SSA-300

ISA Security Compliance Institute –
System Security Assurance –

ISASecure® certification requirements

Version 2.0

February 2018

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

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.

1.2 Scope of the SSA certification program

ISASecure SSA is a certification program for a particular subset of control systems. A control system product 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 device.
- 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 devices 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 SRT specification [SSA-310] 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

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

2.1.1 Specifications for certification elements

NOTE 1 The following document provides the technical evaluation criteria for the System Robustness Testing element of an SSA evaluation.

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

NOTE 2 The following documents provide 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

[EDSA-311] *ISCI Embedded Device Security Assurance – Functional security assessment,* as specified at http://www.ISASecure.org

NOTE 3 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 security development lifecycle processes.

[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 4 The following is the highest level document that describes the related ISASecure SDLA certification program for supplier security 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

2.2 Vulnerability identification testing specifications

NOTE The following document specifies policy parameter values used to perform Vulnerability Identification Testing (VIT) for a specific system. VIT is a sub element of System Robustness Testing.

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

2.3 Communication robustness testing specifications

NOTE 1 The first document in this list is the overarching technical specification that defines how tests are carried out for both ISASecure EDSA and SSA communication robustness testing (CRT), as well as some aspects of SSA network stress testing (NST). It applies for ISASecure SSA to the extent described in [SSA-310]. The list of protocol-specific ISASecure EDSA technical test specifications that follow it, refer to [EDSA-310] for requirements that are common across all protocols.

NOTE 2 Although [EDSA-310] also covers vulnerability identification test for embedded devices, that portion of the document is not referenced by any SSA program documents. [SSA-310] directly addresses this topic for the SSA program.

[EDSA-310] *ISCI Embedded Device Security Assurance –Requirements for embedded device robustness testing,* as specified at http://www.ISASecure.org

[EDSA-401] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols,* as specified at http://www.ISASecure.org

[EDSA-402] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4,* as specified at http://www.ISASecure.org

[EDSA-403] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-404] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol,* as specified at http://www.ISASecure.org

[EDSA-405] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

[EDSA-406] *ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6,* as specified at http://www.ISASecure.org

2.4 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 suppliers to design useful security zones and select appropriate associated capability security levels for these zones. Likewise, these standards are required for system users to understand the capability security levels appropriate for a specific system deployment.

[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*

NOTE 2 [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 3 [SSA-312] is based upon the following standard.

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

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

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accessible network interface

network interface declared by the system certification applicant as suitable for use during operation or maintenance, that supports for operation or instrumentation any protocol subject to SRT, 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, and would not be subject to SRT testing.

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

NOTE [EDSA-310] and [SSA-310] specify how suitability is determined for embedded devices and systems, respectively.

3.1.3
allocatable

able to be met by other components

NOTE As used here, refers to security capabilities capable of being met by other components in a device’s architectural context, although not directly provided by the device itself.

3.1.4
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.

3.1.5
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.

3.1.6
certification level

number associated with a particular certification granted, where requirements to achieve that certification increase in rigor for higher levels

NOTE An SSA certification for a particular security zone may be SSA Level 1, 2, 3, or 4. A zone certified to SSA Level *n* meets requirements for capability security level *n* as defined in the standard [ANSI/ISA-62443-3-3].

3.1.7
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.

3.1.8
control system

hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.9
device

combination of components having a given function forming a part of a piece of equipment, apparatus or system

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
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.

3.1.13
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

3.1.14
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 embedded devices that are components of the system are ISASecure EDSA certified.

3.1.15
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 2.6.1

3.1.16
layout

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

3.1.17
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 certification 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 devices in these zones, interfaces and protocols present in any layout in scope for a certification.

3.1.18
reference system

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

NOTE A reference system is used for direct testing performed by the SSA certifier.

3.1.19
scalable control system

control system which supports replication of zones and/or devices to support small and large installations

3.1.20
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.

3.1.21
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 [ANSI/ISA-62443-3-3]. A security zone configuration is part of the system architecture diagram submitted by applicants for ISASecure SSA certification, as required per [SSA-310].

3.1.22
supported

provided by the entity under evaluation itself

NOTE This term is used when referring to security functionality. In particular, supported functionality need not be allocatable to external entities that exist in the environment of the entity under evaluation.

3.1.23
system

control system

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

3.1.24
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.

3.1.25
zone

security zone

3.2 Abbreviations

The following abbreviations are used in this document.

