ISASecure-113

ISA Security Compliance Institute — ISASecure® certification programs

Policy for transition to EDSA 2.0.0 and SSA 2.0.0

Version 1.2

January 2016

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	2015.04.27	Initial version published to http://www.ISASecure.org
1.2	2016.01.26	Move V 2.0 implementation date from 2016 Feb 1 to 2016 July 1

Contents

FOREWORD

This is one of a series of documents that defines ISASecure® certification programs. This document describes the ISCI policy for transition of certification operations to the updated certification versions ISASecure EDSA 2.0.0 (Embedded Device Security Assurance) and ISASecure SSA 2.0.0 (System Security Assurance). The list of ISASecure certification programs and documents for these program versions, and for their prior versions, can be found on the web site http://www.ISASecure.org.

1 Background and scope

ISCI (ISA Security Compliance Institute) operates product certification programs for embedded devices, called ISASecure® EDSA (Embedded Device Security Assurance) and for control systems, called ISASecure SSA (System Security Assurance). The initial versions of these programs were denoted EDSA 2010.1 and SSA 2014.1. These programs have been updated to new versions denoted EDSA 2.0.0 and SSA 2.0.0.

This document specifies the timeline and related policies for transition of certification operations to EDSA 2.0.0 and SSA 2.0.0.

2 Normative references

An ISASecure certification program version program is defined by a set of associated specification documents and document versions. The documents associated with the four programs named in Clause 1 are published at http://www.ISASecure.org.

The present document refers specifically to:

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

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

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 body

an organization that performs certification

3.1.5

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.

3.1.6
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.

3.1.7
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.8
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.

3.1.9
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

3.2 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
IACS	industrial automation and control system(s)
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
PLC	programmable logic controller
SIS	safety instrumented system
SSA	system security assurance

4 Transition policies

The following policies apply to ISASecure chartered laboratories, which are the certification bodies for the ISASecure certification programs.

- All EDSA and SSA certifications where the application for certification takes place on or after **July 1, 2016,** SHALL comply with the EDSA 2.0.0 and SSA 2.0.0 specifications, respectively, as listed at http://www.ISASecure.org, with one exception described following. " All certifications" includes initial EDSA or SSA certifications, and certifications issued under the maintenance of certification process.

- A supplier MAY apply for an EDSA 2010.1 certification after July 1, 2016, in the following case:
  - The supplier is applying for EDSA 2010.1 certification of a new version of a device that previously achieved EDSA 2010.1 certification.
  - The chartered laboratory to which application is made, in its evidence impact assessment for the revised device (as defined in EDSA-301 v1.0), determines that due to the nature of the changes to the device, there are no updates needed to the prior evidence for EDSA 2010.1 certification, to support EDSA 2010.1 certification of the revised device.

NOTE 1 The specific event that defines "application" is not specified by ISCI. Therefore, it is to be determined by each chartered laboratory.

NOTE 2 This policy does not preclude "early" EDSA 2.0.0 or SSA 2.0.0 certifications, for certification applications *before* Feb 1, 2106.

NOTE 3 The exception acknowledges that a certified embedded device may have been modified, but have no substantive changes from the point of view of cyber security, but rather has undergone other changes that resulted in assignment of a new model number. The intent this case is that the product may continue to maintain its existing ISASecure EDSA 2010.1 certification. In other words, an upgrade to the EDSA 2.0.0 certification criteria is not mandatory in this case.

5 Informative guidance for ISASecure EDSA and SSA program participants

ISCI has developed a document (see Bibliography) that describes the differences between the prior versions and the 2.0.0 versions of the EDSA and SSA certification programs. It is an informative resource intended to assist certifiers, accreditation bodies, test tool suppliers, suppliers interested in certification of their products, and end users, in planning for the transition to the new certification versions. It is intended to be used together with the documentation for the prior and upgraded program versions, as a guide to identifying areas of change.

ISCI has not specified a mandatory date for compliance of ISCI-recognized CRT tools to the updated specifications. ISCI anticipates that submission of tool recognition evidence by tool suppliers per the updated [EDSA-201] and related specifications, by October 5, 2015, will support completion of ISCI tool recognition by early December 2015, and subsequent incorporation of updated tools by the chartered laboratories in time to meet the Feb 1, 2016 transition date.

BIBLIOGRAPHY

ISCI has published the following informative document that describes the changes due to the transition to EDSA 2.0.0 and SSA 2.0.0.

[ISASecure-112] *ISCI ISASecure Certification Programs - Guidance for transition to EDSA 2.0.0 and SSA 2.0.0,* to be published at http://www.ISASecure.org