ISASecure-112

ISA Security Compliance Institute — ISASecure certification programs

Guidance for transition to EDSA 2.0.0 and SSA 2.0.0

Version 1.4

May 2015

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
1.3	2015.04.27	Initial version published to http://www.ISASecure.org
1.4	2015.05.11	Correct SSA 2014.1 versions in Table 4 for SSA-100, SDLA-100, and SDLA-312

Contents

Tables

FOREWORD

This is one of a series of documents that defines ISASecure certification programs. This document is an informative description of the differences between the EDSA 2010.1 certification program and the EDSA 2.0.0 certification program; and between the SSA 2014.1 certification program and the SSA 2.0.0 certification program. Documents that define these ISASecure certification programs, are found on the web site http://www.ISASecure.org.

1 Background and scope

ISCI (ISA Security Compliance Institute) operates a product certification program for embedded devices, called ISASecure EDSA (Embedded Device Security Assurance) and for control systems, called ISASecure SSA (System Security Assurance). These programs were recently upgraded with version identifiers as follows.

- EDSA: initial version EDSA 2010.1
- EDSA: upgraded version EDSA 2.0.0
- SSA: initial version SSA 2014.1
- SSA: upgraded version SSA 2.0.0

The specifications that define these program versions, are found on the ISCI web site http://www.ISASecure.org, and are listed in Sections 6 and 7.

This document describes the differences between the initial and upgraded versions of these certification programs. It is an informative resource intended to assist certifiers, test tool suppliers and suppliers interested in certification of their products, in planning for the transition to the new certification versions. It is intended to be used together with the documentation for the prior and upgraded program versions, as a guide to identifying areas of change.

ISCI will publish a separate policy document [ISASecure-113] that specifies time frames for the transition of certification operations to the new certification versions.

2 References

The following document describes time frames for the transition to ISASecure EDSA 2.0.0 and ISASecure SSA 2.0.0.

[ISASecure-113] *ISCI ISASecure Certification Programs - Policy for transition to EDSA 2.0.0 and SSA 2.0.0,* to be published at http://www.ISASecure.org

The following document was used as a reference by the EDSA 2010.1 and SSA 2014.1 programs. It is no longer a reference for EDSA 2.0.0 and SSA 2.0.0. The program requirements that it contained are transitioned as described in the present document.

[ASCI Lab] *ASCI Chartered Testing Laboratory 2009 Approval Process*, as specified at http://www.ISASecure.org

The following document is used as a reference by the EDSA 2.0.0 and SSA 2.0.0 programs.

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

The present document addresses compliance under the EDSA and SSA programs to the following international standards.

[ISO/IEC Guide 65] ISO/IEC Guide 65, "*General Requirements for Bodies Operating Product Certification Systems*", 1996

[ISO/IEC 17065] ISO/IEC 17065.2012, "*Conformity assessment—requirements for bodies certifying products, processes and services*", October 2012

[ISO/IEC 17025] ISO/IEC 17025, “*General requirements for the competence of testing and calibration laboratories****”,*** 15 May 2005

The full set of normative references for the programs EDSA 2010.1, EDSA 2.0.0, SSA 2014.1, and SSA 2.0.0 can be found on the ISCI web site http://www.ISASecure.org. They are listed in tables in Sections 6 and 7 of this document for reference.

3 Definitions and abbreviations

3.1 Definitions

Definitions are found in the references described in Section 2 of this document

3.2 Abbreviations

The following abbreviations are used in this document.

ASCI	Automation Standards Compliance Institute
ARP	address resolution protocol
CB	certification body
CRT	communication robustness testing
CSSLP	certified secure software lifecycle professional
DUT	device under test
ED	embedded device
EDM	embedded device maintenance [of certification], prefix for requirements in EDSA-301
EDSA	embedded device security assurance
ERT	embedded device robustness testing
FSA-E	functional security assessment for embedded devices
GICSP	Global Industrial Cyber Security Professional
IEC	International Electrotechnical Commission
IETF	Internet engineering task force
ICMP	Internet control message protocol
IP	Internet protocol
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Organization for Standardization
NPDU	network protocol data unit
NST	network stress testing
R*n*	notation for numbering requirements in ISASecure specifications
SDA-E	security development artifacts for embedded devices
SDLA	security development lifecycle assurance
SDSA	software development security assessment
SDLPA	security development lifecycle process assessment
SRT	system robustness testing
SSA	system security assurance
TCP	transmission control protocol
T*n*	notation for numbering tests in ISASecure specifications
UDP	user datagram protocol
VIT	vulnerability identification testing

4 EDSA 2010.1 to EDSA 2.0.0

4.1 Overview

This section includes:

- a list of categories of changes to certification program requirements, used for classifying the changes from EDSA 2010.1 to EDSA 2.0.0 (Section 4.2)
- terminology and notation changes (Section 4.3)
- documentation changes that do not impact certification program requirements (Section 4.4)
- a list of program requirement changes by category, noting relevant references and those types of organizations that may be affected by each change (Section 4.5).

