SSA-102
ISA Security Compliance Institute – System Security Assurance –
Errata for SSA 2.0.0 Specifications

Version 2.2

March 2018

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”)provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SPECIFICATION.

WITHOUT LIMITING THE FOREGOING, ASCI DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THIS SPECIFICATION ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE SPECIFICATION AVAILABLE, ASCI IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS ASCI UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE. ANYONE USING THIS SPECIFICATION SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ASCI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL,PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SPECIFICATION, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SPECIFICATION OR OTHERWISE ARISING OUT OF THE USE OF THE SPECIFICATION, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SPECIFICATION, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF ASCI OR ANY SUPPLIER, AND EVEN IF ASCI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision history

version	date	changes
1.2	2015.04.23	Initial version published to http://www.ISASecure.org
1.4	2015.06.22	Require full CRT tool version number and hash mechanism to verify version; update version of 17025; clarify definition of operational mode
1.5	2016.02.16	Measurement jitter 1% to 2%, broaden spec for detection of transitions
1.6	2016.03.09	Add reference to 62443-3-3 to SSA-204, 205 certificate format
2.0	2018.02.06	In SSA-200: add CACE and CACS as certifications for auditors, permit any bachelor-level degree with sufficient industry experience; in SSA-311: correct applicable levels for session ID requirements under FSA-S-SI-8; scalability updates for SSA-100, 200, 204, 205, 300, 310
2.1	2018.02.27	Modify requirements for SRT of redundant devices in SSA-310
2.2	2018.03.16	In SSA-310: modify 4.1.1.6 regarding definition of adequately maintain essential history data; modify SRT.R8 regarding submission of definition of essential history data

Contents

1 Scope 6

2 Normative references 6

3 Definitions and abbreviations 7

4 Index to errata 7

5 Errata by document 8

5.1 General 8

5.2 SSA-100 Certification scheme 8

5.3 SSA-200 Chartered laboratory 8

5.4 SSA-204 Symbols and certificates 10

5.5 SSA-205 Certificate document format 11

5.6 SSA-300 Certification requirements 12

5.7 SSA-310 Requirements for system robustness testing 15

5.8 SSA-311 Functional Security Assessment for systems 18

FOREWORD

This is one of a series of documents that defines ISASecure® certification for control systems. The ISASecure System Security Assurance (SSA) certification program is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of ISASecure certification programs and documents related to these programs can be found on the web site http://www.ISASecure.org.

1 Scope

This errata document lists approved changes to all ISASecure SSA specifications published at http://www.ISASecure.org. These changes are thus to be considered part of those specifications. This document is updated periodically as additional minor changes are identified. Major changes to any of the SSA specifications will result in a new issue of the relevant specification. This document maintains a list of changes which of themselves do not merit a new version of the specification which is changed. These changes may address typographical errors, cut and paste errors, or technical inaccuracies which are clearly non-controversial in the context of the overall intent of the specification.

When any specification is reissued with a new version number, errata tracked in this document are incorporated, and this document is revised and reissued to remove those errata. Clause 4 specifies the version numbers of the documents to which the errata in this document apply.

2 Normative references

A bibliography of all published SSA specifications is provided in the following highest level document.

[SSA-100] *ISA Security Compliance Institute – System security assurance – ISASecure Certification scheme,* as specified at http://www.ISASecure.org

Errata in the following SSA specifications are listed in the subsequent clauses of this document:

[SSA-100] *ISA Security Compliance Institute – System security assurance – ISASecure Certification scheme,* as specified at http://www.ISASecure.org

[SSA-200] *ISCI System Security Assurance – ISASecure SSA Chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[SSA-204] *ISCI System Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*, as specified at http://www.ISASecure.org

[SSA-205] *ISCI System Security Assurance – Certificate Document Format,* as specified at http://www.ISASecure.org

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

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

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

The SSA certification program refers to documents for the ISASecure Embedded Device Security Assurance (EDSA) program as cited in [SSA-100]. Errata on these EDSA documents are published in [EDSA-102]. Errata on EDSA documents published in [SDLA-102] therefore apply to SSA.

