assessment to determine whether the evidence submitted is applicable to the revised device, per the requirements in [EDSA-301]. The chartered laboratory shall have the option to require the revised device to undergo CRT tests if indicated per [EDSA-301] requirements.

The chartered laboratory shall verify that the CRT evidence submission is consistent with passing CRT. If not, it may request clarification from the CRT laboratory. The chartered laboratory has the responsibility to determine whether the test evidence submitted supports a decision to certify the system of which the device is a component. If a submission or some aspects of a submission are not accepted, the chartered laboratory shall provide a written rationale to the CRT laboratory.

There are some tests in Clause 7 of the CRT test specifications for individual protocols, where the “Result” is NOT designated as simply pass/fail. Some of these tests require vendor documentation of risks depending upon the result of the test. The chartered laboratory shall verify that this documentation is present if required.

6.9 Evaluation report

6.9.1 General requirements

The chartered laboratory shall address the requirements on evaluation reports as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section I Reports and Complaint Procedures, A. Reports.*
- ✓ ISO/IEC Guide 65 Section 11
- ✓ ISO/IEC 17025 Section 5.10 – Testing Report

6.9.2 ISASecure SSA specific requirements

The overall evaluation report shall follow the format of the ISASecure SSA sample report [SSA-303].

Detailed reporting on SRT results shall be carried out in accordance with the requirements on SRT reporting in [SSA-310].

If a CRT lab has carried out CRT for embedded devices that are components of the system, most of the CRT report information will come from the CRT evidence submission. The chartered laboratory's report shall note this source for the information.

ISO/IEC Guide 65 Section 11b) states that in the case of a nonconformance such that certification is not granted, that the report from the chartered laboratory shall advise the certification applicant of the additional testing and assessment that needs to take place once the item is remedied. For ISASecure SSA, if the FSA-S, FSA-E, SDA-S or SDLA (when performed as part of the SSA evaluation) does not pass, the line items in these evaluations that may require reassessment shall be specified. If the CRT, NST or VIT element does not pass, all CRT, NST and VIT tests shall be performed on any modified components of a system presented again for certification in order to pass this element. If the system network or other configuration is modified in manner separate from modifications to specific components, [SSA-301] requirements for evidence impact assessment shall be followed to determine which tests to rerun on the modified system.

6.10 Decision on certification

6.10.1 General requirements

The chartered laboratory shall address the requirements on the decision to certify a system in:

- ✓ ISO/IEC Guide 65 Section 12
- ✓ IAF Guidance on ISO/IEC Guide 65 Section 12

6.10.2 ISASecure SSA specific requirements

The requirement ISASecure_SY.R4 "Criteria for granting an initial certification" in [SSA-300] defines the technical criteria that a chartered laboratory shall use for granting an initial ISASecure SSA certification.

[SSA-301] specifies the technical criteria that the chartered laboratory shall use for granting certification when evidence from a prior certification of a system is accepted as evidence toward a new certification for a modified version of the same system.

The form of letter or certification document provided when a device passes certification shall meet the format requirements in [SSA-204].

6.11 Surveillance

An ISASecure SSA certification states that a specific version of a system meets established security criteria. ISCI does not require a chartered laboratory to verify periodically that systems shipped by the vendor that are labeled with the version number that has been certified, are in fact that version. There are however, requirements for the chartered laboratory to monitor the use of the ISASecure symbol as described in Section 6.12.

As described under 6.10.2, a supplier's ISASecure SDLA certification for their lifecycle development process, may apply toward the ISASecure SSA certification of their system products. Ongoing requirements to maintain an SDLA certification are described in the specifications for that program as listed in [SDLA-100]. However, it should be noted that failure to meet ongoing requirements to maintain ISASecure SDLA certification shall not result in revocation of an ISASecure SSA certification for a system product that has previously been awarded.