ADT	asset discovery testing
ANSI	American National Standards Institute
ARP	address resolution protocol
ASCI	Automation Standards Compliance Institute
CRT	communication robustness testing
DCS	distributed control system
DSG	document security guidelines
ED	embedded device
EDSA	embedded device security assurance
FSA-E	functional security assessment for embedded devices
FSA-S	functional security assessment for systems
HMI	human machine interface
IAC	identification and authentication control
IACS	industrial automation and control system
ICMPv4	internet control message protocol version 4
IETF	Internet engineering task force
ISA	International Society of Automation
IO	input/output
IP	Internet protocol
ISCI	ISA Security Compliance Institute
LAN	local area network
NA	not applicable
NST	network stress testing
OS	operating system
PLC	programmable logic controller
SAD	security architecture design
SCADA	supervisory control and data acquisition
SDA-S	security development artifacts for systems
SDLA	security development lifecycle assurance
SDLPA	security development lifecycle process assessment
SecRS	security requirements specification
SIF	safety instrumented function
SIS	safety instrumented system
SL-C	capability security level
SPV	security process verification
SRA	security risk assessment and threat modeling
SRS	security requirements specification
SRT	system robustness testing
SSA	system security assurance
SUT	system under test

SY	system
TCP	transmission control protocol
TD	test device
UC	use control
UDP	user datagram protocol
VIT	vulnerability identification testing

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 [ANSI/ISA-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.

In order to obtain ISASecure SSA certification, a supplier must pass a Security Development Lifecycle Process Assessment (SDLPA) equivalent to that defined under the ISASecure SDLA process certification, described in the reference [SDLA-100]. Specifically, in order for a system product from a supplier to achieve ISASecure SSA certification, then either:

- the supplier must hold an ISASecure SDLA certification; or

- the supplier passes an equivalent SDLPA evaluation of their development process as part of the SSA evaluation itself.

If the supplier elects the first option, they may apply for ISASecure SSA and SDLA certifications in parallel.

ISASecure SSA certification for systems has four additional elements:

- Security Development Artifacts for systems (SDA-S);

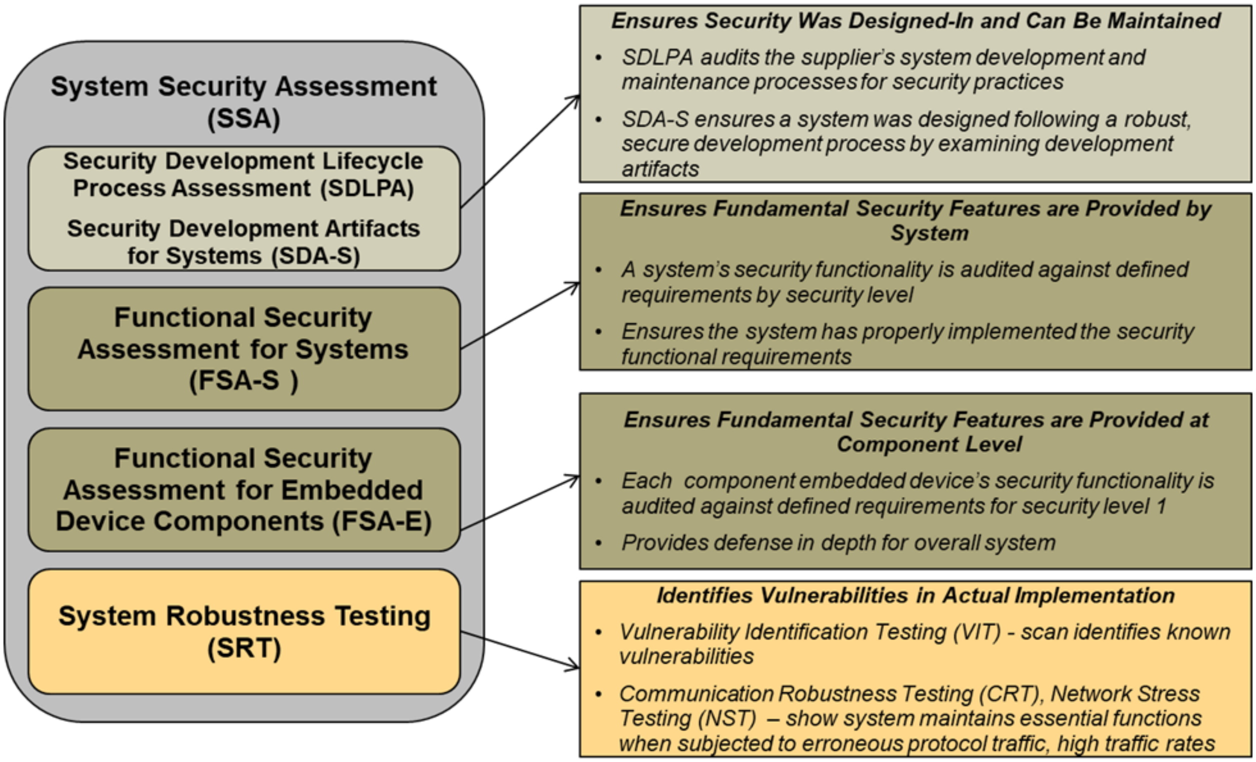
- Functional Security Assessment for systems (FSA-S);

- Functional Security Assessment for embedded devices (FSA-E); and

- System Robustness Testing (SRT).