4.2 Change categories

Categories of changes involved in the transition from the certification program EDSA 2010.1 to EDSA 2.0.0 are as follows.

- **17065:** Replace ISO/IEC Guide 65 compliance by ISO/IEC 17065 compliance, for ISASecure certification bodies (chartered laboratories). This document does not analyze detailed changes in requirements due to this transition.
- **SDLA:** Replace the EDSA SDSA certification element by two elements, security development lifecycle process assessment (SDLPA) and security development artifact assessment (SDA-E). SDLPA may be waived if a supplier holds a separate ISASecure SDLA certification, which is a process certification. This change is a program structural and documentation change. The technical requirements on security lifecycle development processes for embedded device suppliers should remain the same as under SDSA.
- **EDSA VIT:** Add requirement for Vulnerability Identification Testing (VIT).
- **Jitter:** Further detail the specification for detecting excessive jitter, which determines pass/fail for robustness tests.
- **Test coverage:** Add additional tests and test details in the CRT specifications.
- **CB process:** General process requirements on ISASecure certification bodies (CBs), known as chartered laboratories.
- **Tool recognition:** General requirements for CRT tool recognition not related to a specific CRT test.
- **ASCI Lab:** The prior version of EDSA-200 incorporated requirements from [ASCI Lab] by reference. EDSA 2.0.0 directly incorporates most requirements from [ASCI Lab] into EDSA-200. Those not incorporated were either not applicable or already covered by ISO/IEC 17025.
- **Report admin:** Add administrative information and a few technical corrections to sample certification report sample EDSA-303.

The list of specific changes in each of these categories is provided in 4.5.

4.3 Terminology and notation changes

ISASecure programs have a *certification version*, that in turn defines the full set of *specification versions* used to perform a specific certification. Previously, this version number included a year and number such as EDSA 2010.1. Going forward, ISASecure certification programs will use a three place version identifier as in the example EDSA 2.0.0.

In accordance with ISA 62443 effort, the term *essential service* used in EDSA 2010.1, is replaced by the term *essential function* in all ISASecure documents. There is no change to the definition as used for EDSA 2.0.0.

The term *embedded device robustness testing* (ERT) is introduced, which consists of CRT and the newly introduced vulnerability identification testing (VIT), for embedded devices.

The EDSA 2010.1 specification EDSA-312 for SDSA (software development lifecycle assessment) required both examination of a supplier's documented development process, and examination of artifacts from that process for the product presented for certification. These two concepts are now separated and are called, respectively, SDPLA (security development process lifecycle assessment) and SDA-E (security development artifacts for embedded devices).

4.4 Documentation changes with no impact on program requirements

The addition of VIT to EDSA introduced structural changes to EDSA-310 *Embedded device robustness testing*, which resulted in renumbering of existing requirements in that document. This in turn impacted the numbering in EDSA-201 *Recognition process for communication robustness testing tools*, which enumerates requirements in EDSA-310. The appendix to the present document provides a mapping from EDSA-310 v2.2 requirement numbers to their numbers in the prior version EDSA-310 v1.7. There are no VIT related requirements for tool recognition.

The introduction of VIT, SDLPA and SDA-E also introduced structural changes to EDSA-301 *Maintenance of ISASecure certification*. However, material that existed in the prior document has not changed, with the exception of item 21 in Table 1 below, regarding the concept of confidence in an evidence impact assessment.

In EDSA-300*, ISASecure certification requirements*, sub clause 5.3 regarding maintenance of certification is deleted, since this is duplicated in EDSA-301. There is no net impact on program requirements.

Errata for EDSA-403 v1.31 and EDSA-406 v1.41, the IPv4 and TCP CRT specifications, that are presented in EDSA-102 *Errata for EDSA specifications* v1.2, have been directly incorporated into revised versions of these documents. That move had no net impact on program requirements. The revised versions of EDSA-403 and EDSA 406 do incorporate other changes that impact program requirements as detailed in Section 4.5 below. For the remaining protocols, changes to the documents EDSA-401, 402, 404, and 405 are limited to additional errata in a revised EDSA-102.