[EDSA-102] *ISCI Embedded Device Security Assurance – Errata for EDSA specifications*, as specified at http://www.ISASecure.org

The SSA certification program also references [SDLA-312] as cited below. Errata on [SDLA-312] are published in [SDLA-102]. Errata on [SDLA-312] published in [SDLA-102] therefore apply to SSA.

[SDLA-312] *ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*, as specified at http://www.ISASecure.org

[SDLA-102] *ISCI Security Development Lifecycle Assurance – Errata for SDLA specifications*, as specified at http://www.ISASecure.org

3 Definitions and abbreviations

If not provided in errata text of this document, definitions and abbreviations for the terms used in this document are found in the documents for which errata are described, which are those document versions listed in Clause 4.

4 Index to errata

This clause lists all ISASecure SSA specifications that may be the subject of errata, and indicates for each specification whether errata apply to this specification. If so, the table below provides the sub clause reference in this document that lists specific modifications for these errata.

Table 1 - ISASecure SSA Errata Index

Document ID	Document Title	Version	Errata	Reference in this document
SSA-100	*ISA Security Compliance Institute – System device security assurance – ISASecure Certification Scheme*	1.7	Yes	5.2
SSA-200	*ISCI System Security Assurance – ISASecure SSA Chartered laboratory operations and accreditation*	1.9	Yes	5.3
SSA-204	*ISCI System Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*	1.2	Yes	5.4
SSA-205	*ISCI System Security Assurance – Certificate Document Format*	1.2	Yes	5.5
SSA-300	*ISCI System Security Assurance – ISASecure certification requirements*	1.4	Yes	5.6
SSA-301	*ISCI System Security Assurance – Maintenance of ISASecure certification*	1.6	No	
SSA-310	*ISCI System Security Assurance – System robustness testing*	2.0	Yes	5.7
SSA-311	*ISCI System Security Assurance – Functional security assessment for systems*	1.82	Yes	5.8
SSA-312	*ISCI System Security Assurance – Security development artifacts for systems*	1.01	No	
SSA-420	*ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*	2.6	No	

5 Errata by document

5.1 General

This clause lists all errata that apply to the documents in Table 1.

The errata include a subset of errata for each document SSA-100, 200, 204, 205, 300, and 310, grouped below under the sub clauses titled “scalability errata.” Taken together, these errata enhance the SSA certification program to offer a single certificate that covers multiple layouts offered by a supplier for a scalable control system. The terms *layout* and *scalable control system* are defined below in the content of these errata.

5.2 SSA-100 Certification scheme

The following errata apply to SSA-100 version 1.7.

5.2.1 Scalability errata

- **Add definitions:** In Section 3.1, add the following terms and definitions:

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

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

- **Modify scope of SSA certification to cover scalable systems:** In Section 4.1, replace the text of the third bullet which currently says “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, ” by the text “The control system may have a fixed device and zone layout, or may be scalable, that is, may support replication of devices and of zones in order to scale for small and large installations.”

- **Modify scope of SSA certification to cover scalable systems:** In Section 4.1, add to the beginning of the last paragraph, the sentence: “[SSA-300] further specifies the architectural similarity required between layouts that are to be certified under a single SSA certificate.”

- **Overview certification approach for scalable systems:** To the end of Section 4.2, add the paragraph: “For scalable systems, tests performed by the certifier as part of FSA-S or SRT will be performed on a reference system, whose layout meets criteria specified in [SSA-300]. Analyses performed by the certifier will take into account all layouts to be evaluated under the certification.”

- **Require that certificate specify set of layouts:** In Section 4.4, first paragraph, insert in existing text the italicized text as follows: Certification applies to a particular version of a system*, a specific layout or (for a scalable system) a set of layouts*, and references a 3-digit certification version that identifies the set of ISASecure specifications used for the certification. For example, system model 234, version 1.9 *with layouts as described in a named reference document*, might be certified to ISASecure SSA 2.6.1.

