SSA-300

ISA Security Compliance Institute — System Security Assurance –

ISASecure certification requirements

Version 1.1

February 2014

Revision history

version	date	changes
1.1	2014.02.09	Initial version published to http://www.ISASecure.org

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). Certifications available include ISASecure Embedded Device Security Assurance (EDSA) for embedded devices, ISASecure System Security Assurance (SSA) for systems and ISASecure Security Development Lifecycle Assurance (SDLA) which addresses control system supplier development processes. This specification is the overarching document in the series that describes technical requirements for ISASecure SSA certification of systems. It references all other documents that contain these requirements and places them in context. The current list of documents related to 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 the types of 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 supplier has assigned a unique product identifier to the control system which the supplier uses in the marketplace to refer to the integrated set of components as a whole.
- The system product is under configuration control and version management.

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 process.

[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 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.

[EDSA-310] *ISCI Embedded Device Security Assurance – Common requirements for communication robustness testing of IP based protocol implementations,* 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.

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

NOTE 2 [SSA-311] is based upon the following standard.

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

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

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 (for SDLA certification)
number associated with an ISASecure SDLA certification, where a higher number indicates that a more rigorous set of security development lifecycle process evaluation criteria has been met by the supplier

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
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.

3.1.10
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.

3.1.11
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.

3.1.12
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

3.1.13
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.

3.1.14
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 year and release number, such as ISASecure SSA 2013.1

3.1.15
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.

3.1.16
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 [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].

3.1.17
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.

3.1.18
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.

3.1.19
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.

3.1.20
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
SIF	safety instrumented function
SIS	safety instrumented system
SL-C	security level - capability
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 [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 evaluation 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 at a certification level greater than or equal to the highest zone security capability level for which the system will be certified; or

- the supplier passes an equivalent SDLA 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.

A system submitted for certification is comprised of one or more security zones. The supplier identifies a desired capability security level for each zone. The FSA-S evaluation is applied to each security zone; required security capabilities will differ based upon the desired capability security level identified for a security zone. Similarly, requirements for development process artifacts evaluated under SDA-S are more stringent for components in higher security level zones of the system. The ISASecure SSA certificate for a system will name the security zones and capability security levels to which they have been certified.

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 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 formally defines the requirements to achieve ISASecure SSA certification for a system.

5.2 Zone capability security levels and certification version

Requirement ISASecure_SY.R1 – 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 levels possible are 1, 2, or 3, or 4. The certifier SHALL award certification designating each security zone at the highest level less than or equal to this maximum level for which the security zone qualifies, without requiring the system supplier to reapply for certification.

NOTE The SRT specification [SSA-310] requires that a security zone breakdown for the system be submitted with an application for system certification.

Requirement ISASecure_SY.R2 – 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 the version of the certification achieved, designated by the year and release, such as ISASecure SSA 2014.1.

5.3 Initial certification

Requirement ISASecure_SY.R3 – 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 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 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 by security level that must be assessed based upon security zone levels. Validation activities for compliance with these requirements include documentation review, inspection, and in some cases, independent test.

Requirement ISASecure_SY.R4 – 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 1 - Certification Criteria

Topic	Element	Requirement	Reference Document
Secure Development Processes Implemented by Supplier	SDLA	The supplier holds an ISASecure SDLA certification, with SDLA certification level at or above the highest capability security level specified for any security zone of the system. The system is within the stated scope of the certified process, for development going forward. -OR- An SDLA process evaluation is done as part of the SSA evaluation and passes. In particular, all SDLA criteria applicable for an SDLA certification level at or above the highest capability security level specified for any security zone of the system, are assessed as pass. The validation criteria are enumerated in the column labeled "Development Organization and SDL Validation Activity" in [SDLA-312].	[SDLA-300] [SDLA-312]
Secure Development Processes Applied to System	SDA-S	The system passes SDA-S, a review of security development artifacts.	[SSA-312]
Security Functions of System	FSA-S	All FSA-S criteria applicable to the specified capability security level for each security zone are assessed as either *supported* or *NA* for that zone.	[SSA-311]
Security Functions of Embedded Device Components of System	FSA-E	For any embedded device component of the system, all EDSA FSA criteria applicable to 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.	[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 Regarding the second alternative for SDLA, 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.

