SSA-300

ISA Security Compliance Institute – System Security Assurance –

ISASecure® certification requirements

Version 3.1

August 2019

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
1.1	2014.02.09	Initial version published to http://www.ISASecure.org
1.4	2015.04.08	Use acronym SDLPA, clarify relationship to VIT in EDSA, update definition of ISASecure certification version, add figure depicting certification elements, no CRT/NST on perimeter firewall, clarify time for holding SDLA cert
2.0	2018.02.02	Align with ISA 62443-4-1: revise requirements and example since all SDLA requirements are now applicable at all levels, with a few validation differences by capability security level, ANSI/ISA- 62443-4-1 moved to normative references; address scalable systems: 1.2 description of what can be SSA-certified, clause 2 definitions of layout, reference layout, reference system, scalable control system, summary of certification approach for scalable systems at end of 4.2, add 5.2 zone types and layouts including three new numbered requirements, modifications to existing numbered requirements to address scalability, modifications to example in Clause 6 including figures, to illustrate certification of scalable system; apply erratum from SSA-102 v1.6
2.2	2018.10.02	Align with ISA-62443-4-2: update normative references; remove term allocatable and modify definition of supported; modify description of FSA-E in 4.2 and 5.4 Table 2; update FSA-E example in 7.1.1
3.1	2019.08.18	Update along with transition EDSA to CSA: Clarify definition of certification level; systems and zones made up of components instead of devices; add definition of component, host device, network device, software application; remove SRT (CRT/NST) except VIT: remove relationship to EDSA and 62443-4-2; remove FSA-E element of certification; remove option for SDPLA during SSA since SDLA cert is a prerequisite; remove mention of tool recognition; update Figure 1 of certification elements; add example definition in annex for “adequately maintain control capability”

Contents

Table of Tables

Table of Figures

Table of Requirements

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). This specification is the overarching document in the series that describes technical requirements for ISASecure System Security Assurance (SSA) certification of systems. It references all other documents that contain these requirements and places them in context. A description of the ISASecure program and the current list of documents related to ISASecure SSA as well as other ISASecure certification programs can be found on the web site http://www.ISASecure.org.

1 Scope

1.1 Scope of this document

This document defines those systems that fall within the scope of the ISASecure® SSA (System Security Assurance) certification program for control systems, and specifies the criteria for granting an initial certification. An annex contains an illustrative example of how the SSA evaluation would be performed for a specific system. A separate document [SSA-301] covers maintenance of certification for revisions to a system after initial certification has been achieved.

A second annex provides an example of how a supplier testing effort could define whether the control function is adequately maintained during testing.

1.2 Scope of the SSA certification program

ISASecure SSA is a certification program for a particular subset of control systems. A control system that meets all of the following criteria may be certified under the SSA program:

- The control system consists of an integrated set of components and includes more than one component.
- The control system is available from and supported as a whole by a single supplier, although it may include hardware and software components from several manufacturers.
- The control system may be scalable, that is, may support replication of components and/or of security zones in order to support small and large installations.
- The system product is under configuration control and version management.

Small and large versions of a system may be covered by one certification if the control system meets specifications for scaling described later in this document.

NOTE The present specification requires that a security zone breakdown for the system be submitted with an application for system certification.

2 Normative references

2.1 General technical specifications

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

2.2 Specifications for certification elements

NOTE 1 The following document provides the technical evaluation criteria for the Functional Security Assessment element of an SSA evaluation.

[SSA-311] *ISCI System Security Assurance – Functional security assessment for systems,* as specified at http://www.ISASecure.org

NOTE 2 The following documents provide the overall technical evaluation criteria for the Security Development Artifacts element of an SSA product evaluation. [SDLA-312] also provides the technical evaluation criteria for an ISASecure assessment of a supplier's secure product development lifecycle processes for ISASecure SDLA certification.

[SSA-312] *ISCI System Security Assurance – Security development artifacts for systems,* 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

NOTE 3 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier secure product development lifecycle processes.

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

[SDLA-300] *ISCI Security Development Lifecycle Assurance – Requirements for ISASecure Certification and Maintenance of Certification,* as specified at http://www.ISASecure.org

NOTE 4 The following document specifies procedures and policy parameter values used to perform Vulnerability Identification Testing (VIT-S) for a system.

[SSA-420] *ISCI System Security Assurance – Vulnerability Identification Test Specification*, as specified at http://www.ISASecure.org

2.3 IACS security standards

NOTE 1 The content of the following standards was central to the development of the ISASecure SSA certification criteria. It is however not strictly speaking necessary to refer to these documents in order to achieve compliance with the SSA program requirements. However, these standards are essential in order for system integrators to design useful security zones and select appropriate associated capability security levels for these zones. Likewise, these standards are required for asset owners to understand the capability security levels appropriate for a specific system deployment.

NOTE 2 [SSA-100] describes the relationship of ISASecure CSA to the ANSI/ISA/IEC 62443 series of standards.

NOTE 3 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*

NOTE 4 [SSA-311] is based upon the following standard.

[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 5 [SSA-312] and [SDLA-312] are 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
accessible network interface
network interface declared by the system certification applicant as suitable for use during operation or maintenance, and such that connection can occur without physical reconfiguration

NOTE Some network interfaces on systems are internal connections only, and/or have physical protection intended to help prevent an unauthorized network connection. These would not be considered to be accessible network interfaces.

3.1.2
adequately maintain essential function
maintain essential function at a level deemed suitable for a control system or component while under a given type of attack or stress

3.1.3
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.

3.1.4
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.

3.1.5
certification level
capability security level for which conformance is demonstrated by a certification

NOTE An SSA certification assigns a capability security level 1, 2, 3, or 4 for each security zone in a control system. A zone certified to capability security level *n* meets requirements for capability security level *n* as defined in the standard [IEC 62443-3-3].

3.1.6
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.

3.1.7
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.8
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.9
device

asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

NOTE Examples include DCS computers, substation computers, PLCs, RTUs, sensors, etc.

3.1.10
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.

3.1.11
essential function
function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries, additional functions such as history may be considered essential.

3.1.12
host device
general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

3.1.13
independent test
form of requirements validation that requires the certifier's exercise of the entity under evaluation itself, or exercise of a development tool used by the supplier of that entity

NOTE In contrast, some requirements may be validated by an examination of documents alone.

3.1.14
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

3.1.15
initial certification
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of a product under evaluation or of any of its prior versions

NOTE The first ISASecure SSA certification for a system is considered an initial certification *of that system*, regardless of whether *components* of the system are ISASecure certified.

3.1.16
ISASecure version
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 SSA 4.0.0

3.1.17
layout
description of a specific instance of a scalable control system, that defines quantities of zones and resident components, and internal and external interfaces

3.1.18
network device
device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

3.1.19
reference layout
specific layout for scalable control system, that represents security characteristics found in any layout to be SSA certified, in a manner suitable to support testing that provides assurance for all such layouts

NOTE A reference layout may be neither the minimum nor the maximum layout for a scalable system. Its properties are specified in a requirement in the present document. In overview, the reference layout for a control system includes all zones, resident components in these zones, interfaces and protocols present in any layout in scope for a certification.

3.1.20
reference system
physical instance of a control system, that adheres to a reference layout

NOTE Use of a reference system may be specified for testing, when a system has many layouts.

3.1.21
scalable control system
control system which supports replication of zones and/or components to support small and large installations

3.1.22
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.

3.1.23
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.

NOTE 2 This definition and NOTE 1 are from [IEC 62443-3-3]. A security zone configuration is part of the system architecture diagram submitted by applicants for ISASecure SSA certification, as required by the present specification.

3.1.24
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1 Software applications typically execute on host devices or embedded devices.