5.2.2 Other errata

- **Update reference:** In 2.4.2, change the date on reference [ISO/IEC 17025] to 15 May 2005.

5.3 SSA-200 Chartered laboratory

The following errata apply to SSA-200 version 1.9.

5.3.1 Scalability errata

- **Add definitions:** In Section 3.1, add the following terms and definitions, including the note:

  layout, as in 5.2.1 of this errata document for SSA-100

  scalable control system, as in 5.2.1 of this errata document for SSA-100

  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.

- **Modify scope of SSA certification to cover scalable systems** (as in 5.2.1 of this errata document for SSA-100)**:** In Section 4.1, replace the text of the third bullet which currently says "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, " by the text "The control system may have a fixed device and zone layout, or may be scalable, that is, may support replication of devices and of zones in order to scale for small and large installations."

- **Overview certification approach for scalable systems** (as in 5.2.1 of this errata document for SSA-100)**:** To the end of Section 4.1, add the paragraph: "For scalable systems, tests performed by the certifier as part of FSA-S or SRT will be performed on a reference system, whose layout meets criteria specified in [SSA-300]. Analyses performed by the certifier will take into account all layouts to be evaluated under the certification."

- **Add technical readiness criteria related to scalability:** In Section 7.3 table 9, modify the evaluation criteria column as follows:

  - In row 1, add "Comply with requirement for certifying scalable systems, that all certification testing is performed on a reference system that meets requirements of ISASecure_SY.R3S in [SSA-300]"

  - In row 8, insert the text in italics in the existing text shown: "Application requests all items required per *[SSA-300] Section 5.1.1 and* [SSA-310] Sections 6.2 and 8"

  - In row 9, insert the text in italics in the existing text shown: "Scope and results of FSA-S evaluation are consistent with security zone levels *and cover system layouts to be certified*"

  - In row 9, add "Scope, artifacts and results from SDA-S take into account all system layouts in scope for the certification"

5.3.2 Other errata

- **Update reference:** In 2.5.2, change the date on reference [ISO/IEC 17025] to 15 May 2005.

- **Add to the abbreviations table in 3.2,** the following entries:

  - CSSLP, an abbreviation for Certified Secure Software Lifecycle Professional

  - CACE, an abbreviation for Certified Automation Cyber Security Expert

  - CACS, an abbreviation for Certified Automation Cyber Security Specialist

- **Accept CSSLP, CACE and CACS professional certifications:**
    - In 6.4.3.1, Requirement SSA.R10, Table 4 - FSA-S, FSA-E, and SDA-S and SDLPA auditor qualifications, replace the row for Professional certification to add CSSLP, CACE and CACS as follows:

Professional certification	• CISA, CISSP, GICSP, CACE, CACS, or equivalent	• CISA, CISSP, GICSP, CSSLP, CACE, CACS, or equivalent

    - In 6.4.3.1, Requirement SSA.R12, Table 6 - VIT lead evaluator qualifications, replace the row for Professional certification to add CACE and CACS as follows:

Professional certification	• CISA, CISSP, GICSP, CACE, CACS, or equivalent

- **Accept any bachelor's degree:** In 6.4.3.1, Requirement SSA.R10, Table 4 - FSA-S, FSA-E, and SDA-S and SDLPA auditor qualifications, replace the rows for "Formal education" and "Work experience post BS degree," by rows as follows for "Formal education" and "Work experience in field":

Formal education	• BS Electrical Engineering **OR** • BS Computer Engineering (CE) **OR** • BS Computer Science (CS) **OR** • BS Chemical Engineering with CE or CS minor **OR** • Equivalent science or engineering degree **OR** • Bachelors or equivalent level degree (any field)	• BS Electrical Engineering **OR** • BS Computer Engineering **OR** • BS Computer Science **OR** • BS Chemical Engineering with CE or CS minor **OR** • Equivalent science or engineering degree **OR** • Bachelors or equivalent level degree (any field)
Work experience in field	• Min 8 years experience in computer technology field • Degree in field named above substitutes for 4 years of experience	• Min 8 years experience in computer technology field • Degree in field named above substitutes for 4 years of experience

5.4 SSA-204 Symbols and certificates

The following errata apply to SSA-204 version 1.2.