SDA-S examines the artifacts that are the outputs of the supplier's security development processes as they apply to the system to be certified. FSA-S examines the security capabilities of the system. FSA-E examines the security capabilities of any embedded devices that are components of the system, recognizing that in some cases security functionality is provided by other system components. SRT has three major elements - Vulnerability Identification Testing (VIT), Communication Robustness Testing (CRT) and Network Stress Testing (NST). VIT scans all components of a system for the presence of known vulnerabilities. CRT and NST verify that the system adequately maintains essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions) at its network interfaces.

The following figure illustrates the elements of ISASecure SSA certification.


System Security Assessment (SSA)
Security Development Lifecycle Process Assessment (SDLPA)
Security Development Artifacts for Systems (SDA-S)
Functional Security Assessment for Systems (FSA-S)
Functional Security Assessment for Embedded Device Components (FSA-E)
System Robustness Testing (SRT)

Ensures Security Was Designed-In and Can Be Maintained

- *SDLPA audits the supplier's system development and maintenance processes for security practices*
- *SDA-S ensures a system was designed following a robust, secure development process by examining development artifacts*

Ensures Fundamental Security Features are Provided by System

- *A system's security functionality is audited against defined requirements by security level*
- *Ensures the system has properly implemented the security functional requirements*

Ensures Fundamental Security Features are Provided at Component Level

- *Each component embedded device's security functionality is audited against defined requirements for security level 1*
- *Provides defense in depth for overall system*

Identifies Vulnerabilities in Actual Implementation

- *Vulnerability Identification Testing (VIT) - scan identifies known vulnerabilities*
- *Communication Robustness Testing (CRT), Network Stress Testing (NST) – show system maintains essential functions when subjected to erroneous protocol traffic, high traffic rates*

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 certification level for each zone, which will be the desired capability security level for that zone to be demonstrated by the certification. The SDLPA and SDA-S assessments 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 certification level. Since pass/fail criteria for VIT reference applicable FSA-S requirements, VIT is also more rigorous at higher certification levels. The ISASecure SSA certificate for a system will name the security zones and their certified capability security levels.

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 SRT 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.

If the system has a component embedded device that is ISASecure EDSA certified, that certification may be leveraged to meet CRT and FSA requirements for SSA certification of the overall system, to the extent specified in the present document.

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 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 ISA 62443 for IACS security. [SSA-100] discusses the relationship between ISASecure SSA and the ISA 62443 effort.

ASCI (Automation Standards Compliance Institute) will accredit private organizations to perform ISASecure SSA certification evaluations as “certifiers”. ASCI will also recognize test tools suitable for performing CRT. These tools will be used by certifiers for the CRT and NST elements of SRT, and by system suppliers and system component vendors in preparation for certification.

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:

- embedded devices, the ISASecure EDSA program (Embedded Device Security Assurance), defined in certification scheme document [EDSA-100]
- 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 SRT specification [SSA-310] requires that a security zone breakdown for the system be submitted with an application for system certification. A control system may scale by replicating devices, 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 devices 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 certification 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 devices 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 1 operator workstation and the other 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 device 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 Devices	Min and Max Quantity of Devices 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	Best 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 devices within zones may appear in varying quantities. For some systems, neither zones nor devices 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 devices 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 device 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 devices 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 devices 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 second 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.R7, 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 devices 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 devices 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 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.

5.3 Zone certification levels and certification version

Requirement ISASecure_SY.R4 – Application for security zone certification levels

When a system 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 certification levels possible are 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 2.6.1.

5.4 Initial certification

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) for any ISASecure EDSA certified embedded devices that are components of the system, the FSA section of the EDSA certification report; and

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

The following requirement defines the technical criteria for a system to achieve ISASecure SSA certification. It references several SSA program specifications. In particular, [SSA-310] defines requirements on a certifier for carrying out SRT, and criteria for passing this element of the certification. [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.R7 – 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 - 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. -OR- An SDLPA process evaluation is done as part of the SSA evaluation and passes. In particular, all SDLPA criteria that apply to systems, are assessed as pass. The validation criteria are enumerated in the column labeled "Development Organization and SDL Validation Activity" in [SDLA-312]. Validations that depend upon capability security level, SHALL be assessed for all capability security levels *n,* where some system zone is to be certified to level *n*.	[SDLA-300] [SDLA-312]
Secure Development Processes Applied to System	SDA-S	The system passes SDA-S, a review of security development artifacts, for certification level *n,* for each zone to be certified to 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 equal to the certification level 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] [EDSA-310]

Topic	Element	Requirement	Reference Document
Security Functions of Embedded Device Components of System	FSA-E	For any embedded device component of the system, all EDSA FSA criteria applicable to EDSA certification level 1 are assessed as either supported or allocatable as part of the SSA evaluation, OR the embedded device has an ISASecure EDSA certification (which implies this same assessment result was obtained under the EDSA evaluation). Each embedded device requirement assessed as allocatable, is allocated to other system components in such a way that that the embedded device meets the requirement when deployed in the context of the system under evaluation.	[EDSA-311]
System Robustness in Networked Environment	SRT	The system passes SRT. If more than one layout is in scope for the certification, SRT SHALL be performed on a system with a reference layout as defined in requirement ISASecure_SY.R3.	[SSA-310]

NOTE 1 SRT includes the requirement that any embedded device component of the system pass CRT. This same criterion is also a requirement for ISASecure EDSA certification (at all levels) for an embedded device. Therefore, a portion of this SSA requirement is met if a component embedded device of the system already holds an ISASecure EDSA certification.