NOTE 2 Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

3.1.25
supported
provided by the entity under evaluation itself

NOTE This term is used when referring to security functionality.

3.1.26
system
control system

NOTE In the ISASecure SSA documentation, this shorter term is used for convenience to refer to a control system that may fall under the scope of ISASecure SSA certification. Per the definition above, control systems include safety systems.

3.1.27
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.

3.1.28
zone
security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ANSI	American National Standards Institute
ASCI	Automation Standards Compliance Institute
CD	compact disc
CSA	Component Security Assurance
DC	data confidentiality
DCS	distributed control system
DM	defect management
DVD	digital versatile disc
ED	embedded device
FSA-S	functional security assessment for systems
HMI	human machine interface
IAC	identification and authentication control
IACS	industrial automation and control system
ISA	International Society of Automation
IO	input/output
IP	Internet protocol
ISCI	ISA Security Compliance Institute
LAN	local area network
NA	not applicable
OS	operating system
PLC	programmable logic controller
RDF	restricted data flow
SCADA	supervisory control and data acquisition
SD	secure digital (as in SD card reader)
SDA-C	security development artifacts for components
SDA-S	security development artifacts for systems
SDLA	security development lifecycle assurance
SDLPA	security development lifecycle process assessment
SI	system integrity
SIF	safety instrumented function
SIS	safety instrumented system
SL-C	capability security level
SSA	system security assurance
SUT	system under test
SY	system
TCP	transmission control protocol
TRE	timely response to event
UC	use control
UDP	user datagram protocol
USB	universal serial bus

VIT-S	vulnerability identification testing for systems

4 Overview of SSA Certification

4.1 Use cases

This sub clause describes several types of systems to which the SSA certification program applies, subject to the basic conditions listed in 1.2. These use cases are meant to describe typical product offerings to which SSA certification applies. SSA certification may also apply to types of products not described here that meet the conditions listed in 1.2.

Use cases suitable for SSA certification include Control System Platforms and Packaged Control Systems.

4.1.1 Control System Platforms

Control system platforms are typically vendor specific platforms that are designed to integrate the control and/ or supervisory functions of automation systems. There are two main types of control system platforms – tightly integrated and supervisory.

Tightly integrated platforms are typically automation and control vendor platforms designed to integrate the administrative, supervisory, control and IO functions. Typically, these systems include all of the hardware and software components necessary to build a complete control system.

Supervisory platforms typically include only the software components for performing administrative and supervisory functions for integration with a variety of hardware components.

4.1.2 Packaged Control Systems

Packaged control systems are systems that are designed for a specific type of application. There are two main types of packaged control systems – equipment independent and equipment specific.

Equipment independent systems are packaged control systems pre-engineered for a type of application. These systems usually come packaged with typical components used for a specific type of application but must be further engineered for the specific equipment and user.

Equipment specific systems are packaged control systems delivered as an integrated package. Equipment specific systems are typically pre-wired and pre-configured to control specific process equipment, which may or may not be included (e.g. a skid-mounted package). Examples are boiler control system, burner management systems, drilling control systems, wellhead control systems, ovens, dryers, packaging machines, reactors, distillation, fermenters, centrifuges, oxidizers, reformers, extruders, turbine control systems.

In summary, control systems to which SSA certification applies may:

- support administrative and supervisory functions only, and be designed for integration with a variety of control components; or
- support administrative and supervisory functions only, and be designed for integration with specific control components; or
- include control functions as part of the system itself.

Systems of the following types are examples of the range of systems to which ISASecure SSA certification may apply. The definitions here for DCS and SCADA are from the standard [IEC 62443-1-1].

- **HMI/PLC combination system** refers to a supplier offering of one or more HMIs (human machine interfaces) integrated with specific PLC (programmable logic controller) products, to create a system.

Such a system may be a tightly integrated control system platform or an equipment independent packaged control system.

- **Supervisory Control and Data Acquisition (SCADA) system** refers to a type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems.

  Supervisory control systems are also used within batch, continuous, and discrete manufacturing plants to centralize monitoring and control activities for these sites.

- **Distributed Control System (DCS)** refers to a type of control system in which the system elements are dispersed but operated in a coupled manner.

  Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems.

  Distributed control systems are commonly associated with continuous processes such as electric power generation, oil and gas refining, chemical, pharmaceutical, and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, and warehousing.

SCADA and DCS system products may be offered as any of the above described types of control platforms or packaged control systems.

- **Safety Instrumented System (SIS)** systems are specifically designed to monitor certain conditions and act on those conditions to maintain the safety of the personnel and the facility. An SIS is composed of any combination of sensor(s), logic solver(s), and actuator(s). Since an SIS incorporates actuators, it may be offered as a tightly integrated control platform, or a packaged control system, which may be equipment independent or dependent.

4.2 Criteria for certification

This sub clause provides an overview of the requirements for SSA certification of a system. Clause 5 formally presents these requirements. Clause 6 describes the application of these requirements to an example system.

To specify SSA certification criteria, this document references other specification documents that cover detailed requirements for the elements of certification:

- Security Development Lifecycle Process Assessment for systems (SDLPA-S);
- Security Development Artifacts for systems (SDA-S);
- Functional Security Assessment for systems (FSA-S); and
- Vulnerability Identification Testing for systems (VIT-S).

While SDLPA-S is an evaluation of the system supplier's secure product development lifecycle process, SDA-S examines the artifacts that are the outputs of that process for the system to be certified. FSA-S examines the security capabilities of the system. VIT-S scans all components of a system for the presence of known vulnerabilities.

The following figure illustrates the elements of ISASecure SSA certification.