5.4.1 Scalability errata

- **Add definitions:** In Section 3.1, add the following terms and definitions:

  layout, as in 5.2.1 of this errata document for SSA-100

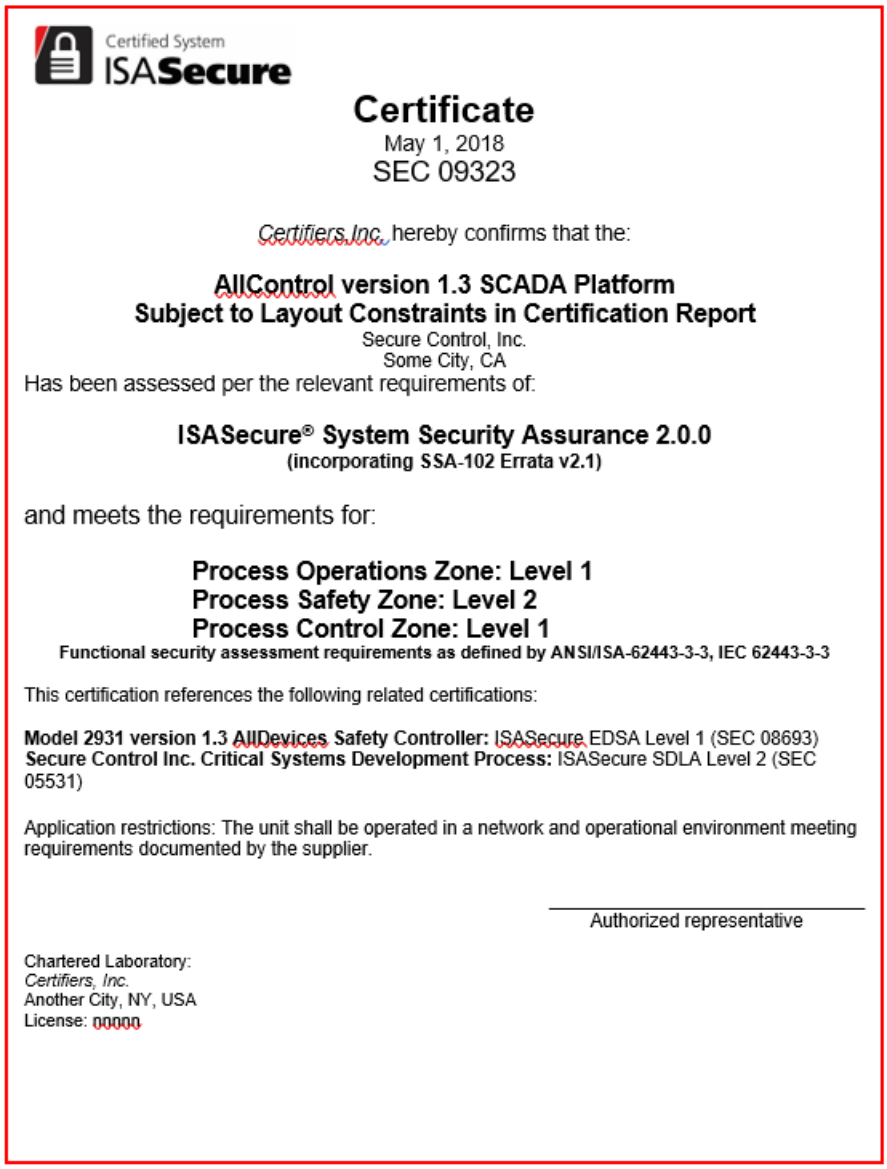
  scalable control system, as in 5.2.1 of this errata document for SSA-100

- **Add layouts to certificate format:** Add the following paragraph before the certificate example in Section 5: “The SSA specifications support a "scalability" scenario in which a single certificate may cover several different layouts for a system. Layouts may include varying quantities of devices and/or

zones to scale for large and small installations. The certificate for such a system shall include a reference to a document that describes the layouts covered by the certification. In the example certificate below, this reference is the certification report."

