ISASecure-111

ISA Security Compliance Institute — ISASecure certification programs

Transition to ISO/IEC 17065

Version 1.1

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, 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
1.1	2014.05.02	Initial version published to http://www.ISASecure.org

Contents

FOREWORD

This is one of a series of documents that defines ISASecure certification programs. This document describes the ISCI policy for accreditation of certification bodies for the ISASecure programs, as it relates to the transition of the international accreditation community from ISO/IEC Guide 65 to ISO/IEC 17065 as the standard for requirements on certification bodies. This document supersedes information in existing documents that define the ISASecure programs, found on the web site http://www.ISASecure.org.

1 Background and scope

ISCI (ISA Security Compliance Institute) defines several certification programs for which organizations may be accredited as certification bodies, by IAF/ILAC (International Accreditation Forum/International Laboratory Accreditation Cooperation) accreditation bodies.

In particular, ISCI operates product certification programs for embedded devices, called ISASecure EDSA (Embedded Device Security Assurance) and for control systems, called ISASecure SSA (System Security Assurance). ISCI also has defined a process certification program for supplier control systems security development lifecycle processes, called ISASecure SDLA (Security Development Lifecycle Assurance), to be operational in 2014.

The standard [ISO/IEC 17065] which defines requirements on certification bodies, has replaced [ISO/IEC Guide 65], as documented in the IAF informative document [IAF 17065 Transition] listed in the bibliography to this document. Accordingly, ISCI has defined a policy for transition of accreditation requirements for ISASecure programs. The present document defines this policy.

2 Normative references

2.1 ISASecure certification schemes

[EDSA-100] *ISCI Embedded Device Security Assurance - ISASecure Certification Scheme*, as specified at http://www.ISASecure.org

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

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

2.2 ISASecure accreditation requirements

[EDSA-200] *ISCI Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

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

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

2.3 International standards for certification programs

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

[ISO/IEC 17065] ISO/IEC 17065.2012, "*Conformity assessment—requirements for bodies certifying products, processes and services*", October 2012

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

NOTE The CRT laboratory accreditation program is not otherwise referenced in, nor impacted by, the present document, since ISCI CRT laboratories are not certification bodies.

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
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.

3.1.4
certification scheme
overall definition of and process for operating a certification program

3.1.5
certification body
an organization that performs certification

3.1.6
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. ASCI is the legal entity representing ISCI.

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
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.

3.1.10
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

3.2 Abbreviations

The following abbreviations are used in this document.

ASCI	Automation Standards Compliance Institute
DCS	distributed control system
EDSA	embedded device security assurance
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
SDLA	security development lifecycle assurance
SIS	safety instrumented system
SSA	system security assurance

4 Transition policy

The following policy applies to ISASecure chartered laboratories, which are the certification bodies for the ISASecure certification programs. The policy is effective as of April 15, 2014. This policy shall take precedence over requirements for compliance with [ISO/IEC Guide 65] in the documents for ISASecure EDSA, SSA and SDLA listed in clause 2 of this document.

- **New certification bodies** - Chartered laboratories new to the ISASecure program after April 15, 2014, SHALL meet ISO/IEC 17065 to be accredited as certification bodies for all ISASecure programs, including EDSA, SSA, or SDLA.

- **Existing certification bodies -** ISASecure chartered laboratories that are accredited to ISO/IEC Guide 65 under the EDSA program prior to April 15, 2014, MAY be accredited as certification bodies for SDLA or SSA under ISO/IEC Guide 65. Existing certification bodies SHALL meet ISO/IEC 17065 requirements by Sept 15, 2015 for all ISASecure programs, including EDSA, to maintain accreditation.

Documents for the ISASecure SDLA program that are current as of the release of that certification program, will be consistent with the above policy.

BIBLIOGRAPHY

[IAF 17065 Transition] *IAF Informative Document for the Transition of Product Certification Bodies to ISO/IEC 17065:2012 from ISO/IEC Guide 65 1996,* http://www.iaf.nu/upFiles/IAF_ID_Transition_to_ISO_17065_MOL_Rev_8131_v2clean_with_final_edit_final.pdf