NOTE 2 SRT includes the requirement that any embedded device component of the system pass VIT. This same criterion is also a requirement for ISASecure EDSA certification (at all levels) for an embedded device. Therefore, a portion of this SSA requirement is met if a component embedded device of the system already holds an ISASecure EDSA certification and if the VIT scan done for that EDSA certification is sufficiently current, as required by [SSA-420].

NOTE 3 Regarding the second alternative for SDLPA, it is acceptable to apply for both SDLA and SSA certifications at the same time. In effect, in this case, the supplier achieves, along with their system product certification, a process certification that applies toward certifications for other products going forward.

Requirement ISASecure_SY.R8 – Consideration for prior SDLPA

A certifier SHALL consider evidence from prior ISASecure audits of a supplier's security development process, toward the SDLPA element of an SSA certification.

NOTE For example, evidence from the SDLPA evaluation performed as part of an SSA evaluation of a control system, is considered when a modified version of that system, or a completely different system model, is presented for certification.

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.R7. 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 devices 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.

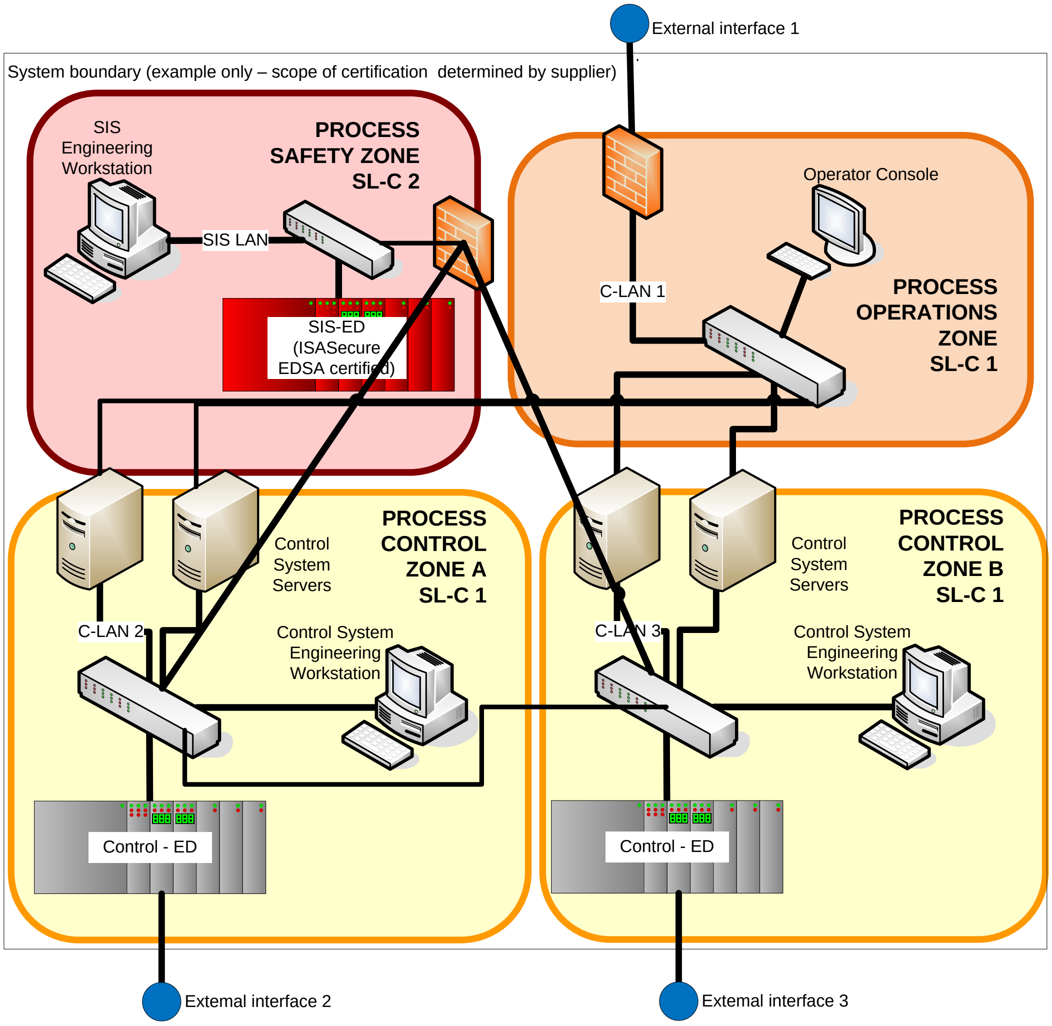

External interface 1
System boundary (example only – scope of certification determined by supplier)
SIS Engineering Workstation
PROCESS SAFETY ZONE SL-C 2
SIS LAN
SIS-ED (ISASecure EDSA certified)
Operator Console
C-LAN 1
PROCESS OPERATIONS ZONE SL-C 1
Control System Servers
PROCESS CONTROL ZONE A SL-C 1
C-LAN 2
Control System Engineering Workstation
Control - ED
Control System Servers
PROCESS CONTROL ZONE B SL-C 1
C-LAN 3
Control System Engineering Workstation
Control - ED
External interface 2
External interface 3

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 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 [ANSI/ISA-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 device 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. For the example, the safety PLC has been certified under the ISASecure EDSA (Embedded Device Security Assurance) program, before the supplier applies for SSA certification for this system. The control PLC has not been ISASecure EDSA-certified.