6.12 Use of the ISASecure symbol

6.12.1 General requirements

The procedures for use of the ISASecure symbol for a system shall address the requirements as specified in:

- ✓ *ASCI Chartered Testing Laboratory 2009 Approval Process Section II Control Programs, A. Listing and Labeling.*
- ✓ ISO/IEC Guide 65 Section 14
- ✓ IAF Guidance on ISO/IEC Guide 65 Section 14

6.12.2 ISASecure SSA specific requirements

The interpretation of the above requirements for ISASecure entails that the chartered laboratory shall monitor the use of the ISASecure symbol by the system supplier to insure appropriate use, and take appropriate action if the symbol is used incorrectly.

[SSA-204] provides detailed instructions and policies regarding use of the ISASecure symbol for the SSA program. The agreement that the chartered laboratory signs with the certification applicant shall acknowledge and require adherence to this information.

6.13 Complaints to system suppliers

6.13.1 General requirements

A chartered laboratory shall include the following in its signed agreement with a system supplier: that the supplier has a process for meeting the requirements regarding complaints they receive, as specified in:

- ✓ ISO/IEC Guide 65 Section 15

These requirements address handling and disclosure of complaints known to the vendor of a certified system, regarding the compliance of that system with the ISASecure SSA requirements.

6.13.2 ISASecure SSA specific requirements

In addition, the signed agreement between the laboratory and the system supplier shall include the following broader provision. Any complaint known to the supplier of a certified system that is determined to affect product security shall be brought to the attention of the chartered laboratory that granted a certification for the system. The laboratory shall evaluate the impact on the product conformance to the ISASecure requirements.

The chartered laboratory process for handling such reports from a supplier shall include a process to advise ISCI if a modification to the ISASecure specifications should be considered based upon this event. This process shall be contingent upon approval from the supplier to disclose to ISCI any information concerning their system, whether or not it is attributed to their system.

7 Accreditation of chartered laboratories

7.1 Overview

Accreditation of a chartered laboratory involves an assessment of the organization against the requirements in the following documents, and an assessment of technical readiness for performing ISASecure SSA evaluations.

- ASCI Chartered Testing Laboratory 2009 Approval Process [ASCI Lab]
- ISO/IEC Guide 65 [ISO/IEC Guide 65]
- IAF Guidance on ISO/IEC Guide 65 [IAF Guide 65 Guidance]
- ISO/IEC 17025 [ISO/IEC 17025]
- Section 6 this document, all ISASecure specific requirements subsections

Technical readiness assessment is based upon review of documented laboratory processes and procedures as well as review of artifacts produced by the chartered laboratory from sample SDA-S, FSA-S, FSA-E, and SRT audits carried out by the laboratory on a system approved for this purpose by ISCI, as described in Section 7.3. The review of artifacts may take place during the pilot phase of the ISASecure SSA program and be related to an early certification performed by the laboratory.

To be recognized as a chartered laboratory for the ISASecure SSA program, a laboratory shall attain the following accreditations, performed by an IAF/ILAC recognized accreditation body:

- accredited to ISO/IEC 17025, with technology scope of accreditation covering testing to ISASecure SSA SRT specifications; and
- accredited to IAF ISO/IEC 65, with technology scope of accreditation covering ISASecure SSA certification.

The second accreditation will require compliance with the IAF Guidance on ISO/IEC Guide 65 in addition to Guide 65.

These internationally recognized accreditations shall be obtained by a laboratory within 9 months of obtaining a provisional chartered laboratory status, as described in Section 5. The following section discusses requirements for attaining provisional chartered laboratory status.

7.2 Provisional chartered laboratory status

Provisional chartered laboratory status allows an organization to begin certification activities before accreditation has been formally granted by the accreditation body. Formal granting of the accreditation can occur several months after the evaluation of the laboratory has taken place and results submitted by the evaluators to the board within the SSA accreditation body that makes the final accreditation decision.

ASCI will grant a laboratory provisional chartered status based on the results of an evaluation of the laboratory by a qualified assessor for the 17025 and Guide 65 accreditations listed in Section 7.1. Provisional chartered status is granted if the evaluation shows that the laboratory complies with all of the requirements in the five documents listed in Section 7.1, as well as those technical readiness criteria in Table 3 that may be verified based upon process and procedure documentation evidence. These criteria are in

rows 1-8 and 11 of Table 3. All ISASecure specific requirements in Section 6 of this document are also mandatory to receive provisional chartered status.