The TCP protocol description in EDSA-406 has been updated to mark some protocol features as obsolete. Since attackers may continue to use obsolete features, these changes have been made for accuracy but have no net impact on program requirements.

Note that there are no changes to the document EDSA-311 *Functional security assessment for embedded devices.*

4.5 List of changes to program requirements

The following table enumerates changes to program requirements when moving from ISASecure EDSA 2010.1 to EDSA 2.0.0.

- The first column is a reference number for the purposes of this document.
- The second column indicates whether the change places *additional* requirements on one or more organizations participating in the program (+), whether it *changes* a requirement already present (C), or whether it *deletes* a requirement previously present (-).
- The third column shows the change category and describes the change.
- The references in the fourth column refer to EDSA 2.0.0 document versions listed in Section 6 of this document.

- The last three columns indicate which participating organizations are expected to find a difference in their requirements for participating in the program, due to this change.

Table 1. Certification program changes EDSA 2010.1 to EDSA 2.0.0

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
1.	C	**17065:** Change from ISO/IEC Guide 65 compliance to ISO/IEC 17065 compliance for chartered laboratories. EDSA-200 is restructured in accordance with the new standard.	EDSA-100 EDSA-200		X	
2.	C	**SDLA:** Replace SDSA certification criteria by requirement for equipment supplier either to hold an ISASecure SDLA certification, or to undergo SDPLA as part of EDSA certification, as well as to undergo (in either case) a security artifact assessment (SDA-E) for the embedded device. EDSA-312 *Software Development Security Assessment* is replaced by new documents SDLA-312 *Security Development Lifecycle Assessment* and EDSA-312 *Security development artifacts for embedded devices.* The new EDSA-312 replaces the previous SDSA document that used this same document number.	EDSA-100 EDSA-300 ISASecure_ED.R5 EDSA-301 Clause 5 ISASecure_EDM.R1-R3 EDSA-303 Management Summary, Sections 1, 5 EDSA-312	X	X	
3.	+	**EDSA VIT:** Add Vulnerability Identification Testing (VIT) to EDSA certification criteria. This new criterion is covered in the revised and renamed EDSA-310 (from "*Common requirements for communication robustness testing of IP-based protocol implementation*" to "*Requirements for embedded device robustness testing*"), and SDLA-420 " *ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification* ". This requirement entails additional processes, tools and qualifications for the chartered laboratory.	EDSA-100 EDSA-200 EDSA.R12, Table 8 EDSA-300 Clauses 1 and 4, and ISASecure_ED.R5 (via reference to ERT) EDSA-303 Management Summary, 1, 6.5, 8 EDSA-301 6.2 EDSA-310 Clause 8, 9.4 SSA-420 (entire	X	X	

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
			document)			
4.	-	**Jitter:** Delete requirement to submit cycle time for device	EDSA-310 ERT.R12 (formerly CRT.R11)	X	X	
5.	+	**Jitter:** Require at least 95% confidence for submitted maximum jitter tolerance	EDSA-310 ERT.R12 (formerly CRT.R11)	X	X	
6.	C	**Jitter:** Changed maximum permitted measurement jitter	EDSA-310 ERT.R30 (formerly CRT.R39)		X	X
7.	+	**Jitter:** Added specification detail for determining excessive jitter	EDSA-310 ERT.R30, (formerly CRT.R39) text after NOTE 2	X	X	X
8.	-	**Test coverage:** Deleted requirement to support testing of devices that do blacklisting	EDSA-310,removed former CRT.R53. Requirement had not been enforced in practice, so no actual impact.		X	
9.	C	**Test coverage:** Increase duration of load stress tests from tens of seconds to two minutes.	EDSA-310 ERT.R28 EDSA-401 "Ethernet".R10 "Ethernet".T8 EDSA-402 ARP.R10, ARP.T10 EDSA-404 ICMPv4.R13, ICMP.T08 EDSA-405 UDP.R9, UDP.T09 For all of above, change seen in 5.4, 5.5, 5.6, 5.7 EDSA-102 *Errata for EDSA Specifications* EDSA-403 IPv4.R14, IPv4.T14 EDSA-406 TCP.R11, TCP.T24	X	X	X