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 Devices	Min and Max Quantity of Devices 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 devices, 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	Protocol XYZ for communication	None	2	0-2

Zone	Resident Devices	Min and Max Quantity of Devices 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
	SIS-ED	1	Workstation and SIS-ED	to Process Control 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 devices 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.R7 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. If the supplier does not have an SDLA certification, or has an SDLA certification that does not meet these criteria, they may either:

- undergo an SDLPA evaluation to the criteria defined in Table 2, where validations that depend upon capability security level are assessed at levels 1 and 2, as part of this SSA evaluation;
- update the scope of an existing SDLA-certified process so that it applies to the system product; or
- apply for a new ISASecure SDLA certification that applies to the system product.

The last two options may 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.

Under all of these options, 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.) Also, whether an existing, updated, or new SDL process passes evaluation as applicable to this system product, this implies that it has passed requirement validations that depend upon capability security levels, for both levels 1 and 2, since the system has zones to be certified to these two levels.

The validation of these requirements by the certifier for SDLPA is performed per the column labeled "**Development Organization and SDL Validation Activity**" in [SDLA-312].

Table 4 presents examples of SDLA requirements that would be assessed for the supplier's SDLPA evaluation under any of the above options.

In SDLA-312 v4.52, validation of the one requirement SDLA-DM-4 for SDLPA depends upon the capability security level for products that fall under the scope of the SDL being examined. The SDLPA validation for SDLA-DM-4 is shown in the last row, last column of Table 4. Note that for this example SDLPA evaluation, for validation of SDLA-DM-4, it will be required that processes and related criteria applying to capability security levels 1 and 2 be in place, since those levels apply to the example system.

Table 4 - Example SDLPA Requirements

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-SM-4	Security Expertise	A process shall be employed for defining security training and assessment programs to ensure that personnel assigned to the organizational roles and duties specified in SDLA-SM-2 – Identification of responsibilities, have demonstrated security expertise appropriate for those processes.	Verify that company has a procedure to assess that personnel assigned to processes defined in SDLA-SM-2 have demonstrated security expertise appropriate for those processes. Verify that the development process states that for each defined role a list of required security training must be created and tracking who attends that training must be done. Verify that the required security training has been identified and that at least some developers have been trained.
SDLA-SR-1	Product security context	A process shall be employed to ensure that the intended product security context is documented.	Verify SecRS includes a description of the operating environment for any product developed according to the process currently being evaluated. Or verify that the development process or SecRS template states that the SecRS must include a statement of expected security environment. May verify SecRS for any component or system developed according to the process being evaluated identifies and explains assumptions about the intended usage of the product and the environment. Or may verify that the development process or SecRS template states that assumptions about intended usage of the product and the environment are included in the SecRS.
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 –	Verify that the process includes this step. Verify that it applies to security issues found internally and externally throughout any phase of the development

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
		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.	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.

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 SSA 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.

Similar to the SDLPA assessment, in SDLA-312 v4.52, 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 [ANSI/ISA-62443-4-1] is shown above in Table 4. 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 certification level for the zone. First, for each security zone, the certifier identifies FSA-S requirements that must be met. For a zone of a particular certification level, these will be the requirements shown in [SSA-311] as applicable to the capability security level equal to that certification level. 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			
7 …Table continues for additional IAC requirements and other categories UC, DI, 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 device 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.R7 – *Criteria for granting an initial certification* in 5.4 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 equal to the certification level 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 test use the reference system for testing.

7.1.1 FSA-E (Functional Security Assessment – Embedded Device)

In addition to FSA-S which assesses functional security capabilities for each security zone, under FSA-E the certifier will perform a component-level assessment of the functional security capabilities of all embedded devices that are components of the system. “Embedded device” is defined in 3.1 of this document.

In the example system, there are two types of embedded devices. These are the SIS-ED (Safety Instrumented System Embedded Device) which resides in a Process Safety Zone and the Control-ED (Control Embedded Device) which resides in a Process Control Zone. For FSA-E under an SSA evaluation, the assessment is the same regardless of the security zone in which the embedded device resides. In particular, Requirement ISASecure_SY.R7– *Criteria for granting an initial certification* in 5.4 of this document states that for any embedded device component of the system, all EDSA FSA criteria listed in the document [EDSA-311] as applicable to EDSA certification level 1 must be assessed as either supported or allocatable. This is one of the criteria required for an embedded device to achieve ISASecure EDSA certification. EDSA certification of a component embedded device is therefore sufficient to meet this criterion. However, it is not necessary that a component embedded device be EDSA certified in order for a system containing it to achieve ISASecure SSA certification.