NOTE 3 [SSA-100] presents a figure that illustrates these certification elements.

Requirement ISASecure_SY.R5 – Consideration for prior SDLA

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

NOTE For example, evidence from the SDLA 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.R4.

6.2 Example system description

Figure 1 depicts an example system with three security zones. This system is a tightly integrated control platform that includes safety instrumented system functions, as defined in 4.1.1. The three security zones are a process operations zone, a process control zone, and a process safety zone. 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. The process control zone and process safety zone each contain a PLC (Control-ED and SIS-ED, respectively). The supplier-specified capability security level for the process safety zone is 2; the supplier has specified the other zones as security level 1.

Each of the three security zones forms a separate network segment (C-LAN 1, C-LAN 2 and SIS LAN) and thus contains a switch. The system has two external interfaces. External Interface 1 permits higher level business functions to access the process operations zone. External Interface 2 permits the process control equipment to communicate with an external device using an IP network (e.g. Modbus TCP). 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.

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.

Two control system servers are accessible from both C-LAN 1 and C-LAN 2, the process operations and process control zones. 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.

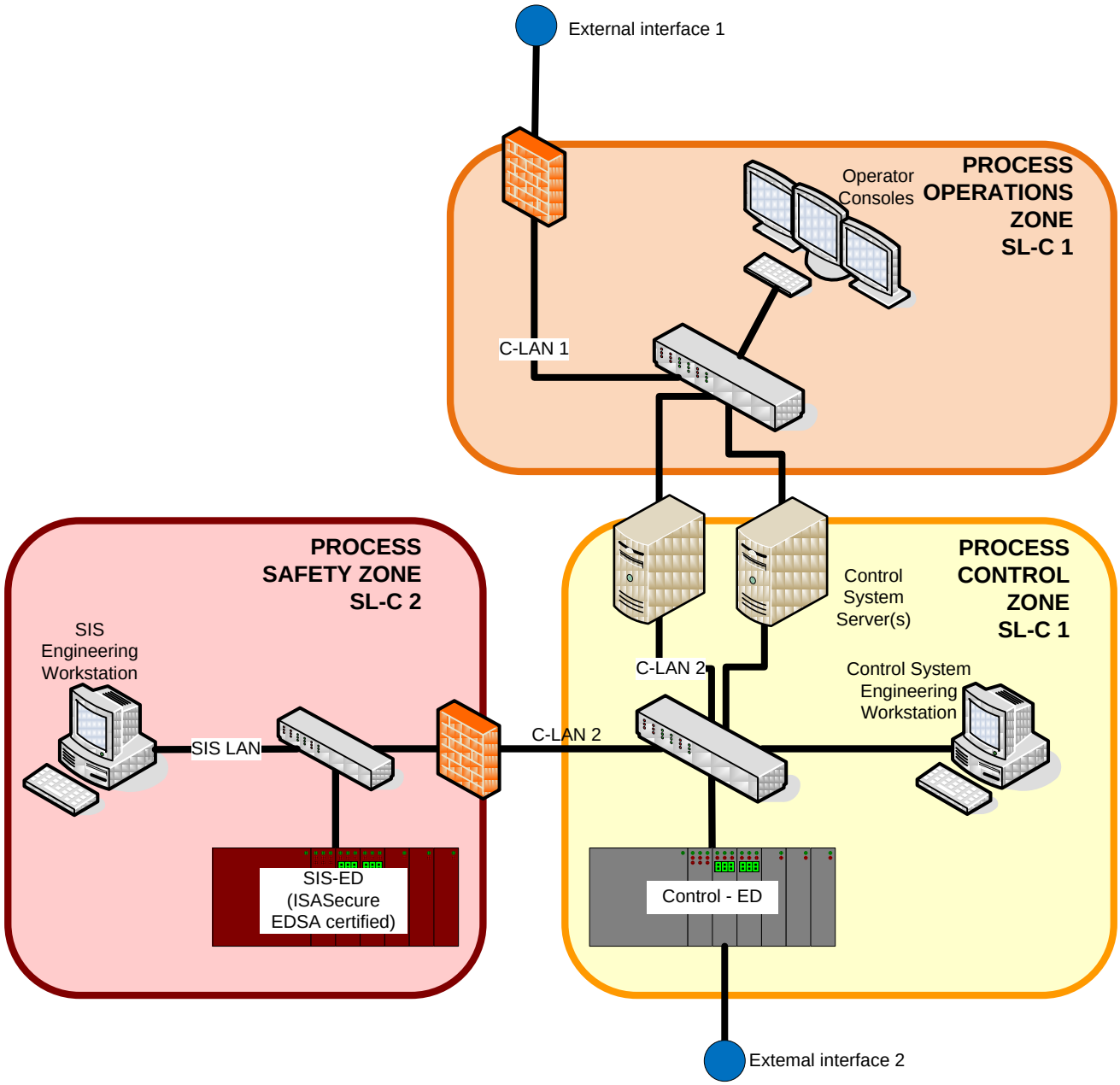

Figure 1 - Example Three Security Zone System

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.R4 in this document. The follow sub clauses discuss each of these elements for the example system.

6.3.1 SDLA (Security Development Lifecycle Assurance)

If the supplier has an ISASecure SDLA development process that has been certified at level 2 and which applies to this system going forward, the SDLA criterion is satisfied. This is because 2 is the highest capability security level designated by the supplier for a security zone of the example system. 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 SDLA evaluation at level 2, to the criteria defined in Table 1, as part of this SSA evaluation;
- update the scope and/or certification level of an existing SDLA-certified process so that it achieves level 2 and applies to the system product; or
- apply for a new ISASecure SDLA certification at level 2.

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 would be subject to the requirements enumerated in [SDLA-312] in cells that meet the criteria:

- Requirement is in a row labeled "**System**"