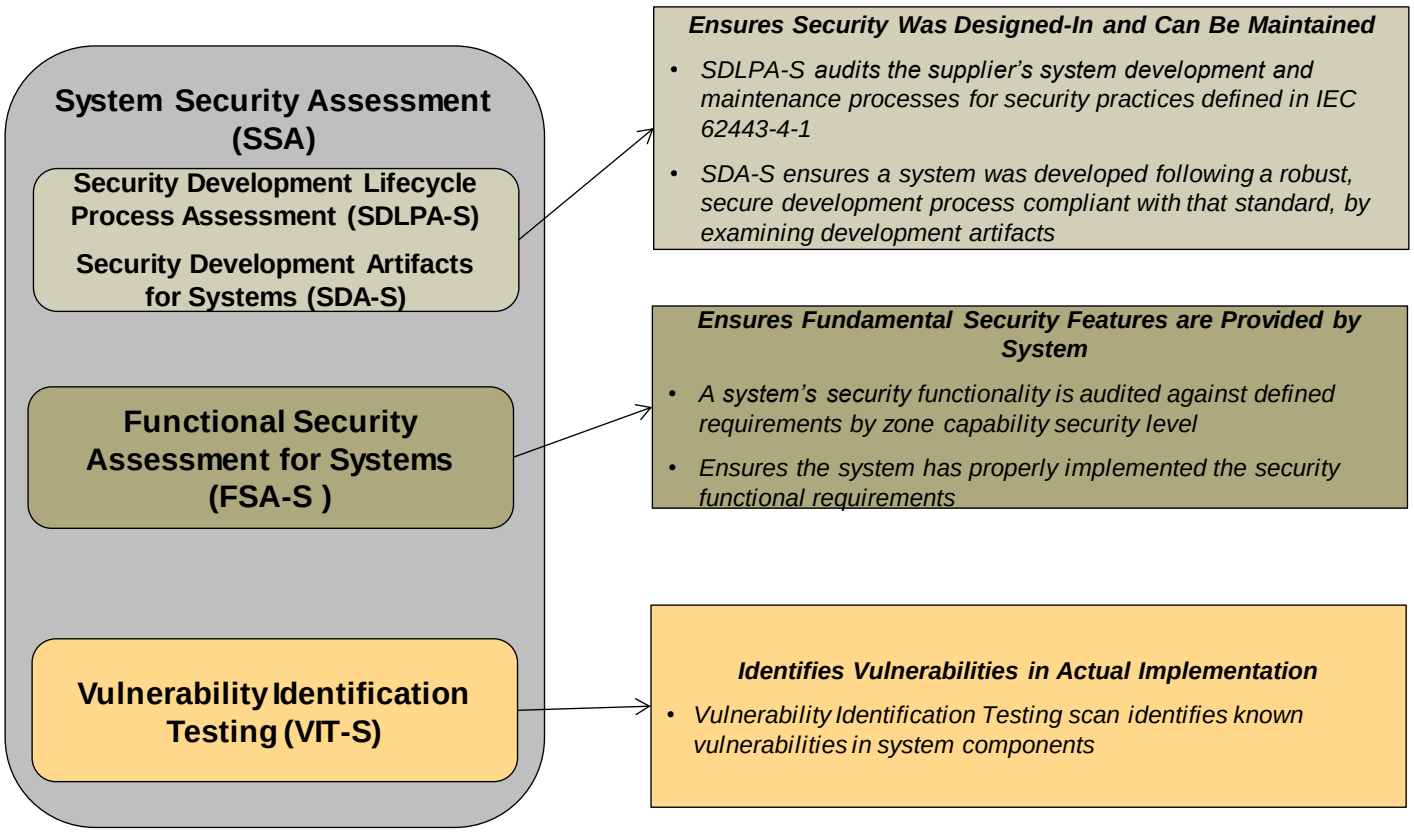

Figure 1 - Evaluation Elements for ISASecure SSA Certification

A system submitted for certification is comprised of one or more security zones. The supplier identifies a desired capability security level for each zone to be demonstrated by the certification. The SDLPA assessment does not have an associated level. SDA-S and VIT-S are the same for all certification levels with the exception of allowable residual risk for known security issues. The FSA-S evaluation is applied to each security zone; required security capabilities will differ based upon the zone capability security level. The ISASecure SSA certificate for a system will name the security zones and their certified capability security levels.

NOTE In SDLA-312 v5.5, certifier validation for requirement SDLA-DM-4 which applies for SDA-S, differs by capability security level. SDLA-DM-4 states that products certified to higher capability security levels require lower residual risk, in particular where this is affected by the severities of unmitigated vulnerabilities identified in the product.

To certify a scalable control system where several layouts of this system are to be certified under one certificate, tests performed by the certifier as part of FSA or for VIT-S will be performed on a reference system, whose associated reference layout meets criteria specified in this document. Analyses performed by the certifier will consider all layouts to be evaluated under the certification.

4.3 Program background and implementation

The ISASecure certification program has been developed by an industry consortium called the ISA Security Compliance Institute (ISCI) with a goal to accelerate industry wide improvement of cyber security for Industrial Automation and Control Systems (IACS). ISASecure SSA supports this goal by offering a common standards-based, industry-recognized set of system and development process requirements that drive system security, simplifying procurement for asset owners, and system assurance for system suppliers.

It is a goal for the ISASecure programs to support and align with the developing standards ANSI/ISA/IEC 62443 for IACS security. [SSA-100] discusses the relationship between ISASecure SSA and the ANSI/ISA/IEC 62443 effort.

ASCI (Automation Standards Compliance Institute) will accredit private organizations to perform ISASecure SSA certification evaluations as “certifiers”.

NOTE ISCI is organized under the umbrella structure provided by ASCI.

ASCI grants accredited certifiers the right to grant ISASecure SSA certifications for systems based upon the certifier’s tests and assessments conforming to ISASecure SSA specifications listed in Clause 2. Subject to permission of each system supplier, ISCI will post the names of certified systems on its web site http://www.ISASecure.org.

ISCI also has developed certification programs for:

- IACS components, the ISASecure CSA program (Component Security Assurance)
- supplier development lifecycle process for control systems and components, the ISASecure SDLA program (Security Development Lifecycle Assurance), defined in certification scheme document [SDLA-100].

5 Certification requirements

5.1 General

This clause provides an informal overview of scalability concepts, and then formally defines the requirements to achieve ISASecure SSA certification for a system.

5.2 Zone and layout definition

The present specification requires that a security zone breakdown for the system be submitted with an application for system certification. A control system may scale by replicating components, or zones, or both. One or several instances of a zone may be used in a system layout. The supplier specifies a zone by defining the components and their quantities that may reside in that zone, together with the internal and external protocols that may be used for zone communications, and the capability security level to be applied to all instances of that zone. An example of a specification for a zone called Processing Zone is shown in columns 1-7 of Table 1 below.

A particular selection of quantities of zones, and quantities of resident components in those zones that make up an instance of the control system, is called a *layout*. For a particular certification, the set of layouts to be covered by the certification will be specified.

Thus, for example, consider a control system for which only one zone called Processing Zone described in columns 1-7 of Table 1 has been specified. One possible layout for this control system might consist of two instances of Processing Zone, where one of these instances has one operator workstation and the other instance has three, and where the embedded devices in these zones communicate peer-to-peer using UDP. Another possible layout is the same as the one just described, except both zones have three workstations and the embedded devices do not employ peer-to-peer communication. An example of a description for a set of layouts a supplier might apply to certify, which includes these two example layouts and many others, is shown in Table 1. The table including the last column, conveys the fact that this supplier wishes to certify a control system that consists of up to 10 instances of Processing Zone with capability security level 1, where each of these zone instances may have any of the component quantities permitted for this zone, and where peer-to-peer communication between embedded devices may or may not be present between any pair of instances of these zones.

Table 1 - Example Layout Specification Using Multiple Instances of One Zone

Zone	Resident Components	Min and Max Quantity of Components in Zone	Protocols Internal to Zone	Protocols Internal to System Crossing Zone Boundary	Protocols Crossing System Boundary	Capability Security Level to be Certified	Min and Max Quantity of Instances of Zone
Processing Zone	BestControl Embedded Device Model XYZ Version 1.6	1	Modbus TCP (Operator workstation to embedded device)	UDP (embedded device peer-to-peer to another Processing Zone, optional)	HTTP, HTTPS (Windows updates to operator workstation)	1	1-10
	Best Operator Workstation Model ABC Version 2.2	1-3					

Many control systems will have more than one type of zone, and therefore there will be more than one row in the corresponding table that describes layouts to be certified for such systems.

It is possible that zones are not replicated to achieve system scaling, rather only components within zones may appear in varying quantities. For some systems, neither zones nor components may be used in varying quantities, in other words the system layout is fixed.

The following requirements formalize the above discussion. They do not apply to systems for which a single fixed layout is presented for certification.

Requirement ISASecure_SY.R1 – Zone definition for scalable systems

If a system uses replication of zones or components to scale for small and large installations, then in order that multiple layouts be considered under one certification, the certification applicant SHALL define a set of zones to be evaluated in the certification as follows. A zone SHALL be specified by:

- minimum and maximum quantities of each component permitted to reside in the zone
- protocols used, and optionally used, only internally to the zone
- protocols used, and optionally used by the zone to communicate to other instances of this zone in the system, or to other zones
- protocols used, and optionally used by the zone to communicate outside the system
- capability security level to which the zone is to be certified.

The format in Table 1 columns 1-7 SHOULD be used to define the set of zones to be evaluated in the certification.

Requirement ISASecure_SY.R2 – Layouts in scope for certification

If a system uses replication of zones or components to scale for small and large installations, then in order that multiple layouts be considered under one certification, the certification applicant SHALL specify the set of system layouts for which they would like to achieve certification.