The evaluation for a candidate chartered laboratory is performed by an assessor that has been qualified by an IAF/ILAC recognized accreditation body. A candidate organization shall apply for accreditation as required by the accreditation body. [ISASecure-202] provides the ASCI application process and forms for provisional chartered laboratory status based on the evaluation by the accreditation body. “Provisional” chartered laboratory status is a term applied by ASCI/ISCI within the ISASecure SSA program and is not recognized or managed by the accreditation body.

During the period when a chartered laboratory is operating in provisional status, ASCI shall be made aware of the laboratory’s expectations for receipt of formal internationally recognized accreditation by an IAF/ILAC organization. ASCI shall have the option to perform an interim review and update its evaluation for provisional status of the chartered laboratory 6 months after it is received. Once a chartered laboratory has achieved accreditation by an IEC 17011 accreditation body, that accreditation body determines the requirements and frequency for maintenance audits to maintain accredited status.

7.3 Technical readiness assessment

The technical readiness assessment reviews technical criteria required for competent performance of the various ISASecure SSA certification elements. The evaluation consists of assessment of evidence supplied by the candidate laboratory per the evaluation criteria in Table 3. The requirements numbered UDP.Rnn in this table are from [EDSA-405]. The requirements numbered CRT.Rnn are from [EDSA-310]. The requirements numbered SRT.Rnn are from [SSA-310].

Table 3 - Technical readiness criteria for SSA chartered laboratory

ID	Evidence supplied by candidate laboratory	Evaluation criteria
1	Vendor statement of test tools and versions in use for SRT	• Appropriate tool is in place for asset discovery test • Tool and version for CRT/NST robustness tests is recognized by ISCI • ISCI-specified tool is in place for VIT per SRT.R42 with tool version specified in [SSA-420]
2	Asset discovery test and CRT processes/procedures	• Comply with set up procedure for asset discovery test per SRT.R30-32; and for individual protocol tests • Comply with SRT.R38 regarding requirement for TD measurement jitter relative to device cycle time and monitoring coverage for various device outputs • Comply with asset discovery test procedure requirements SRT.R33-37 • Comply with SRT.R40 for how pass of asset discovery test is defined • Comply with coverage of various phases of CRT testing per SRT.R48 (CRT.R50)

ID	Evidence supplied by candidate laboratory	Evaluation criteria
		• Comply with SRT.R49 on how protocols and components for CRT are selected; SRT.R29 on test order; and SRT.R23 on use of a single SUT; • Comply with SRT.R67 on documentation and reporting of discussions with customers on anomalies; SRT.R68 on reporting conditional branches of test execution; • Comply with SRT.R48 (CRT.R59) for traffic rate for CRT load testing and NST • Comply with SRT.R51 for how pass of CRT is defined • Comply with SRT.R52 regarding repeating failures before giving failed status • Comply with SRT.R48 (CRT.R63) for setting pseudo random seed value if used • Instructions for evaluation report creation comply with SRT.R71-75 for asset discovery and SRT.R79-83 for CRT
3	NST processes/procedures	• Comply with SRT.R54 (CRT.R59) for traffic rate for testing and NST • Comply with SRT.R55 on scope of NST • Comply with SRT.R56 regarding configuration for NST • Comply with SRT.R57 for how pass of NST is defined • Comply with SRT.R58 regarding repeating failures before giving failed status • Instructions for evaluation report creation comply with SRT.R84-88
4	VIT processes/procedures	• Comply with SRT.R43 and SRT.R44 on VIT test configuration including use of the VIT tool, tool version with appropriate scanning policy and a method for jitter monitoring; • Comply with [SSA-420] regarding selection of the set of known vulnerabilities used for test and archiving of this selection • Comply with SRT.R45 on interfaces to test under VIT • Comply with SRT.R46 on criteria for VIT pass • Comply with SRT.R47 regarding repeating failures before giving failed status • Instructions for VIT evaluation report creation comply with