- Requirement is applicable to level 2, as seen in the column labeled **"ISASecure Level."**

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

Following are examples of SDLA requirements from [SDLA-312] that meet these criteria, and that would be assessed for the supplier's SDLA evaluation under any of the above options.

Table 2 - Example SDLA Requirements for Level 2

Requirement ID	Requirement Name	Requirement Description	Levels
SDLA-SMP-1.4	Basic Security Training	All personnel involved in software development of an embedded device or system, that has security concerns shall be given basic training in good security engineering practice and the secure development process that will be used on the project. In addition, software developers shall receive detailed training on common basic causes and mitigation techniques. System integration personnel shall receive training in network security administration/configuration techniques involved in a system. Testers shall receive training in security test techniques. The security management plan should document the security training plan for all those working on the software development. Evidence shall exist to show that those who have been trained have obtained the required knowledge from the training.	1, 2, 3, 4
SDLA-SMP-5.5	Authorized Changes	The CM process shall provide a means by which only authorized changes are made to the embedded device or system, implementation representation, and to all other configuration items.	2, 3, 4
SDLA-SRA-3	Threat Modeling	A threat model shall be created and documented for the ... system.	1, 2, 3, 4

Requirement ID	Requirement Name	Requirement Description	Levels
SDLA-DSD-4	Data security policy	The detailed software design should document the security policy for all data (i.e. which user roles or service roles can access the data)	2, 3, 4

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 (1) apply to systems (vs. components only) and (2) that apply for a particular capability security level and to security zones designated at this level. As stated more precisely in Requirement ISASecure_SDA.R1 in [SSA-312], these artifacts and the requirements placed upon them are enumerated in [SDLA-312] in cells that meet the criteria:

- Requirement is in a row labeled "**System**"
- Requirement is applicable to a capability security level for some security zone in the system, as seen in the column labeled **"ISASecure Level."** For the example system, this would be security levels 1 and 2.

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

Following are a few examples of artifacts from [SDLA-312] requirements that are required for all security levels. These examples are high level summaries of detailed requirements found in [SDLA-312]. Requirement IDs are in parentheses.