In the case of the example system, since the SIS-ED is already ISASecure EDSA certified, it has been determined as part of that certification that all EDSA FSA requirements at certification level 1 are either supported or allocatable, so that analysis does not need to be done as part of the SSA evaluation. However, it should be noted that this is the case only if the EDSA certification has been granted to same version of the SIS-ED that is used as a component of the system. If an earlier version of the embedded device was certified, the certifier will perform an FSA assessment of the modified embedded device as required for maintenance of ISASecure EDSA certification, as defined in [EDSA-301]. If there are very minor changes to the SIS-ED since it was certified, this will be a brief assessment. It is not required that the existing EDSA certification be updated, although the supplier of the embedded device may elect to do this. If it is updated, then the certifier does not need to reassess the EDSA FSA requirements under the SSA evaluation for the example system.

Even though SIS-ED is to be certified within a capability security level 2 zone, the evaluation of EDSA FSA requirements for SIS-ED at EDSA certification level 2 is not required by Requirement ISASecure_SY.R7.

Since Control-ED is not ISASecure EDSA certified, the certifier would assess for this device, each of the criteria in [EDSA-311] applicable to EDSA certification level 1, to determine whether it is supported or allocatable.

For both SIS-ED and Control-ED, the certifier then performs an additional evaluation of any EDSA FSA requirements assessed as allocatable. This evaluation verifies that the requirement is in fact allocated to other components of the system and therefore supported by the embedded device *when in the system context, for any layout in scope for this certification*. For example, suppose that the following FSA requirement from [EDSA-311] was assessed as allocatable for Control-ED:

FSA-AC-2.1.1 *Management of Password:* The IACS embedded device shall provide the capability for [IACS Administrator] or the user to modify password within their control without impacting normal operation.

The certifier in this case would verify that management of passwords per this requirement is provided for Control-ED by other components within the scope of the system that has been presented for SSA certification. For example, if the Control System Server was required to support this functionality, then a layout without such a server could not be in scope for certification unless another method to support the functionality covers that case. If not, then Table 3 which describes the layouts in scope, would need to be modified, to require 1-2 control system servers instead of 0-2.

7.1.2 SRT (System Robustness Testing)

7.1.2.1 Overview

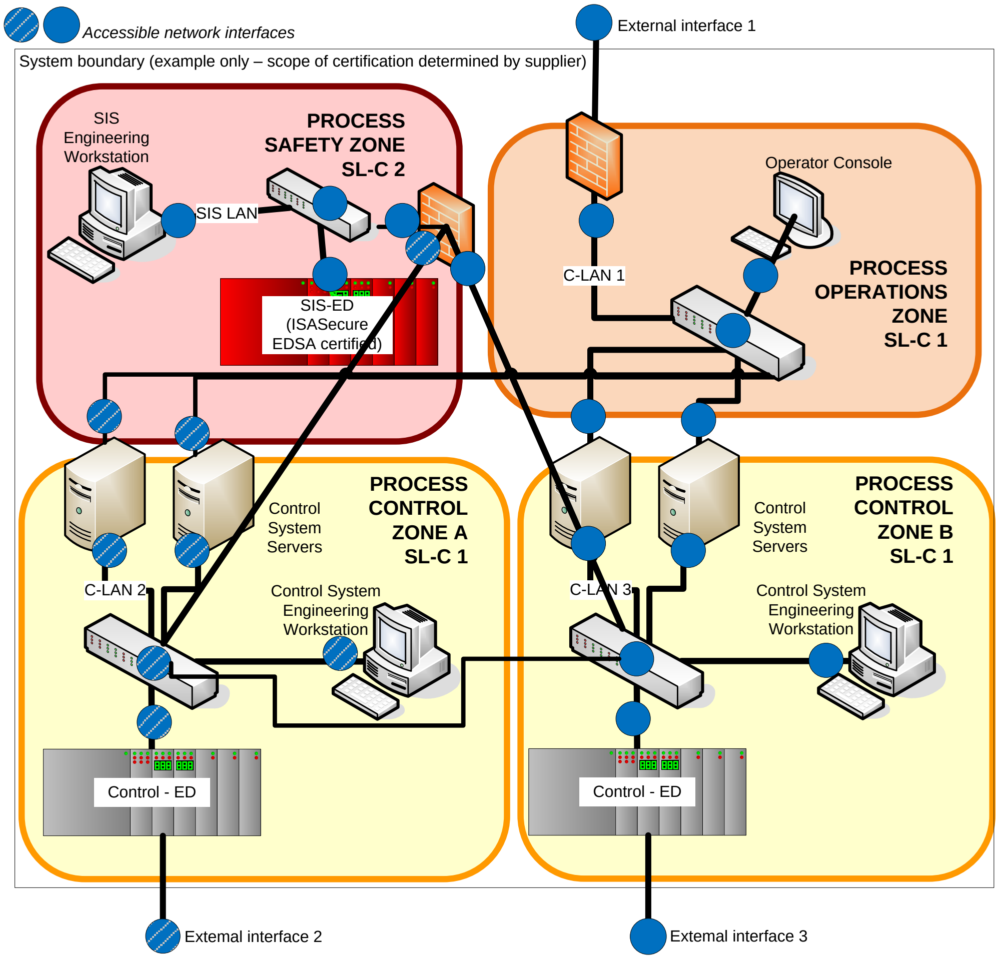
The supplier applying for certification of this system would make available to the certifier, a reference system with the reference layout shown in Figure 2, for running SRT. This includes the firewalls and routers shown, as well as the internal firewalls on the various workstations and servers, regardless of whether the supplier provides these to the customer. In either case, the firewalls and routers used for SRT should meet the functional and configuration requirements stated by the supplier in their user documentation. The fully configured equipment may be made available at the certifier’s site, the supplier’s site or another location.