ID	Evidence supplied by candidate laboratory	Evaluation criteria
		SRT.R76-78
5	Mapping that maps each asset discovery test requirement in [SSA-310] Sections 10.2-10.3 to a portion of a test procedure	• Mapping is complete and accurate
6	Mapping that maps each table in Section 7 of each CRT protocol-specific specification to a portion of the SRT CRT test procedure	• Mapping is complete and accurate
7	Mapping that maps each table that represents a load stress test in Section 7 of each CRT protocol specific specification to a portion of the SRT NST test procedure	• Mapping is complete and accurate
8	Application form and instructions to be given to supplier submitting the system	• Application requests all items required per [SSA-310] Sections 6.2 and 8
9	Intermediate artifacts, paperwork and final evaluation report for an ISCI-approved sample system covering SDA-S, FSA-S, FSA-E, and SRT. Artifacts from candidate laboratory include procedure for non-standard tests created for the sample system to monitor upward essential functions per ISO/IEC 17025 5.4.4 and validation of these tests per 5.4.5.	• Test plan complies with SRT.R16-17 in specifying types of tests and test points and test order • Scope and results of FSA-S and FSA-E evaluations are consistent with security zone levels • Scope, artifacts and results from SDA-S are consistent with security zone levels and validation activities in [SDLA-312] • Results of asset discovery test are as expected and indicate compliance with procedures • Report from VIT evaluation indicates use of tool version and set of known vulnerabilities specified by [SSA-420] • Report from VIT evaluation indicates compliance with pass/fail criteria in SRT.R46 • Results of CRT and NST test are as expected and indicate compliance with procedures including required scope • Report of test configurations for tests meet requirements SRT.R30-31 and CRT.R48-49 in appropriate protocol tests • Records of control signal generated for testing meet requirements of SRT.R38 • Check for reporting of pseudo random seed value per SRT.48

ID	Evidence supplied by candidate laboratory	Evaluation criteria
		(CRT.R63) • Artifacts that describe test method to monitor upward essential services comply with SRT.R39 • Evaluation report and detailed SRT report meet requirements per Section 6.9 of this document • Evaluation report complies with UDP.R12 and similar requirements for other protocols. • Evidence meets [ASCI Lab] IV.A.1, I.C.1, I.C.2
10	Evidence demonstrating that asset discovery test result, CRT test result, NST test result and VIT result for sample system can be reproduced based on information in evaluation report; document steps used to reproduce these	• Verify that steps for creation of reproduced results required only information in the evaluation report; and that results are same as initial results
11	CRT lab interface	• Verify that the requirements in 6.8.2.3 are reflected in the chartered laboratory processes and procedures.

Annex A Mapping from sources for general requirements to this document

In this section we show the coverage of the ISO/IEC Guide 65 and 17025 international standards, and the ASCI chartered laboratory process, as called out in this document. Each mapping table is preceded by a summary statement regarding the coverage shown by that mapping.

A.1 ISO/IEC Guide 65 1996 coverage

As shown in Table 4, all sections of [ISO/IEC Guide 65] are called out as requirements in this document, with the exception of clause 13 regarding surveillance. The reason for this omission is noted below.

Table 4 - Mapping from ISO/IEC Guide 65 to this document

	Reference in ISO/IEC Guide 65	Reference this document	Comments
4.	Certification body	6.2	
5.	Certification body personnel	6.3	
6.	Changes in the certification requirements	6.4	
7.	Appeals, complaints and disputes	6.5	
8.	Application for certification	6.6	
9.	Preparation for evaluation	6.7	
10.	Evaluation	6.8	
11.	Evaluation report	6.9	
12.	Decision on certification	6.10	
13.	Surveillance	NA	There are no requirements under this topic. The rationale for this is discussed in Section 6.11 of this document.
14.	Use of licenses, certificates and marks of conformity	6.12	
15.	Complaints to suppliers	6.13	

A.2 IAF ISO/IEC 65 Guidance coverage

As shown in Table 5, all sections of [IAF Guide 65 Guidance] are called out as requirements in this document, with the exception of Clause 13. Clause 13 has no associated requirements in this document for the reasons referenced below.

