SSA-312

ISA Security Compliance Institute – System Security Assurance –

Security development artifacts for systems

Version 1.6

August 2019

Copyright © 2013-2019 ASCI - Automation Standards Compliance Institute, All rights reserved

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
1.01	2014.02.10	Initial version published to http://www.ISASecure.org
1.4	2018.02.02	Alignment with approved ANSI/ISA-62443-4-1: revise treatment of levels as related to SDA-S certification criteria, add reference to SSA-100 for relationship to IEC 62443, revise normative references and bibliography
1.6	2019.08.18	State that SDLA certification is a requirement; add explanatory notes regarding ANSI/ISA vs. IEC 62443-4-2; revise note to clarify case in which SDA differs by level

Contents

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 Component Security Assurance (CSA) for software applications, embedded devices, host devices, and network 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 document in the series that specifies the technical 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

In order for a control system to pass an ISASecure SSA (System Security Assurance) certification as defined in [SSA-100] per the technical pass criteria in [SSA-300], it must pass several evaluation elements. One of these elements is a security development artifact assessment for the system (SDA-S). The purpose of this document is to state the criterion for passing the SDA-S element of an SSA certification evaluation.

In order to define the criteria for passing SDA-S, this brief document refers to the separate document [SDLA-312] that includes an enumeration of the detailed technical requirements for the SDA-S.

2 Normative references

2.1 General technical specifications

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

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

[SDLA-100] *ISCI Security Development Lifecycle Assurance – ISASecure certification scheme*, 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

2.2 IACS security standards

NOTE 1 [SSA-100] describes the relationship of ISASecure SSA to the ANSI/ISA/IEC 62443 series of standards.

NOTE 2 The following pairs of references that have the same document number 62443-m-n, provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

[ANSI/ISA-62443-1-1] ANSI/ISA−62443−1−1 (99.01.01) - 2007, *Security for industrial automation and control systems Part 1-1: Terminology, concepts and models*

[IEC 62443-1-1] IEC TS 62443-1-1:2009 *Industrial communication networks - Network and system security -Part 1-1: Terminology, concepts and models*

[ANSI/ISA-62443-3-3] ANSI/ISA−62443−3−3 (99.03.03) - 2013 *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

[IEC 62443-3-3] IEC 62443−3−3:2013 *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

NOTE 3 [SDLA-312] is based upon the following standard.

[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*

3 Definitions and abbreviations

3.1 Definitions

3.1.1
artifact
tangible output from the application of a specified method that provides evidence of its application

NOTE Examples of artifacts for secure development methods are a threat model document, a security requirements document, meeting minutes, internal test results.

3.1.2
capability security level
security level that a component or system can provide when properly configured and integrated

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.

3.1.3
certifier
chartered laboratory, which is an organization that is qualified to certify products or supplier development processes as ISASecure

NOTE This term is used when a simpler term that indicates the role of a “chartered laboratory” is clearer in a particular context.

3.1.4
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.5
industrial automation and control system
collection of personnel, hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process

3.1.6
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.

3.1.7
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.

3.1.8
target security level
desired security level for a particular zone

NOTE This is usually determined by performing a risk assessment on a system and determining that particular zones need a particular level of security to ensure its correct operation.

3.1.9
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document

ANSI	American National Standards Institute
DCS	distributed control system
IACS	industrial automation and control system
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
PLC	programmable logic controller
SDA-S	security development artifacts for systems
SDLA	security development lifecycle assessment
SIS	safety instrumented system
SSA	system security assurance

4 Background

The document [SSA-100] provides general background on the ISASecure programs, the ISASecure SSA certification program for systems, and its relationship to the ANSI/ISA/IEC 62443 standards. This clause discusses the rationale and structure of these programs as it relates to SDA-S.

The evaluation of secure development lifecycle processes is a key characteristic of the ISASecure certification programs. This evaluation has two aspects. The first aspect is to determine whether a *supplier has defined and is maintaining* a documented secure product development lifecycle process. The second aspect is to determine whether the supplier is *following* the documented process.

In order to achieve a product certification under ISASecure SSA for a system, both aspects are required. First, an assessment is required to determine whether the supplier has defined and is maintaining a documented development process that meets ISASecure SDLA requirements. This assessment is done as part of the evaluation toward an ISASecure SDLA certification of the supplier's secure product development lifecycle process, which is a prerequisite to SSA certification.

Secondly, the ISASecure SSA certifier will verify that the required artifacts that result from carrying out the documented secure product development lifecycle process exist for the specific system that has been presented as a candidate for certification. This aspect of an SSA evaluation is called Security Development Artifacts for systems, or SDA-S. SDA-S is the topic of the present document.

The requirements for a secure product development lifecycle process and the requirements on the artifacts that result from the implementation of that process are closely related. For this reason, the document [SDLA-312] covers both the requirements assessed for an ISASecure SDLA certification evaluation of a supplier's development lifecycle process, and the requirements assessed for the SDA-S element of an ISASecure SSA certification evaluation of a supplier's system. Whereas an ISASecure SDLA certification requires examining process documentation and *representative samples* of artifacts for secure development methods that comprise that process, the SDA-S requirements call for artifacts resulting from these same methods, *for the specific system* that is a candidate for ISASecure SSA certification.

A system submitted for certification is comprised of one or more security zones. The supplier identifies these zones and the capability security level to which each zone will be evaluated for certification, as part of their application for certification, as described in [SSA-300]. These levels will impact the SDA-S evaluation as described in the following section.

5 Criterion for passing SDA-S for SSA certification

Requirement ISASecure_SDA-S.R1 – Criterion for passing SDA-S

A system SHALL pass the security development artifacts evaluation (SDA-S) element of an evaluation for ISASecure SSA certification if requirements in [SDLA-312] that are in rows that have the "System" column marked with an ‘X’, pass verification.

Verification is performed per the column labeled "**Component or System Validation Activity**" in [SDLA-312]. For requirements where this validation activity depends upon capability security level, the validation shall be performed for each security zone, in particular for the elements of the system that support that zone and the capability security level for which that zone is evaluated.

NOTE 1 Most SDA-S requirements do not depend upon capability security level. In SDLA-312 version 5.5, only SDLA-DM-4 regarding allowable residual risk for known security issues, depends upon it.

NOTE 2 A product developed for a particular capability security level, could seek certification to any capability security level less than or equal to that intended capability security level. Thus a supplier may specify and develop a system zone as capability security level 2, and apply for certification to ISASecure SSA capability security level 1, for that zone, for example, as an interim milestone.

NOTE 3 For existing products which predate an organization’s adoption of a well-defined secure development process, artifacts to satisfy SDA-S may be created during the organization’s transition to that process.