SSA-312

ISA Security Compliance Institute — System Security Assurance –

Security development artifacts for systems

Version 1.01

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
1.01	2014.02.10	Initial version published to http://www.ISASecure.org

Contents

1 Scope 6

2 Normative references 6

3 Definitions and abbreviations 6

3.1 Definitions 6

3.2 Abbreviations 7

4 Background 7

5 Criterion for passing SDA-S for SSA certification 8

Requirement ISASecure_SDA-S.R1 – Criterion for passing SDA-S 8

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 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

[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

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

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
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.

3.1.6
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

3.1.7
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.

3.1.8
security zone
grouping of logical or physical assets that share common security requirements

NOTE 1 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.

3.1.9
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.

3.1.10
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document

DCS	distributed control system
EDSA	embedded device security assurance
IACS	industrial automation and control system
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

General background on the ISASecure programs and the ISASecure SSA certification program for systems is provided in [SSA-100]. This clause discusses the rationale and structure of these programs as it relates to SDA-S.

The evaluation of security development 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 development 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 can be done separately as part of the evaluation toward an ISASecure SDLA certification of the supplier's development process. It may also be done as part of the ISASecure SSA certification process itself.

Secondly, the ISASecure SSA certifier will verify that the required artifacts that result from carrying out the documented development process exist for the specific system product that has been presented as a candidate for certification. This aspect of an SSA product 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 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 product. 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 a desired capability security level for each zone as part of their application for certification. 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 meet the following selection criteria, pass verification:

- Requirement is in a row labeled "**System**"
- Requirement is applicable to a capability security level for some zone in the system, as seen in the column labeled **"ISASecure Level."**

Verification is performed per the column labeled "**Component or System Validation Activity**" in [SDLA-312], for elements of the system that support zones with a capability security level equal to the security level of the requirement. Therefore, for example:

- verification for requirements designated for security levels "1, 2, 3, 4," applies across the entire system;
- verification for requirements designated for security levels "2, 3, 4" applies to software, hardware and tools that support system zones to be certified at level 2 or higher.

NOTE 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.

BIBLIOGRAPHY

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

[2] ISA 62443-3-2, *Security for industrial automation and control systems – Security risk assessment and system design* (under development February 2014)

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

NOTE 1 It is the intent going forward to align ISASecure SDLA certification and SDA-S for ISASecure SSA with the approved version of the following standard.

[4] ISA 62443-4-1 *Security for industrial automation and control systems – Product development requirements* (under development February 2014)

NOTE 2 The following technical specification in the ISASecure SSA series specifies that a system candidate for ISASecure SSA certification is partitioned into zones.

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