5.4.2 Other errata

- **Update reference:** In Clause 2, change the date on reference [ISO/IEC 17025] to 15 May 2005.
- **Add name of standard to certificate:** Replace Clause 5, Figure 1 with the following figure, which adds a line to reference the 62443-3-3 standard. Note this figure also reflects the certificate format change related to scalability described in 5.4.1 of this errata document.



Certified System
ISASecure

Certificate
May 1, 2018
SEC 09323

Certifiers Inc. hereby confirms that the:

AllControl version 1.3 SCADA Platform
Subject to Layout Constraints in Certification Report
Secure Control, Inc.
Some City, CA
Has been assessed per the relevant requirements of:

ISASecure® System Security Assurance 2.0.0
(incorporating SSA-102 Errata v2.1)

and meets the requirements for:

Process Operations Zone: Level 1
Process Safety Zone: Level 2
Process Control Zone: Level 1
Functional security assessment requirements as defined by ANSI/ISA-62443-3-3, IEC 62443-3-3

This certification references the following related certifications:

Model 2931 version 1.3 AllDevices Safety Controller: ISASecure EDSA Level 1 (SEC 08693)
Secure Control Inc. Critical Systems Development Process: ISASecure SDLA Level 2 (SEC 05531)

Application restrictions: The unit shall be operated in a network and operational environment meeting requirements documented by the supplier.

Authorized representative

Chartered Laboratory:
Certifiers, Inc.
Another City, NY, USA
License: nnnnn

5.5 SSA-205 Certificate document format

The following errata apply to the format document SSA-205 version 1.2.

5.5.1 Scalability errata

- **Add reference for certified layouts to certificate:** For scalable control systems where more than one layout is covered by a certification, add a line to the certificate document format to reference a document that lists certified layouts, as shown above, in the erratum for SSA-204 Figure 1

5.5.2 Other errata

- **Add name of standard to certificate:** Add a line to the certificate document format to reference the 62443-3-3 standard, as shown above, in the erratum for SSA-204 Figure 1

5.6 SSA-300 Certification requirements

The following errata apply to the specification SSA-300 version 1.4.

5.6.1 Scalability errata

- **Add definitions:** In Section 3.1, add the following terms and definitions, including the note:

  layout, as in 5.2.1 of this errata document for SSA-100

  scalable control system, as in 5.2.1 of this errata document for SSA-100

  reference layout, as in 5.3.1 of this errata document for SSA-200

  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.

- **Modify scope of SSA certification to cover scalable systems** (as in 5.2.1 of this errata document for SSA-100)**:** In Section 1.2, replace the text of the third bullet which currently says “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, ” by the text “The control system may have a fixed device and zone layout, or may be scalable, that is, may support replication of devices and of zones in order to scale for small and large installations.”

- **Modify scope of single certificate:** In Section 1.2, add paragraph at end: “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.”

- **Overview certification approach for scalable systems** (as in 5.2.1 of this errata document for SSA-100)**:** To the end of Section 4.2, add the paragraph: “For scalable systems, tests performed by the certifier as part of FSA-S or SRT will be performed on a reference system, whose layout meets criteria specified in this document. Analyses performed by the certifier will take into account all layouts to be evaluated under the certification.”

- **Introduce scalability background material:** In Section 5.1, insert the text in italics into the existing text shown: “This clause *provides an informal overview of scalability concepts in 5.1.1, and then* formally defines the requirements to achieve ISASecure SSA certification for a system.

- **Add scalability background material:** Add section 5.1.1 with title “Zone and layout definition,” and content as follows:

“5.1.1 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 2S 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 2S, 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 2S. 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 2S - 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.R1S – 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 2S columns 1-7 SHOULD be used to define the set of zones to be evaluated in the certification.