Table 5 - Mapping from IAF Guidance on ISO/IEC Guide 65 to this document

	Reference in IAF ISO/IEC 65	Reference this document	Comments
4.	Certification body	6.2	
5.	Certification body personnel	6.3	
6.	Changes in the certification requirements		No requirements in this clause of standard
7.	Appeals, complaints and disputes	6.5	
8.	Application for certification		No requirements in this clause of standard
9.	Preparation for evaluation	6.7	
10.	Evaluation		No requirements in this clause of standard
11.	Evaluation report		No requirements in this clause of standard
12.	Decision on certification	6.10	
13.	Surveillance	NA	There are no requirements under this topic. The rationale for this is discussed in Section 6.11.
14.	Use of licenses, certificates and marks of conformity	6.12	
14.	Complaints to suppliers		No requirements in this clause of standard

A.3 ISO/IEC 17025 coverage

All requirements in ISO/IEC 17025 are referenced in this document. As shown in Table 6, the requirements clauses 4 and 5 of ISO/IEC 17025 are called out in their entirety in this document, respectively in 6.2 which covers management elements and in 6.8 which covers evaluation. In addition, some sub clauses of those clauses are called out in more specific sections as shown below.

Table 6 - Mapping from ISO/IEC 17025 to this document

	Reference in ISO/IEC 17025 document	Reference this document
4.	4. Management requirements	6.2
4.1	4.1 Organization	6.2
4.2	4.2 Management system	6.2
4.3	4.3 Document control	6.2
4.4	4.4 Review of requests, tenders and contracts	6.6, 6.7
4.5	4.5 Subcontracting	6.2
4.6	4.6 Purchasing	6.2
4.7	4.7 Service to clients	6.2
4.8	4.8 Complaints	6.5
4.9	4.9 Control of nonconforming work	6.2
4.10	4.10 Improvement	6.2
4.11	Corrective action	6.2
4.12	Preventive action	6.2
4.13	Control of records	6.2
4.14	Internal audit	6.2

	Reference in ISO/IEC 17025 document	Reference this document
4.15	Management review	6.2
5.	Technical	6.8
5.1	General	6.8
5.2	Personnel	6.3
5.3	Accommodation and environmental conditions	6.8
5.4	Test and calibration methods and method validation	6.8
5.5	Equipment	6.8
5.6	Measurement traceability	6.8
5.7	Sampling	6.8
5.8	Handling of test and calibration items	6.8
5.9	Assuring the quality of test and calibration results	6.8
5.10	Reporting the results	6.9

A.4 ASCI Chartered Testing Laboratory 2009 Approval Process coverage

As shown in Table 7, all sections of the ASCI Chartered Testing Laboratory 2009 Approval Process are called out as requirements in this document, with the exception of II.B Follow up and field inspections and I.D. Calibration Program, which do not apply to the ISASecure SSA program.

Table 7 - Mapping from ASCI Chartered Testing Laboratory 2009 Approval Process to this document

	Reference in ASCI Chartered Testing Laboratory 2009 Approval Process document	Reference this document	Comments
I.A.	Capability - Testing Facilities	6.8	
I.B.	Capability - Test Equipment	6.8	
I.C.	Capability - Testing, Evaluation and Processing Procedures	6.8	
I.C 7-8	Capability - Testing, Evaluation and Processing Procedures C7-C8	6.6	
I.D.	Capability - Calibration Program		No application seen for ISASecure SSA.
I.E.	Capability - Quality Assurance	6.2	
I.F.	Capability - Records (including Specifications Library)	6.2	
I.G.	Capability - Personnel	6.3	
II.A.	Control Programs - Listing and Labeling	6.12	
II.B.	Control Programs - Follow up and Field Inspections		Not applicable. The initial assessment of the manufacturer (system supplier) described in this section is superseded by the SDLA. Follow up inspections are not required by the ISASecure SSA program. See rationale in Section 6.11.
III.	Independence	6.2	
IV.A.	Report and Complaint Procedures - Reports	6.9	
IV.B	Report and Complaint Procedures - Complaints	6.4	