This set of layouts SHALL be described by:

- specifying the minimum and maximum quantity of zone instances permitted for each zone specified in ISASecure_SY.R1 and;
- stating that either:
  - The supplier is applying for certification of systems with layouts consisting of all combinations of zone instances for the zones meeting characteristics specified under ISASecure_SY.R1 and subject to the zone instance quantity constraints.
  - The supplier is applying for certification of systems with layouts consisting of a proper subset of all combinations of zone instances for the zones meeting the characteristics specified under ISASecure_SY.R1, and subject to the zone instance quantity constraints.

If a proper subset of combinations is presented for certification (meaning the subset does not consist of all combinations meeting the stated criteria), the supplier SHALL provide a description of that subset.

All layouts in scope for certification SHALL include all components required to meet requirements found in [SSA-311] for the capability security level to which each zone will be certified.

NOTE If the supplier is applying for certification of all combinations of zone instances per the first sub bullet above, then a table in the form of Table 1 will fully describe the set of system layouts. As an example of a description of a proper subset of layouts to be certified, a supplier could present for certification all system layouts possible under Table 1, subject to the further restriction that the supplier supports a maximum of 20 operator workstations across the overall system.

As will be stated below in ISASecure_SY.R16, although a number of layouts may be in scope for a certification, one reference system that adheres to a reference layout will be used for testing that is performed by the certifier. The following requirement specifies the characteristics of a reference layout.

Requirement ISASecure_SY.R3 – Reference layout

If a system uses replication of zones or components to scale for small and large installations, then in order that multiple layouts be considered under one certification, the supplier SHALL identify a reference layout with the following characteristics, from among the layouts in scope for the certification as identified per ISASecure_SY.R2:

- The layout includes all zones identified per ISASecure_SY.R1
- Each instance of a zone includes all permitted types of components for that zone
- Each instance of a zone supports all protocols present in any layout for that zone in scope for certification
- Each instance of a zone supports all software present in any layout for that zone in scope for certification
- The layout exposes all external interfaces present in any layout in scope for certification
- The layout includes all interfaces present between instances of the same or different zones, in any layout in scope for certification.

NOTE 1 As examples, this requirement implies the following particular constraints. (1) Adding redundant components such as replicated pairs of servers, may add new protocols to the system. In such cases, redundant components will appear in the reference layout. (2) If there may be an interface between instances of the same zone, at least two instances of this zone will appear in the reference architecture to represent that interface.

NOTE 2 Under SDA-S as specified in [SSA-311], the certifier also validates that fuzz and network traffic load tests performed by the supplier either are run on a system meeting the requirements of a reference layout, or a rationale is provided that equivalent or better test coverage over all layouts to be certified, has been achieved.

5.3 Zone certification levels and certification version

Requirement ISASecure_SY.R4 – Application for security zone certification levels

When a supplier applies for certification of a system, the certification applicant SHALL specify the maximum capability security level for which they would like to achieve certification for each security zone. The levels possible are capability security levels 1, 2, or 3, or 4. The certifier SHALL award certification designating each security zone at the highest level for which the security zone qualifies, up to this maximum level.

Requirement ISASecure_SY.R5 – Publication of system certification status

If ISCI, the certifier, or the system supplier publishes certification status information for certified systems in a public venue, information provided SHALL include the most granular version identifier of the system to which the ISASecure SSA certification applies, and SHALL specify the layouts covered under the certification (which may take the form of a reference to a separate document), and the version of the certification achieved, such as ISASecure SSA 4.0.0.

5.4 Technical submissions from certification applicant

Requirement ISASecure_SY.R6 – ISASecure application requirements for certification

Items specified as follows SHALL be submitted to the ISASecure SSA certification process by an applicant for an initial certification:

a) technical items as required by this specification and the specifications listed in Clause 2;

b) administrative and potentially additional technical items defined by the certifier.

Requirement ISASecure_SY.R7 – Submission of architecture diagram of system

A certification applicant SHALL submit an architecture diagram of the reference system to be tested that clearly defines its components and connections. The architecture diagram SHALL show every component (embedded, I/O, PC, network, etc.) included in the system along with its connections to other components in the system and external to the boundaries of the system. The diagram SHALL show the boundaries of the system as well as the boundaries of all included security zones within the SUT, and all communication protocols that traverse the boundary of the system, including IP as well as I/O communications protocols (wired or wireless).

NOTE 1 Figure 2 shows an example architecture diagram.

Requirement ISASecure_SY.R8 – Submission of list of system hardware and software (e.g. Bill of Materials)

A certification applicant SHALL submit a system for testing that is or will be unambiguously identifiable and specifiable by an end customer for procurement. The information submission SHALL be for each component defined in the Bill of Material and SHALL include:

- Manufacturer, and part numbers of all embedded devices;
    - Hardware, firmware, and software versions of each embedded and I/O component.
- Manufacturer, and part numbers of all hosts;
    - Hardware;
    - OS, OS version and service pack levels;
    - VM OS versions and service pack levels (if Virtual Machines are included).
- Applications installed on all hosts:

    - Certification applicant developed and third party application name and type;
    - Versions and service pack versions of all installed and included applications.
- Manufacturer, and part numbers of all network components with:
    - Version and service pack levels;
    - Details of configuration rules (e.g. ACL's).

Requirement ISASecure_SY.R9 – Submission of end user system documentation

The certification applicant SHALL submit to the certification process all documentation (printed, on-line or otherwise) that is delivered along with, or made available to, an end customer who purchases the system submitted for certification. This SHALL include all manuals and pertinent documentation for each component of the system.

Requirement ISASecure_SY.R10 – Submission of essential function information

The certification applicant SHALL submit a list of essential functions of the system, in accordance with the definition in 3.1.11, and a list of all components of the system that are performing these essential functions. The information may include (optionally) a list of events where associated event record data is considered to be essential history data.

Requirement ISASecure_SY.R11 – Submission of list of accessible network interfaces

A certification applicant SHALL submit to the certification process a list that clearly identifies all network interfaces present for each of the components of the system that they define as *accessible* interfaces. The list SHALL include and identify those accessible interfaces that provide an external interface to the system or to a security zone. The list of accessible interfaces SHOULD include all interfaces such that:

- the certification applicant recommends the interface to customers as suitable for use during operations or maintenance;
- the interface is used to interface with operator consoles or instrumentation; and
- connection to the interface can occur without physical reconfiguration of the normal operational configuration.

NOTE 2 For example, consider a network switch or router that is installed in a cabinet which can be locked by the end user. Physical network ports that have cables outside the cabinet are considered "accessible". Physical network ports that are contained within the cabinet (e.g. maintenance port) are not considered "accessible."

Requirement ISASecure_SY.R12 – Submission of list of accessible points of entry

A certification applicant SHALL submit to the certification process a list that clearly identifies all accessible points of entry for each of the components of the system that is defined as performing essential functions. The list of accessible points of entry SHALL include all points of data entry whether they are enabled or not, and SHALL include:

- all network connections (e.g. Ethernet);
- all local connections (e.g. USB, Firewire, serial);
- all wireless communications or wireless communications options (e.g. Wireless HART, ISA100, WiFi, Bluetooth, wireless mouse, wireless keyboard, etc.);
- all insertable media points (e.g. CD, DVD, floppy disk, SD card readers, etc.).

These SHALL include both hardware and software points of entry.

Requirement ISASecure_SY.R13 – Submission of list of implemented protocols

The certification applicant SHALL submit a list of all IP protocols that are supported on each of the components of the system that are performing essential functions.

Requirement ISASecure_SY.R14 – Submission of description of intended system defensive behavior

For each protocol supported by the system, a certification applicant SHALL submit information that indicates one of:

a) traffic received under that protocol is not subject to rate limiting, in other words the design of the system does not distinguish between rates of incoming traffic

b) traffic received by the system is subject to rate limiting.