Requirement ISASecure_SY.R2S – 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.R1S 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.R1S 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.R1S, 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 2S 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 1S, 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.R4, 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.R3S – 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.R2S:

- The layout includes all zones identified per ISASecure_SY.R1S
- 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."

<end of new section 5.1.1>

- **Reference certified layouts in published certification information:** In Section 5.2, Requirement ISASecure_SY.R2, insert the text in italics in the existing text shown: "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.

- **SDA and FSA assessments take layouts into account:** In Section 5.3, Requirement ISASecure_SY.R4, add the text in italics to the existing text shown in the SDA and FSA rows and Requirement column of the table:

  - 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.*

  - 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.R3S. Other FSA-S validations SHALL take into account all layouts for each zone in scope for the certification.

- **SRT takes layouts into account:** In Section 5.3, Requirement ISASecure_SY.R4, add the text in italics to the existing text shown in the Requirement column, SRT row in the table: "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.R3S*."

- **Reference to example scalable system:** Add the following note at the beginning of Section 6, Annex: System example: "NOTE The example described in this section has a fixed layout. A certification example for a scalable system, will be available in the document SSA-300 as revised for certification program version SSA 2.1.0."

5.6.2 Other errata

- **Delete restriction of NST addressing modes:** In 6.3.5.4, Table 6, first column, delete the phrase "using broadcast and multicast addressing"

5.7 SSA-310 Requirements for system robustness testing

The following errata apply to the specification SSA-310 version 2.0.

5.7.1 Scalability errata

- **Add definitions:** In Section 3.1, add the following terms and definitions:

  layout, as in 5.2.1 of this errata document for SSA-100

  scalable control system, as in 5.2.1 of this errata document for SSA-100

  reference layout, as in 5.3.1 of this errata document for SSA-200

  reference system, as in 5.6.1 of this errata document for SSA-300

- **Distinguish system certified from system tested:** In Section 4.1.2, Requirement SRT.R1 replace two instances of the phrase “submitted for certification” by “submitted for SRT”

- **Introduce scalability concepts:** Replace the text in Section 6.1 by: “The system to be certified, in part based upon SRT, is a system such as a Control System (CS), SCADA system or monitoring system that is available from a single system supplier. A system to be certified may be comprised of hardware and software components from several manufacturers but is integrated into a single system and supported, as a whole, by a single supplier. A system may be scalable, that is, that is, may support replication of devices and of zones in order to scale for small and large installations. SRT evaluation will be performed on a reference system, referred to here as the SUT (system-under-test) that is clearly defined by the applicant. For scalable systems, requirements for choosing a reference system are found in [SSA-300].”

- **Require system diagram for reference system:** In Section 6.2, Requirement SRT.R2, in the first sentence, replace the phrase “system to be certified” by “reference system to be tested”

- **Submission of reference system:** In Section 6.2, Requirement SRT.R15, replace the text of this requirement by “A certification applicant SHALL submit to the certification process a suitable test system that meets the requirements for a reference system in [SSA-300], and that is representative of the specified usage of the system to be certified.”

5.7.2 Other errata

- **Clarify definition of operational mode:** In 3.1.14, modify the definition of operational mode and the note following it to read: " one of several states selectable by the user that are mutually exclusive, such that the device must be in exactly one of these states, and where the state determines which device functions are available when the device is in that state, such as functions for configuration, control operations, update of firmware

  NOTE Not all embedded devices use the concept of operational mode. An operational mode is primarily designed to control the availability of functions on the device rather than to define details about how these functions will operate."

- **Clarify definition of adequately maintain essential history reporting:** In 4.1.1.6, replace the following text “Essential history data is not lost during flooding, though reporting of data may be delayed” by the text “Reporting of data may be delayed. However, essential history data is not lost other than due to continuous flooding on the reporting interface for an extended period. Essential history data is considered lost if records for events that have been specified as essential history are permanently missing from essential history storage. The supplier documents parameters that define the extent of continuous flooding that can occur without the loss of any essential history data. If extended flooding occurs that exceeds these parameters, then the loss of essential history data is acceptable.”