- Security requirements specification for the system (SDLA-SRS-1)
- Description of the system attack surface (SDLA-SAD-19)
- Threat Model (SDLA-SRA-3)
- Security guidelines for users and administrators (SDLA-DSG-1)
- Product security assessment results (SDLA-SPV-1.2)
- List of unfixed security bugs at release (SDLA-SPV-1.9)

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 evaluation of requirements for security levels greater than one is limited to artifacts for elements of the system that support security zones of that security capability level. The following table shows examples of requirements for artifacts required under level 2 process requirements in [SDLA-312]. These requirements will be evaluated only for the capability security level 2 process safety zone, per the scope indicated. Examples are shown of requirements from several different lifecycle phases.

Table 3 - Evaluation of Example SDA-S Requirements for Levels >1 for the Example System

SDA-S Requirement Identifier (from [SSA-312])	Requirement Name	Requirement Security Level	Requirement Statement	Validation Activity for Example System As Limited to Process Safety Zone
SDLA-SMP-1.6.1	Development Tools Options	2, 3, 4	The development organization shall document the selected implementation-dependent options of the development tools in the security management plan.	Verify for each development tool listed *that is used to develop system support of the process safety zone*, or a sampling of such tools listed, whether there are any implementation dependent options, and if so whether they have been documented.
SDLA-DSD-4	Data security policy	2, 3, 4	The detailed software design should document the security policy for all data (i.e. which user roles or service roles can access the data)	For software that executes in the process safety zone, may inspect the detailed software design specification and verify that it documents the security policy for specific data.
SDLA-MIV-1	Security Coding Standard	2, 3, 4	Software shall be developed compliant with a security coding standard	*For code that executes in the process safety zone*, confirm that coding standard is being followed by reviewing artifacts such as code review minutes or static analysis results or by looking at code.

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 specified capability security 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 capability security level, these will be the requirements shown in [SSA-311] as applicable to that level. For the example system, requirements that must be met for each security zone are checked in Table 4 below.

Table 4 - FSA-S Requirements Applicable to Security Zones of Example System

FSA-S Requirement Identifier (from [SSA-311])	Requirement Name	Requirement Security Level	Process Operations Zone (SL 1)	Process Control Zone (SL 1)	Process Safety Zone (SL 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, 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. 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 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”

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 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 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 levels 2, 3 and 4. Therefore it would not be required for the Process Operations Zone or the Process Control Zone, and would be assessed only for the Process Safety Zone.

In accordance with Requirement ISASecure_SY.R4 – *Criteria for granting an initial certification* in 5.3 of this document, the system will pass the FSA-S element of the evaluation if all FSA-S criteria applicable to the specified security capability level of each security zone of the system are assessed as either *supported* or *NA* for that zone.

6.3.4 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 embedded devices. These are the SIS-ED (Safety Instrumented System Embedded Device) in the Process Safety Zone and the Control-ED (Control Embedded Device) in the 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.R4 – *Criteria for granting an initial certification* in 5.3 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 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, since the SIS-ED is already ISASecure EDSA certified, it has been determined as part of that certification that all EDSA FSA requirements at 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 in a security level 2 zone, the evaluation of EDSA FSA requirements for SIS-ED at level 2 is not required. An ISASecure EDSA level 1 certification meets the SSA requirement for evaluation of EDSA FSA requirements at level 1.

Since Control-ED is not ISASecure EDSA certified, the certifier would assess for this device, each of the criteria in [EDSA-311] applicable to 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 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.

6.3.5 SRT (System Robustness Testing)

6.3.5.1 Overview

The supplier applying for certification of this system would make the full configuration shown in Figure 1 available to the certifier for 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 system.

6.3.5.2 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 as shown in Figure 2 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.