SRT consists of Asset Discovery Testing, Vulnerability Identification Testing, Communication Robustness Testing and Network Stress Testing. Asset Discovery Testing contributes to scope definition for the other tests. As described in [SSA-310], all four tests must pass in order to pass SRT. The following sub clauses describe each of these tests in turn for the example reference system.

7.1.2.2 ADT (Asset Discovery Testing)

Asset discovery testing (ADT) is a scan to determine ports and services active for system components. It also verifies that essential functions are adequately maintained under high scan rates, as defined in [SSA-310]. For the example system, asset discovery testing will be performed as part of the SSA evaluation for this system against all the accessible network interfaces indicated in Figure 3 with blue or blue striped markers, except for the interface to the SIS-ED safety PLC, since this device is ISASecure EDSA certified and therefore has already passed this test. For the purposes of determining active protocols, the internal firewall functionality in the three workstations and the control PLC will be turned off. For the purposes of testing maintenance of essential functions under high scan rates, the internal firewalls would be configured as specified for operational use in the system user documentation.

The "duplicate" accessible interfaces indicated by striped blue markers in Process Control Zone A will yield identical protocols, ports and behavior as for Process Control Zone B, since their architectures are identical. Therefore the certifier may elect that these interfaces do not need to be separately tested under ADT. Nevertheless, it is required that Process Control Zone A be present and operating during ADT testing of the maintenance of essential functions from accessible interfaces of Process Control Zone B. This aspect of the test will show that a scan of one of the Control-ED devices does not interfere with the essential functions of the other Control-ED device in the reference architecture via the peer-to-peer interface.



Accessible network interfaces
External interface 1
System boundary (example only – scope of certification determined by supplier)
SIS Engineering Workstation
PROCESS SAFETY ZONE SL-C 2
SIS LAN
SIS-ED (ISASecure EDSA certified)
Operator Console
C-LAN 1
PROCESS OPERATIONS ZONE SL-C 1
Control System Servers
PROCESS CONTROL ZONE A SL-C 1
C-LAN 2
Control System Engineering Workstation
Control - ED
Control System Servers
PROCESS CONTROL ZONE B SL-C 1
C-LAN 3
Control System Engineering Workstation
Control - ED
Extemal interface 2
Extemal interface 3

Figure 3 - Accessible Network Interfaces for the Example Reference System

7.1.2.3 VIT (Vulnerability Identification Testing)

For the example system, in accordance with [SSA-310] 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-310]. System essential functions are also monitored during the scan.

Since SIS-ED is ISASecure EDSA certified, it will have passed VIT as part of that certification. However, SSA certification per [SSA-420] defines a criterion such that VIT be current relative to the date on the SSA certificate. So, although VIT passed for the EDSA certification, VIT may need to be rerun on SIS-ED for the SSA certification to meet this criterion.

As for ADT, 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. Also as described for ADT, it nevertheless is required that both zones of this type be present and operational during VIT.

7.1.2.4 CRT and NST

This section describes CRT and NST for the example reference system, beginning with CRT.

After baseline operations tests verify the system under test is operating as expected, communication robustness testing includes two types of tests:

- Basic robustness tests, which subject the SUT to protocol field boundary conditions and special cases; and
- Load stress tests, in which the system under test is subjected to high traffic rates.

In accordance with [SSA-310], communication robustness testing is performed as shown in the following table and illustrated in Figure 4.