Similarly, a certification applicant SHALL provide a description of any other defensive behavior employed by the system that may impact certification assessments. For example, the system may employ IP address blacklisting, where an IP address is blocked if it previously has sent suspicious or excessive traffic to the system, or may employ a redundant configuration that provides automatic failover if one or more of the redundant units detects adverse conditions or fails.

Requirement ISASecure_SY.R15 – Submission of reference system

A certification applicant SHALL submit to the certification process a suitable test system that meets the requirements for a reference layout in Requirement ISASecure_SY.R3, and that is representative of the specified usage of the system to be certified.

5.5 Criteria for initial certification

The following requirement defines the technical criteria for a system to achieve ISASecure SSA certification. It references several SSA program specifications. In particular, [SSA-311] contains a list of functional security requirements by capability security level that must be assessed for each security zone. [SDLA-312] contains a list of requirements on the system development and maintenance process and related artifacts that must be assessed. Validation activities for compliance with these requirements include documentation review, inspection, and in some cases, independent test.

Requirement ISASecure_SY.R16 – Criteria for granting an initial certification

An initial ISASecure SSA certification SHALL be granted for a system if the following requirements are met, as defined in the reference documents shown:

Table 2 – SSA Certification Criteria

Topic	Element	Requirement	Reference Document
Secure Development Processes Implemented by Supplier	SDLPA	The supplier holds an ISASecure SDLA certification, at the time of issuance of the SSA certificate. The system is within the stated scope of the certified process, for development going forward.	[SDLA-300] [SDLA-312]
Secure Development Processes Applied to System	SDA-S	The system passes SDA-S, a review of security development artifacts, for capability security level *n,* for each zone to be certified to capability security level *n*. SDA-S requirements validation SHALL take into account all layouts in scope for the certification.	[SSA-312]
Security Functions of System	FSA-S	All FSA-S criteria applicable to the capability security level to be certified for each security zone, are assessed as either *supported* or *NA* for that zone. If more than one layout is in scope for the certification, FSA-S requirements validation by testing SHALL be performed on a system with a reference layout as defined in requirement ISASecure_SY.R3. Other FSA-S validations SHALL take into account all layouts for each zone in scope for the certification.	[SSA-311]
Vulnerability Identification Testing	VIT-S	The system passes VIT-S, per the pass/fail criteria for capability security level *n*. If more than one layout is in scope for the certification, VIT-S SHALL be performed on a system with a reference layout as defined in requirement ISASecure_SY.R3.	[SSA-420]

6 Annex: System example

6.1 General

This clause describes as an illustration, the evaluations that would be conducted on an example system for SSA certification, in accordance with the specifications listed under Requirement ISASecure_SY.R16. The example is a scalable control system. Therefore, the requirements found in 5.2 apply.

6.2 Example system description

Figure 2 depicts an example reference system for a control system with four security zone instances, two of which are instances of the same type of zone. The rationale for the reference layout is described below. This

system is a tightly integrated control platform that includes safety instrumented system functions, as defined in 4.1.1. The three security zones specified for this system are a process operations zone, a process control zone, and a process safety zone.

It should be noted that the scope of this system is an example for illustration only; is not required that all of the functions depicted in the example that are offered by a supplier, be submitted for SSA certification, or be submitted together as a single system. The "packaging" of functional elements together for certification as one system under SSA is up to the supplier and not determined by SSA certification requirements. A certified system is required to have two components at a minimum according to 1.2. Beyond this, the scope of the system to be certified may be influenced by how a supplier develops and sells various functional elements of an overall solution, and by customer requirements related to these elements. In a different example, a supplier might elect to request certification of the process safety zone separately as a safety "system."

In the example here, each zone has an interface for human interaction with the zone equipment, in particular via operator consoles, a control system engineering workstation and an SIS engineering workstation, respectively.

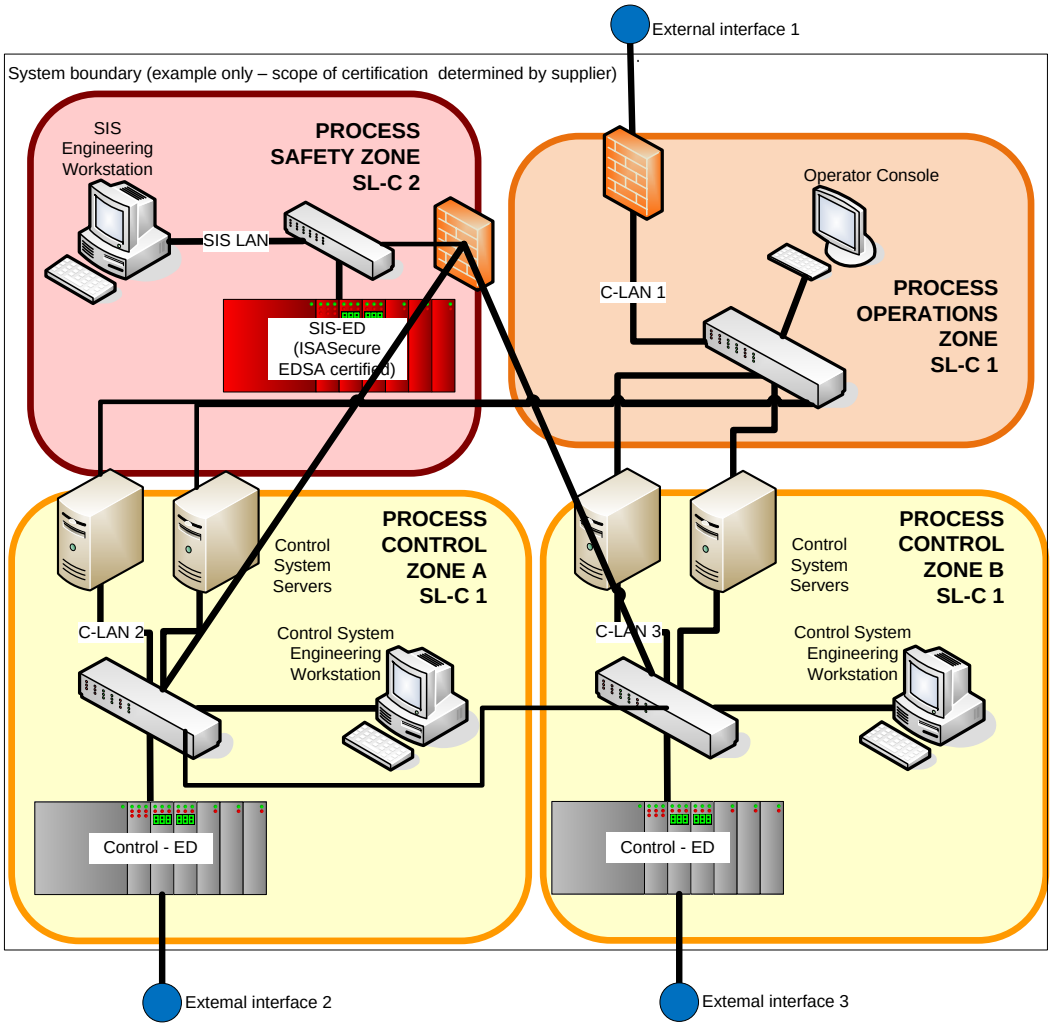

Figure 2 - Reference Layout for Example Scalable System

Up to three instances of this console and these workstations are permitted in their respective zones. The process control zone and process safety zone each contain one PLC (Control-ED and SIS-ED, respectively). The supplier-specified certification level for any process safety zone is capability security level 2; the supplier has specified that the other zones are to be certified to level 1. Therefore, the certification will demonstrate that a process safety zone achieves capability security level 2, and the other zones achieve capability security level 1, as defined in [IEC 62443-3-3].