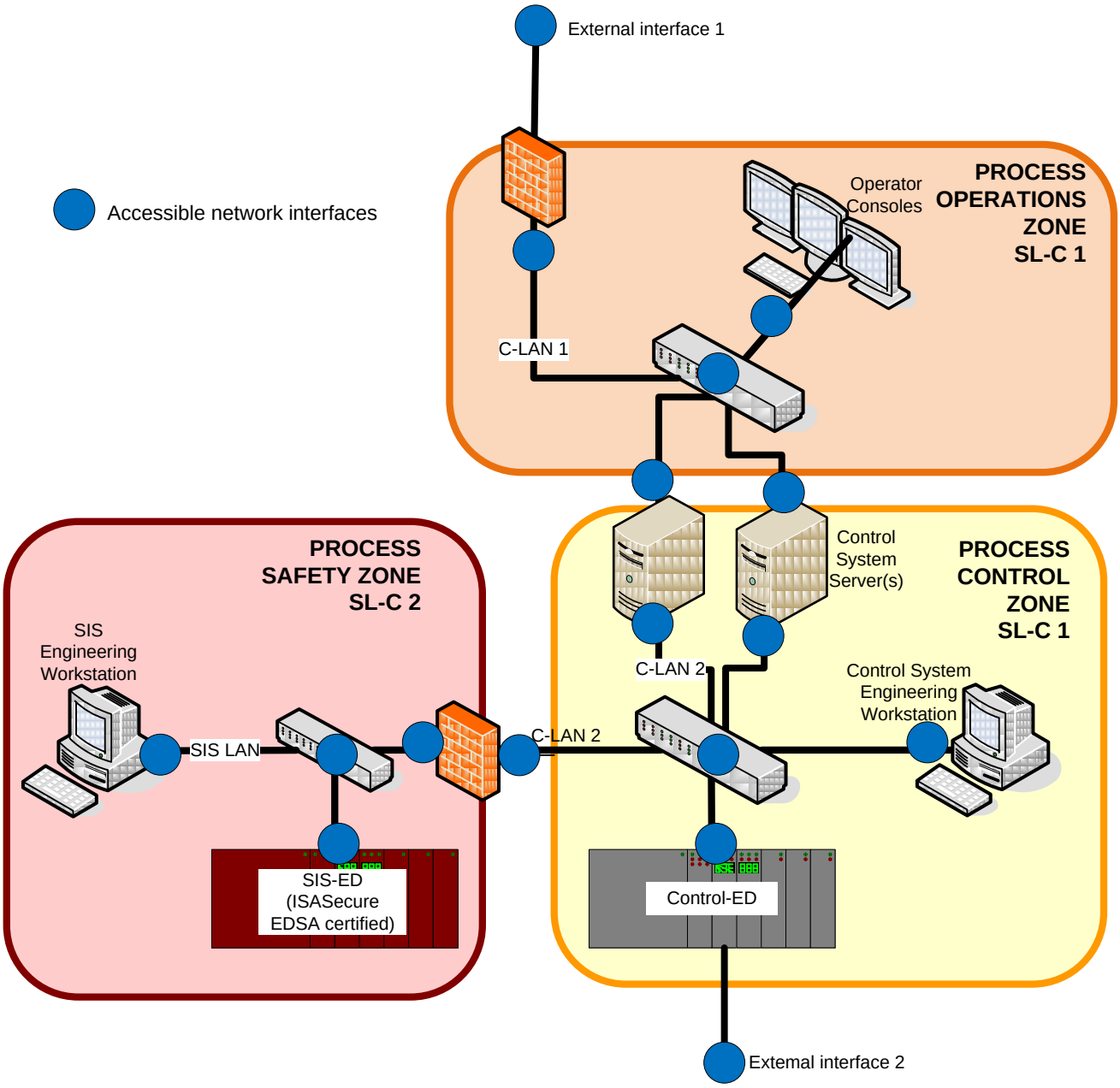

Figure 2 - Accessible Network Interfaces for the Example System

6.3.5.3 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 2, including the SIS-ED. 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].

6.3.5.4 CRT and NST

This section describes CRT and NST for the example 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 3.

Table 5 - CRT for the Example 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	• The firewall protecting the Process Operations Zone at External interface 1 is visible from External interface 1, so is tested from this interface. • Control servers are visible from External interface 1, so are tested from this interface. • Only the Control-ED is visible from External interface 2, and it also meets the criterion in the next row that indicates that both basic and load stress CRT should be run.
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 (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 3.

Table 6 - NST for Example 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 using broadcast and multicast addressing	• Test traffic is generated on a test device connected to each of the three security zone switches, since each security zone is a network segment in this example. Stress tests for all protocols supported by any device on the network segment are run against all device interfaces, shown in yellow in Figure 2. 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).

