ISASecure-118

ISA Security Compliance Institute — ISASecure® certification programs

Policy for transition to SDLA 3.0.0 specifications

Version 1.0

May 2020

A. DISCLAIMER
ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the SPECIFICATION.

Without limiting the foregoing, ASCI disclaims all liability for harm to persons or property, and users of this SPECIFICATION assume all risks of such harm.

In issuing and making the SPECIFICATION available, ASCI is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASCI undertaking to perform any duty owed by any person or entity to someone else. Anyone using this SPECIFICATION should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES
To the maximum extent permitted by applicable law, in no event shall ASCI or its suppliers be liable for any special, incidental, punitive, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the SPECIFICATION, the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION, or otherwise under or in connection with any provision of this SPECIFICATION, even in the event of the fault, tort (including negligence), misrepresentation, strict liability, breach of contract of ASCI or any supplier, and even if ASCI or any supplier has been advised of the possibility of such damages.

C. OTHER TERMS OF USE
Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.0	2020.05.01	Initial version published to http://www.ISASecure.org

Contents

1 Background and scope 6

2 Normative references 6

3 Definitions and abbreviations 6

3.1 Definitions 6

3.2 Abbreviations 7

4 Transition policy 7

FOREWORD

This is one of a series of documents that defines ISASecure® certification programs. This document describes the policy for transition of certification operations to the revised certification version ISASecure SDLA 3.0.0 (Security Development Lifecycle Assurance). The list of ISASecure certification programs and documents for this new program version, and for the prior program version SDLA 2.0.0, can be found on the web site http://www.ISASecure.org.

1 Background and scope

ISCI (ISA Security Compliance Institute) operates a process certification program for control system supplier secure product development lifecycle processes called ISASecure® SDLA certification (Security Development Lifecycle Assurance). The prior version of this program was called SDLA 2.0.0. An updated version of this program has been modified to offer an option for certification for a limited time period, when a compliant secure product development process is in place but has not yet been fully executed by the development organization to be certified. The certifier can grant certification based upon a review of the development organization's readiness to execute the process. This new version of the ISASecure certification program is called SDLA 3.0.0. SDLA 3.0.0 also strengthens certifier validation of the supplier's policies for enforcement of their development process, as defined in ISASecure specification [SDLA-312], in accordance with [IEC 62443-4-1] requirement SM-12.

The present document specifies the timeline for transition of certification operations to SDLA 3.0.0.

2 Normative references

Standards with which the ISASecure SDLA program aligns are as follows.

NOTE The following two references that have the same document number 62443-4-1, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

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

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

An ISASecure certification program version is defined by a set of associated specification documents and document versions. The documents associated with SDLA 3.0.0 are published at http://www.ISASecure.org, with document versions enumerated in the following document.

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

The present document refers specifically to:

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

3 Definitions and abbreviations

3.1 Definitions

3.1.1
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.

3.1.2
certification body
an organization that performs certification

3.1.3
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.

3.1.4
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.

3.1.5
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.6
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

3.1.7
version (of ISASecure certification)
ISASecure certification criteria in force at a particular point in time, defined by the set of document versions that define the certification program, and identified by a three-place number, such as ISASecure SDLA 3.0.0

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
IACS	industrial automation and control system(s)
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
SDLA	security development lifecycle assurance
SM	security management

4 Transition policy

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

- ISASecure SDLA certifications granted on or after January 1, 2021, SHALL use SDLA 3.0.0 specifications.
- ISASecure SDLA certifications granted before January 1, 2021 MAY use SDLA 3.0.0 specifications.