- **Clarify meaning of parameters defining extensive flooding:** At the end of 4.1.1.6, add the following note: “NOTE 2 Maximum parameters specified by the supplier for an extended network interruption may for example be a length of time, a number of records, or the data size of a set of records.”

- **Clarify how essential history data may be specified:** In 6.2, replace requirement SRT.R8 by: “A certification applicant that considers maintaining process history an essential function and does not exclude this per SRT.R7 SHALL describe those events that are considered essential history, and associated types of historical records and fields in these records that are therefore considered to be essential history data.”

- **Permit alternative method of transition detection:** In section 10.4.1, requirement SRT.R38, change the second sentence after NOTE 2 to read as follows, and add a note as shown: " A transition SHALL be determined to have occurred using one of these criteria:
    - when the voltage crosses above a high threshold level of 90% of total voltage rise expected, or below a low threshold level of 90% of the total fall expected
    - when the voltage crosses above a high threshold level which is a specified voltage less than the total voltage rise expected, or a specified voltage more than the total fall expected. For all steps, the specified voltage shall be 10% of the voltage of the smallest step found in the signal.

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

- **Change limit on measurement jitter:** In section 10.4.1, requirement SRT.R38, change 1% measurement jitter permitted to 2%, so that the third sentence after NOTE 2, and the text of NOTE 3 are modified to read: "The TD employed to test an embedded device shall itself introduce a maximum measurement error (measurement jitter) of no more than 2% of the period at constant state for the test signals defined in this requirement.

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

  The number of this note has changed from 3 to 4, due to the previous erratum.

- **Modify CRT requirement for testing of redundant devices:** In 12.1, requirement SRT.R48, delete the requirement for CRT when performed as part of SRT, to comply with requirement ERT.R37 in [EDSA-310], except for the case of embedded devices. Therefore SRT.R48 and the note following it are replaced with the following text:

Requirement SRT.R48 – Types of CRT tests

CRT for a system SHALL comply with requirements of protocol specific robustness testing as defined below, as well as [EDSA-310] requirements: ERT.R36, ERT.R38, ERT.R39, ERT.R40, ERT.R41, ERT.R42, ERT.R43, ERT.R48, and ERT.R49. CRT for embedded devices that are components of the system SHALL also comply with ERT.R37.

NOTE 1 ERT.R37 discusses test of redundant device configurations. Even if an embedded device component is only deployed in a redundant configuration for the system submitted for certification, a test with non-operational units is required, to assure continued operation in the event of a failed or non-operational device.

- **Clarify CRT requirement from external interfaces:** In 12.1, the first sentence of the first paragraph of Requirement SRT.R49 is modified to read " Communication robustness testing as defined in Section 12 SHALL be performed from each external interface to the system, transiting any boundary devices, and targeting any device reachable from that external interface, except that firewall devices on the system perimeter SHALL NOT be a target for test traffic."

  Also, the note to Requirement SRT.R49 is modified to read:

"NOTE 2 "Ethernet" and ARP CRT tests are performed from external interfaces even though this test traffic may not reach any devices inside the system boundary."

- **Modify NST requirement for testing of redundant devices:** In 13.1, requirement SRT.R54, delete the requirement for NST to comply with requirement ERT.R37 in [EDSA-310].

- **Require CRT tool full version and hash values:** In 14.1, requirement SRT.R69, replace "full version identifiers or hash values” by "full version identifiers and hash values"

5.8 SSA-311 Functional Security Assessment for systems

The following erratum applies to SSA-311 version 1.82.

- **Correct applicable levels for session ID requirements:** For Requirement FSA-S-SI-8.1 and Requirement FSA-S-SI-8.2, add Security level 2, thereby replacing Security level "3, 4" by "2, 3, 4."

— — — — — —