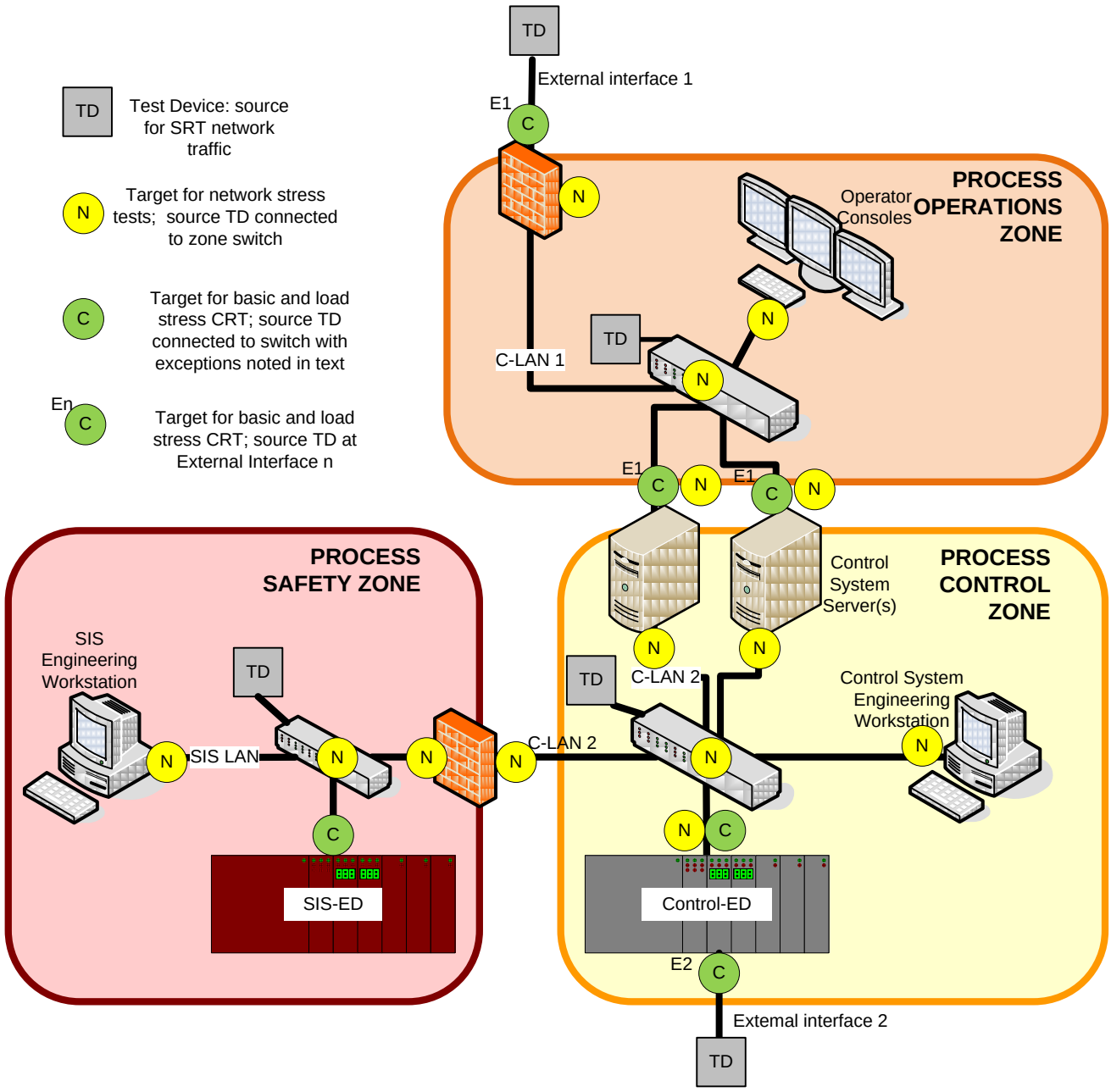

Figure 3 - CRT and NST for the Example System

BIBLIOGRAPHY

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

NOTE It is the intent going forward to align ISASecure SDLA evaluation criteria with the approved version of the following standard.

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