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
10.	+	**Test coverage:** Add test: Inconsistent frame length	EDSA-401 Ethernet.T09 Change seen in 5.4 EDSA-102 *Errata for EDSA Specifications*	X	X	X
11.	+	**Test coverage:** Add test: Invalid hardware or protocol type	EDSA-402 ARP.T11 Change seen in 5.5 EDSA-102 *Errata for EDSA Specifications*	X	X	X
12.	C	**Test coverage:** Correct definition and meaning of NPDU header field TotalLength	EDSA-403 4.2.2 and 4.2.4.6.1 b) and c), IPv4.R10			X
13.	+	**Test coverage:** require IPv4.T06 to test each defined option; require IPv4.T08 to test instances of each restricted source-address class, require IPv4.T11 to include defects of IPv4.R10 classes c), d) and e); extended IPv4.T12 to include DUT discard of overly-long reassembled NPDU; add detail to IPv4.T13	EDSA-403 Clause 7	X		X
14.	+	**Test coverage:** Add requirements to existing test: UDP.T07 should address unassigned as well as reserved ports	EDSA-405 UDP.T07; change seen in 5.7 EDSA-102 *Errata for EDSA Specifications*	X		X
15.	+	**Test coverage:** Sample size requirement for dieharder tests	EDSA-406 Clause 7 TCP.T01	X	X	X
16.	C	**Test coverage:** Change expected DUT response to test to remove conformance aspects	EDSA-406 Clause 7 TCP.T14	X	X	X
17.	+	**Test coverage:** Add sentence to test descriptions TCP.T07 and TCP.T09; correct "connection" to say "connections" in TCP.T13 test description	EDSA-406 Clause 7 TCP.T07, TCP.T09, TCP.T13	X	X	X
18.	C	**Test coverage:** Clarify specification for TCP.T11	EDSA-406 Clause 7 TCP.T11	X	X	X

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
19.	+	**Test coverage:** For tool recognition, added tests will require mapping under "Ethernet".R14 et. al. in Table 4, and PCAPs under Step 4. Added tests are "Ethernet".T09 and ARP.T11, described in errata document EDSA-102.	EDSA-201 EDSA-102 5.4, 5.5			X
20.	+	**CB process:** Added detail regarding submission of rate limiting information	EDSA-310 ERT.R19 (formerly CRT.R18)	X	X	
21.	C	**CB process:** Introduced concept of confidence in an evidence impact assessment, replacing "cost effectiveness" in prior version	EDSA-301, throughout	X	X	
22.	-	**CB process:** Reference for test failure can be a set of requirements, does not need to be a single requirement	EDSA-310 ERT.R61 (formerly CRT.R24)		X	X
23.	+	**CB process:** Recovery of essential functions from flooding must be without operator intervention	EDSA-310 7.1.4.2	X	X	
24.	C	**CB process:** Changed definitions for adequately maintain alarms, history, peer to peer communication	EDSA-310 7.1.4.2	X	X	
25.	C	**CB process:** Change to meaning of provisional chartered laboratory status; must meet all requirements and be awaiting final accreditation body approval - except for part of technical readiness requirements typically verified during first certification	EDSA-200 7.2		X	
26.	+	**CB process:** Clarified impartiality requirements for chartered laboratory, revising requirements previously found in [ASCI Lab] section III, and referenced from EDSA-200.	EDSA-200 6.3.3		X	
27.	C	**CB process:** No calibration is required for the CRT tool.	EDSA-200 EDSA.R28		X	
28.	C	**CB process:** GICSP and CSSLP certification added as options for professional certification.	EDSA-200 6.4.3.1 GICSP in Tables 4		X	

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
			and 6 CSSLP in Table 4			
29.	+	**CB process:** Confirmation of full software version of CRT tool on reports is required	EDSA-200 EDSA.R19		X	X
30.	C, -	**CB process:** Process for determining equipment supplier applicant eligibility; clarifies responsibilities and escalation. Otherwise, I.C.8 in [ASCI Lab] does not apply and these requirements are deleted.	EDSA-200 EDSA.R15	X	X	
31.	+	**CB process:** Requirement related to withdrawal of certification	EDSA-200 EDSA.R38	X	X	
32.	+	**Tool recognition:** Require full version identifiers on reports, AND hash values for CRT tool under ERT.R64 (previously CRT.R27)	EDSA-201 Table 3		X	X
33.	C	**Tool recognition:** Modified specification of maximum traffic rate for CRT tool; deleted maximum CRT tool traffic rate requirement from EDSA-310 (CRT.R54); instead made it an evidence requirement for ERT.R43	EDSA-201 Table 3			X
34.	+	**Tool recognition:** Require pseudo random test generation for CRT tools	EDSA-401 "Ethernet".R11 EDSA-402 ARP.R11 EDSA-402 ICMPv4.R14 EDSA-405 UDP.R10 For all above, change seen in 5.4, 5.5, 5.6, 5.7 EDSA-102 *Errata for EDSA Specifications* EDSA-201 Table 3 reflects changes for the above and:			X