Table 7 - CRT for the Example Reference System

CRT Test Requirement from [SSA-310]	Application for Example System
CRT basic and load stress tests are run against any devices with IP addresses visible at an external interface, from that external interface, with the exception of perimeter firewall devices	• Although the firewall protecting the Process Operations Zone at External interface 1 is visible from External interface 1, it is a perimeter firewall so does not require CRT test from External interface 1. • Control servers are visible from External interface 1, so are tested from this interface. • Only the Control-ED is visible from External interfaces 2 and 3, and it also meets the criterion in the next row that indicates that both basic and

CRT Test Requirement from [SSA-310]	Application for Example System
	load stress CRT should be run. As for ADT and VIT, running CRT from either one of external interface 2 or 3 is sufficient.
CRT basic and load stress tests are run against all accessible interfaces of all embedded devices	• In the example, since SIS-ED is already ISASecure EDSA certified, this criterion is met for that device. • Since Control-ED has two accessible network interfaces, full CRT is run against Control-ED with traffic originating from External Interface 2 or 3 (already covered above), and also originating from the Process Control Zone switch, with possible exceptions as follows. For basic CRT tests that send unusual traffic that may be deleted by the switch, a connection must be used that permits this type of traffic between the TD (test device generating CRT traffic) and the Control-ED.

In accordance with [SSA-310], network stress testing is performed as shown in the following table and illustrated in Figure 4.

Table 8 - NST for Example Reference System

NST Test Requirement from [SSA-310	Application for Example System
Network traffic is generated as for all defined CRT load stress tests, and run against all devices in each network segment	Test traffic is generated on a test device connected to the switches in each of the three different types of security zone, since each security zone is a network segment in this example. It is not required to run these tests against both Process Control zones, but it is required to have both of these zones present and operating during the test. Stress tests for all protocols supported by any device on the network segment are run against all device interfaces, shown in yellow in Figure 4. Note this means that the control servers are subjected to load stress tests both from External Interface 1 (under CRT) as well as from the security zone switch (under NST). NST is not applied to the perimeter firewall on C-LAN 1. All system essential functions in all four zones are monitored except for the control function of the embedded devices.

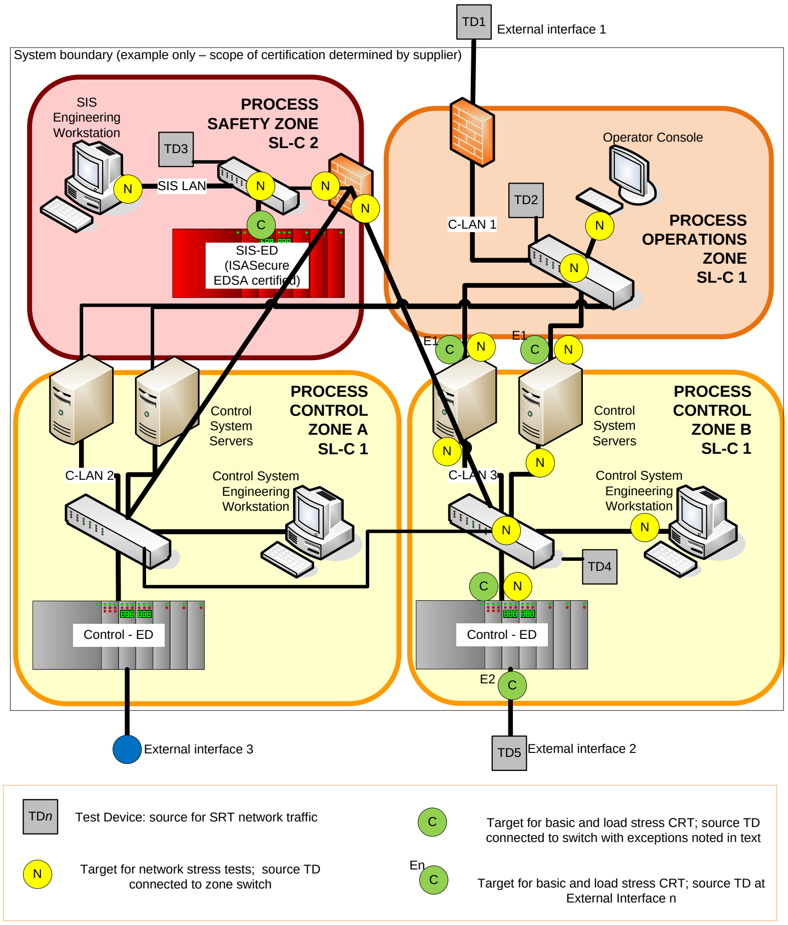

TD1
External interface 1
System boundary (example only – scope of certification determined by supplier)
SIS Engineering Workstation
PROCESS SAFETY ZONE SL-C 2
TD3
SIS LAN
N
C
SIS-ED (ISASecure EDSA certified)
Operator Console
TD2
C-LAN 1
PROCESS OPERATIONS ZONE SL-C 1
E1
E1
Control System Servers
PROCESS CONTROL ZONE A SL-C 1
C-LAN 2
Control System Engineering Workstation
Control - ED
External interface 3
Control System Servers
PROCESS CONTROL ZONE B SL-C 1
C-LAN 3
Control System Engineering Workstation
TD4
Control - ED
E2
TD5
External interface 2
TDn
Test Device: source for SRT network traffic
Target for basic and load stress CRT; source TD connected to switch with exceptions noted in text
Target for network stress tests; source TD connected to zone switch
En
Target for basic and load stress CRT; source TD at External Interface n

Figure 4 - CRT and NST for the Example System

BIBLIOGRAPHY

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