Each of the security zones forms a separate network segment (C-LAN 1, C-LAN 2, C-LAN 3 and SIS LAN) and thus contains a switch. The system has three external interfaces. External Interface 1 permits higher level business functions to access the process operations zone. External Interfaces 2 and 3 permit the process control equipment to communicate with an external component using an IP network. A firewall protects the system from higher level business functions at the interface to the process operations zone. A second firewall protects the internal system interface into the process safety zone. The interface between the switches for the process control zones is for the purpose of peer-to-peer communication between embedded devices, which is an available option.

Due to the configuration of the firewall that protects External Interface 1, only the IP addresses of the control system servers are visible from that interface.

The supplier's submitted configuration also has internal firewall software incorporated in all of the HMI components (operator consoles, control system engineering workstation, SIS engineering workstation), as well as in the control PLC.

The two control system servers in the process operations zones on C-LAN 2 and C-LAN 3, are also accessible from C-LAN 1, the process operations zone.

An example of a set of layouts that might be requested by a supplier for certification is shown in Table 3. This table follows the format specified in the requirement ISASecure_SY.R2.

Table 3 - Layouts for Example System

Zone	Resident Components	Min and Max Quantity of Components in Zone	Protocols Strictly Internal to Zone	Protocols Internal to System Crossing Zone Boundary	Protocols Crossing System Boundary	Capability Security Level to be Certified	Min and Max Quantity of Instances of Zone
Process Operations	Operator Console	1-3	None	HTTPS (to Process Control zone, view and control via servers)	HTTP, HTTPS (Windows updates to zone components, external visibility to process data)	1	1
	Switch	1					
	Boundary firewall	1					
Process Control	Engineering Workstation	1-3	Modbus TCP (configuration, control and view via control system servers or engineering workstation) Protocol ABC (for server replication if 2 servers)	Modbus TCP (peer-to-peer communication to embedded device in another Process Control zone) Protocol XYZ for communication to Process Safety zone	Fieldbus (external communication with embedded device)	1	1-6
	Control System Server	0-2					
	Control-ED	1					
	Switch	1					
Process Safety	SIS Engineering Workstation	1-3	Protocol DEF between SIS Engineering Workstation and SIS-ED	Protocol XYZ for communication to Process Control zone	None	2	0-2
	SIS-ED	1					

Zone	Resident Components	Min and Max Quantity of Components in Zone	Protocols Strictly Internal to Zone	Protocols Internal to System Crossing Zone Boundary	Protocols Crossing System Boundary	Capability Security Level to be Certified	Min and Max Quantity of Instances of Zone
	Safety firewall	1					
	Switch	1					

A reference layout intended to adequately represent all of these layouts for testing, in accordance with ISASecure_SY.R3, must include:

- Two process control zones, since one such zone may have an interface to another (peer-to-peer connection of embedded devices)
- Two control system servers in each process control zone, since having two servers introduces a replication protocol to the system.

Other than these cases, the reference layout for this control system may contain the minimum number of zones and components represented in the set of layouts in scope for certification described in Table 1, as illustrated in Figure 2.

6.3 Evaluation of the example system

To achieve an ISASecure SSA certification, the system must meet the requirements for the evaluation elements in the table under Requirement ISASecure_SY.R16 in this document. The follow sub clauses discuss each of these elements for the example system.

6.3.1 SDLPA (Security Development Lifecycle Process Assessment)

If the supplier has an ISASecure SDLA development process which applies to this system going forward, the SDLPA criterion is satisfied.

An SDLA certification could be carried out concurrently with the supplier's application for this SSA system certification. The document [SDLA-100] describes the ISASecure SDLA certification program in overview. [SDLA-300] states the criteria for achieving SDLA certification.

To achieve SDLA certification of a process applicable to systems, the supplier lifecycle process would be subject to the SDLA requirements enumerated in [SDLA-312] in cells that meet the criteria that are in rows that have the “System” column marked with an "X," which means the requirement applies to systems. (Some requirements apply to components only.) Validations for SDLPA are in the column titled “**Development Organization and SDL Validation Activity**.”

6.3.2 SDA-S (Security Development Artifacts – System)

To perform the SDA-S evaluation, the certifier will request for review, copies of artifacts that are outputs from secure development methods. These are outputs that apply to systems, as opposed to those that apply to components only. As stated in Requirement ISASecure_SDA.R1 in [SSA-312], these artifacts and the requirements placed upon them are described in [SDLA-312] in rows that have the "System" column marked with an "X."

In accordance with [SSA-312], the validation of these artifacts is performed per the column labeled "**Component or System Validation Activity**" in [SDLA-312]. Validations that depend upon capability

security level must be met for capability security level 2, for system elements that support a Process Safety Zone which is to be certified to capability security level 2, and for capability security level 1 otherwise.

Following are a few examples of artifacts from [SDLA-312] validation requirements that do not depend upon capability security level. These examples are high level summaries of detailed requirements found in [SDLA-312]. The SDLA IDs for these requirements are in parentheses.

- Security requirements specification for the system (SDLA-SR-3)
- Description of all externally accessible exposed network interfaces (SDLA-SD-1)
- Up-to-date threat model (SDLA-SR-2)
- Security guidelines to support installation, operation and maintenance (SDLA-SG-1A, 1B, 1C)
- Documentation identifying externally provided components, associated risks, and how managed (SDLA-SM-9)
- Tracking security issues to closure (SDLA-SM-11)

These artifacts should address the system as a whole. For example, security requirements and a threat model should cover the overall system; providing this information for individual components or security zones is neither required nor sufficient.

The artifacts should also address all layouts in scope for the certification. The specific layout of a system may or may not be relevant to artifacts related to various SDLA requirements. For example, it is expected that the threat model would be impacted by supporting an optional peer-to-peer interface between embedded devices that reside in different instances of the Process Control Zone.

In SDLA-312 v5.5, for the requirement SDLA-DM-4, the SDA-S validation depends upon capability security level. Thus, it must be met for capability security level 2 when evaluated for elements of the system that support the Process Safety zones, and for level 1 for the other zones. The evaluation of SDLA-DM-4 is illustrated as follows.

The source requirement DM-4 in [IEC 62443-4-1] and its SDLPA validation are shown below in Table 4.

Table 4 – IEC 62443-4-1 requirement DM-4 and SDLA-312 SDLPA Validation Activity

SDLA ID	ANSI/ISA-62443-4-1 IEC 62443-4-1 Requirement Name	ANSI/ISA-62443-4-1 IEC 62443-4-1 Requirement Description	Development Organization and SDL Validation Activity
SDLA-DM-4	Addressing security-related issues	A process shall be employed for addressing security-related issues and determining whether to report them based on the results of the impact assessment (DM-3 – Assessing security-related issues). The supplier shall establish an acceptable level of residual risk that shall be applied when determining appropriate way to address each issue. Options include one or more of the following: a) fixing the issue through one or more of the following: 1) defence in depth strategy or design change; 2) addition of one or more security requirements and/or capabilities; 3) use of compensating mechanisms; and/or 4) disabling or removing features b) creating a remediation plan to fix the problem, c) deferring the problem for future resolution (reapply this requirement at some time in the future) and specifying the reason(s) and associated risk(s), d) not fixing the problem if the residual risk is below the established acceptable level of residual risk In all cases the following shall be done as well: e) informing other processes of the issue or related issue(s), including processes for other products/product revisions, and f) inform third parties if problems found in included third-party source code When security related issues are resolved recommendations to prevent similar errors from occurring in the future shall be evaluated. This process shall include a periodic review of open security-related issues to ensure that issues are being addressed appropriately. This periodic review shall at a minimum occur during each release or iteration cycle.	Verify that the process includes this step. Verify that it applies to security issues found internally and externally throughout any phase of the development lifecycle. Verify that there is an established acceptable level of residual risk defined. Verify that the development process states deferring or not fixing the problem is only an option if the risk is less than the established acceptable level of residual risk. The threshold for acceptable risk varies by SL capability (SL-C) of the product is defined using the base CVSS score as follows: SL-C = 1. All "critical" issues identified are either corrected or the reason for them not being relevant has been documented. SL-C = 2. All "critical" and "high" issues identified are either corrected or the reason for them not being relevant has been documented. SL-C = 3. All "critical", "high", and "medium" issues identified are either corrected or the reason for them not being relevant has been documented. SL-C = 4. All issues identified are either corrected or the reason for them not being relevant has been documented. Verify that there is a periodic review of open issues. Verify that a mechanism exists to inform third party suppliers if errors are uncovered in their product.

The following description of the SDA-S validation activity is found in the column labeled "**Component or System Validation Activity**" for SDLA-DM-4 in [SDLA-312].

> View the list of security issues found during development. Verify that a severity was established for all issues and that all issues with a severity above the established level of residual risk were either fixed or addressed in some other manner. Also, verify that all issues of the appropriate severity have been addressed based on the required security level of the product as defined in the development organization verification activity defined for this requirement (e.g. if SL-C = 1, all critical issues identified are either corrected or the reason for them not being relevant has been documented).

The third column in Table 5 shows the application of this validation activity to each zone in the system.

Table 5 - SDA-S Evaluation of SDLA-DM-4 "Addressing security-related issues"

Zone	Certification Level	Validation Activity for Example System By Zone
Process Operations Zone	1	For elements of the system supporting this zone, view the list of security issues found during development. Verify that a severity was established for all issues and that all issues with a severity above the established level of residual risk were either fixed or addressed in some other manner. Also, verify that all "critical" issues identified are either corrected or the reason for them not being relevant has been documented.
Process Control Zone	1	Same as above.
Process Safety Zone	2	For elements of the system supporting this zone, view the list of security issues found during development. Verify that a severity was established for all issues and that all issues with a severity above the established level of residual risk were either fixed or addressed in some other manner. Also, verify that all "critical" and "high" issues identified are either corrected or the reason for them not being relevant has been documented.

6.3.3 FSA-S (Functional Security Assessment – System)

The FSA-S evaluation is an examination of security capabilities of the system that is carried out on a security zone by security zone basis, and is based upon the capability security level for the zone. First, for each security zone, the certifier identifies FSA-S requirements that must be met. These will be the requirements

shown in [SSA-311] as applicable to the capability security level for that zone. For the example system, requirements that must be met for each security zone are checked in Table 6 below.

Table 6 - FSA-S Requirements Applicable to Security Zones of Example System

FSA-S Requirement Identifier (from [SSA-311])	Requirement Name	Requirement Capability Security Level	Process Operations Zone (SL-C 1)	Process Control Zone (SL-C 1)	Process Safety Zone (SL-C 2)
FSA-S-IAC-1	Human user identification and authentication	1, 2, 3, 4	✓	✓	✓
FSA-S-IAC-1.1	Unique identification and authentication	2, 3, 4			✓
FSA-S-IAC-1.2	Multifactor authentication for untrusted networks	3, 4			
FSA-S-IAC-1.3	Multifactor authentication for all networks	4			
FSA-S-IAC-2	Software process and device identification and authentication	2, 3, 4			✓
FSA-S-IAC-2.1	Unique identification and authentication	3, 4			
FSA-S-IAC-3	Account management	1, 2, 3, 4	✓	✓	✓
FSA-S-IAC-3.1	Unified account management	3, 4			
…Table continues for additional IAC requirements and other categories UC, SI, DC, RDF, TRE, etc.					

To assess the requirements identified, the certifier would consider them with respect to each security zone for which they applied, and determine whether the requirement is supported, not supported, or not applicable. In some cases, [SSA-311] specifies that this determination be made by consulting user documentation, or by conducting a test. In other cases, the method for determining the status of the requirement is left to the discretion of the certifier.

As an example, the requirement FSA-S-IAC-1, *Human user identification and authentication* is applicable at all capability security levels. Therefore, for all security zones in the system the certifier will validate it as shown in the “Validation Activity” column of [SSA-311] for this requirement:

“Verify that the SUT can uniquely identify and authenticate all users at all accessible interfaces and record results as:

a. Supported, or

b. Not Supported”

SUT (system under test) refers to any layout for the system in scope of certification as shown in Table 3. If user authentication is built into each component used to construct the system, then the certifier could conclude that the specific layout would not affect compliance to this requirement.

As a second example requirement that would appear in the fully developed FSA-S table, the requirement FSA-S-UC-1.2 *Permission mapping to roles* is required for capability security levels 2, 3 and 4. Therefore it is required only for the Process Safety Zone in the example system. This means that for permissions to perform functions provided in the Process Safety Zone, the certifier will:

“Verify SUT provides the capability to map permissions to roles if authorized by a supervisory level account and record results as:

a. Supported, or

b. Not Supported”

Note that although support for segregation of duties and least privilege is required for all capability security levels and thus all security zones per FSA-S-UC-1 *Authorization enforcement*, the flexible, configurable support for user roles specified in FSA-S-UC-1.2 is applicable for capability security levels 2, 3 and 4. Therefore it would not be required for a Process Operations zone or a Process Control zone, and would be assessed only for a Process Safety zone. The requirement would be assessed for a Process Safety zone, taking into consideration how the feature would be supported in any layout in scope for certification as shown in Table 3.

As a third example requirement that would appear in the fully developed FSA-S table, the requirement FSA-S-UC-9 *Audit storage capacity* is required for all capability security levels. This means that the certifier will:

"Review audit record storage capacity and determine how many records can be stored. Estimate rate of audit record generation based on existing systems. Verify that there is sufficient storage for at least 30 days of audit information based on record generation on existing systems. Review system documentation and verify that the SUT provides mechanisms to reduce the likelihood of this capacity being exceeded (such as warnings when approach the limit or periodic archiving of audit records)."

For the assessment of FSA-S-UC-9, the certifier would consider the system layouts in scope for certification and how storage of audit records is supported for layouts of various sizes.

An example of a requirement whose validation requires direct testing is FSA-S-UC-3.3 *Restricting code and data transfer to/from portable and mobile devices.* This requirement is applicable to all levels. Testing would be performed against all zones of the reference system shown in Figure 2. In particular, the certifier will:

"Configure the system such that portable and mobile devices are not permitted in a certain context. Connect such a device to the system within the prohibited context and attempt to transfer data between the device and the system. Verify that no data can be sent to or from this device and record results as:

a. Supported

b. Not Supported"

In accordance with Requirement ISASecure_SY.R16 – *Criteria for granting an initial certification* in 5.5 of this document, the system will pass the FSA-S element of the evaluation if all FSA-S criteria applicable to the capability security level to be certified for each security zone of the system, are assessed as either *supported* or *NA* for that zone. As illustrated in the examples above, requirements validated by analysis take into account all layouts in scope for the certification; requirements validated by certifier test use the submitted reference system for testing.

6.3.4 VIT (Vulnerability Identification Testing)

For the example system, in accordance with [SSA-420] VIT requirements, vulnerability scanning will be performed at each accessible network interface pictured in Figure 3. The scan will identify known vulnerabilities present in the operating systems and application software running on the workstations. It will also identify well known switch and PLC vulnerabilities applicable to the components used for the system. The reported "risk factors" for the vulnerabilities found are considered when determining whether the results are acceptable, per pass/fail criteria described in [SSA-420].

The certifier may elect that accessible interfaces duplicated between the two Process Control zones (shown as striped blue markers in Figure 3) do not need to be separately tested. It nevertheless is required that both zones of this type be present and operational during VIT.

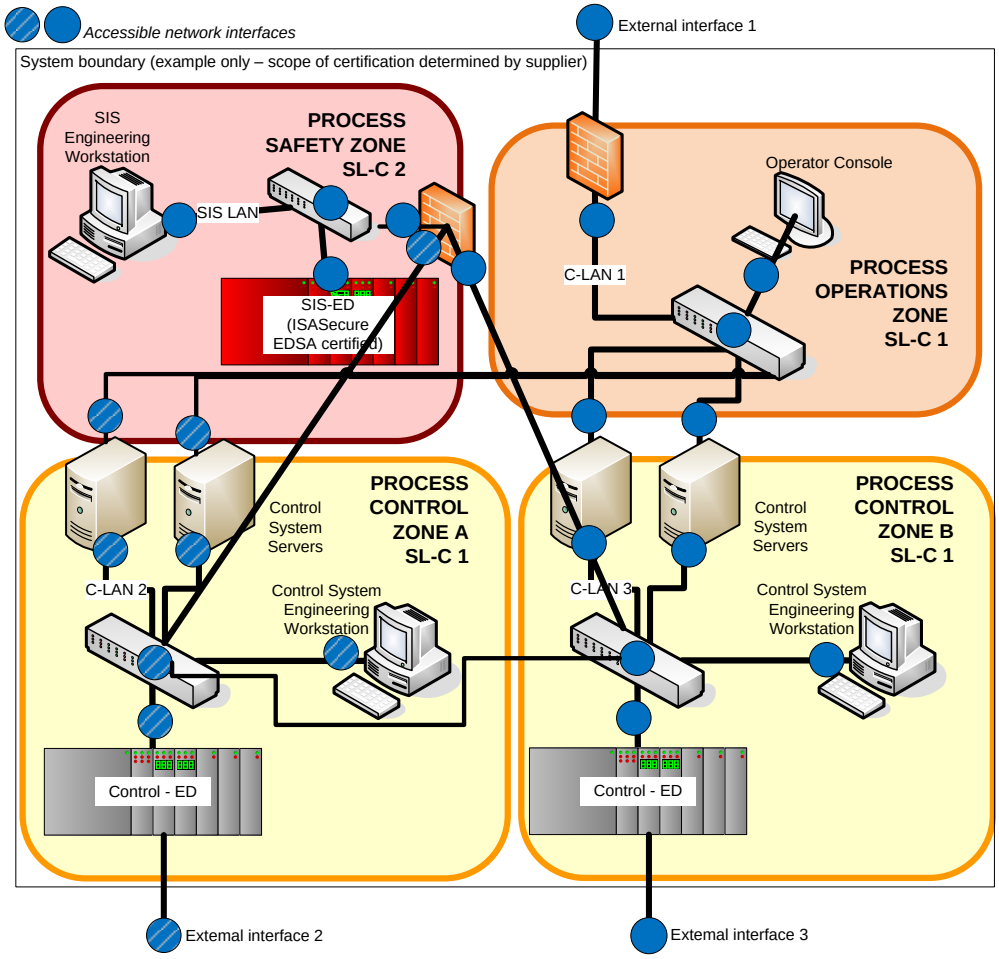

Figure 3 - Accessible Network Interfaces for the Example Reference System

7 Annex: Example test criteria for “adequately maintain control capability”

7.1 General

As part of the SDA-S and SDA-C evaluations for ISASecure SSA and ISASecure CSA certifications respectively, the certifier evaluates testing that has been performed by the IACS supplier. As part of this

evaluation, the test criteria that the supplier uses to determine whether those tests have passed, may be examined. For some tests it is required that “essential functions are adequately maintained,” in order to pass the test. The certifier will verify that this criterion has been applied during supplier testing.

The supplier defines the specific technical interpretation for “adequately maintain essential function” for each essential function, as appropriate for their product and market, and applies those criteria during their testing. This annex provides an example of how one might define such test criteria for the control function. This definition has been implemented by several test tools recognized under the prior ISASecure EDSA (Embedded Device Security Assurance) program.

7.2 Example definition for “adequately maintain control capability”

In order to use the following definition for “adequately maintain control capability,” the IACS device supplier first defines a time unit value for **maximum jitter tolerance for control output (value and confidence)** that represents the expected performance of a device that is creating a control signal. Jitter is the difference between the time a signal event is detected and the expected time, based on a reference signal.

The intent of the following definition is that, for example, during a network flooding test against a device, the control function is adequately maintained if the supplier’s expectation for amount of jitter in a control signal being generated during the test (as expressed by their maximum jitter tolerance), is met during the test period.

Example definition of adequately maintain control capability:

A device is determined to have adequately maintained control capability during a test if a specified cyclically-repeated waveform is measured to have observed time jitter over the test period that meets or exceeds the maximum jitter tolerance and confidence value determined by the device supplier, and does not exhibit specified anomalous behavior, as defined in detail below.

a) for devices that can create an analog output, each cycle of the waveform consists of 10 equal steps of increasing value and then 20 equal steps of decreasing value, both at one step per second, transitioning between the nominal minimum and maximum values of the output device;

b) for devices that can create a digital output, the waveform consists of a rectangular wave with a 1/3 duty cycle and 3 s period, of 1 s at nominal “1” and 2 s at nominal “0”; and

c) these waveforms are generated by the ladder/control/supervisory logic of the device, and not autonomously by the I/O logic

d) both digital and analog outputs with these characteristics are measured if both are present

e) if digital or analog outputs can be conveyed using more than one method (such as via pneumatic, electrical, or using a Fieldbus message), then these outputs for all supported forms of conveyance are monitored per the criteria of this requirement

NOTE 1 This definition is intended to permit the output monitoring process to detect anomalous behavior of the control software of the device, which monitoring could be defeated if low-level I/O were generating the waveform autonomously.

NOTE 2 The intent of this definition is to test whether the supervisory logic continues to perform under adverse network conditions; Use of this definition will not provide validation of the supervisory logic itself.

The jitter requirements of a) and b) are with respect to the relative timing of the transitions, not the analog value of the analog or digital output. A transition SHALL be determined to have occurred using one of these criteria:

- when the voltage crosses above a high threshold level of 90% of total voltage rise expected, or below a low threshold level of 90% of the total fall expected
- when the voltage crosses above a high threshold level which is a specified voltage less than the total voltage rise expected, or a specified voltage more than the total fall expected. For all steps, the specified voltage shall be 10% of the voltage of the smallest step found in the signal.

NOTE 3 The analog signal defined above has different voltage values for its rising and falling steps. Under the first criterion, the voltage allowance for a transition will therefore be different for a rising step and a falling step. Under the second criterion, the voltage allowance for a transition is the same for a rising or falling step.

The test device employed to test an IACS device shall itself introduce a maximum measurement error (measurement jitter) of no more than 2% of the period at constant state for the test signals specified in this definition.

NOTE 4 Since the period at constant state is 1 second, 2% is 20 ms.

The device under test is considered to adequately maintain control capability if both of the following hold:

- The percent of jitter measurements taken during the test that are less than the maximum jitter tolerance defined by the device supplier, is greater than or equal to the confidence percentage value defined by the device supplier, after allowing for measurement jitter.
- There is no occurrence of jitter during the test, that is greater than the sum of measurement jitter plus 1.5 times the maximum jitter tolerance.

NOTE 5 For example, assuming measurement jitter of 10ms and a maximum jitter tolerance of 50 ms, a jitter observation of greater than 85ms would indicate failure to adequately maintain control capability.

BIBLIOGRAPHY

[1] ISA-62443-3-2 *Security for industrial automation and control systems Part 3-2: Security risk assessment and system design*