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
			EDSA-403 IPv4.R15 EDSA-406 TCP.R12 In addition, Table 4 EDSA-310 ERT.R47 (formerly CRT.R62)			
35.	+	**Tool Recognition:** Tool supplier to provide test reports along with PCAP files in Step 4	EDSA-201 4.1 Table 1			X
36.	-	**Tool Recognition:** Delete basic Step 3 evidence of original and reproduced results	EDSA-201 4.1 Table 1			X
37.	+	**Tool Recognition:** Delete specific count of Step 1 requirements to be met before going on to Step 2	EDSA-201 4.2, paragraph after Table 2			X
38.	-	**Tool Recognition:** Delete evidence under ERT.R1 of compliance with protocol reference standards (previously CRT.R1)	EDSA-201 Table 3			X
39.	C	**Tool Recognition:** Clarified guidance regarding required evidence in ERT.R14, ERT.R21, ERT.R30 (previously CRT.R13, CRT.R30 and CRT.R39)	EDSA-201 Table 3			X
40.	+	**Tool recognition:** Added required evidence regarding rate limiting and maximum traffic rate under ERT.R43 (previously CRT.R59)	EDSA-201 Table 3			X
41.	+	**Tool recognition:** Added requirement to verify device "hears" test traffic, as evidence under ERT.R45 (previously CRT.R60)	EDSA-201 Table 3			X
42.	+	**Tool recognition:** Added requirement to report max jitter tolerance and confidence per ERT.R57 (was CRT.R20 and this requirement has changed)	EDSA-201 Table 3			X

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
43.	+	**Tool recognition:** Request evidence related to verifying baseline operation under "Ethernet".R3 et. al.	EDSA-201 Table 4			X
44.	C	**Tool recognition:** Permit higher (design) level of evidence for test coverage under "Ethernet".R5 et. al.	EDSA-201 Table 4			X
45.	+	**Tool recognition:** User documentation to enumerate values of all configurable settings for ISASecure tests under "Ethernet".R14 et. al.	EDSA-201 Table 4			X
46.	C	**Tool recognition:** Added additional detail to evidence guidance for IPv4.R6 et. al., ICMPv4.R5 et. al., and TCP.R5 et. al.	EDSA-201 Table 4			X
47.	C	**ASCI Lab:** Document *ASCI Chartered Testing Laboratory 2009 Approval Process*, no longer a reference for EDSA-200; requirements directly incorporated into EDSA-200, if not already covered by ISO/IEC 17025.	EDSA-100 EDSA-200		X	
48.	-	**ASCI Lab:** Specific requirements regarding calibration and estimated accuracy of results deemed not applicable, so no longer included in EDSA-200, were [ASCI Lab] I.D.5, 6, 8 and IV.A.h.	EDSA-200		X	
49.	-	**ASCI Lab:** Employee safety program requirement deleted, so no longer included in EDSA-200, was [ASCI Lab] I.G.6.	EDSA-200		X	
50.	-	**ASCI Lab:** Follow-up and field inspection requirements not applicable, so no longer included in EDSA-200, were [ASCI Lab] II.B.1-8, 9b,c,e	EDSA-200		X	
51.	-	**Report admin:** Deleted concept of low/medium/high strength, not required	EDSA-303 Section 7 in bullet lists in hidden and regular text, was second bullet		X	

Number	Add/Delete /Change	Description	References	Embedded device supplier	Chartered laboratory	CRT tool supplier
52.	+	**Report admin:** Add restriction on reproduction of report; use ISASecure certification body logo	EDSA-303 title page		X	
53.	+	**Report admin:** Add dates of assessment	EDSA-303 Management Summary		X	
54.	+	**Report admin:** Add address of chartered laboratory	EDSA-303 2.1		X	
55.	+	**Report admin:** Added signatures to certification report	EDSA-303 Section 8.2		X	

5 SSA 2014.1 to SSA 2.0.0

5.1 Overview

This section includes:

- a list of categories of changes to certification program requirements, used for classifying the changes from SSA 2014.1 to SSA 2.0.0 (Section 5.2)
- terminology and notation changes (Section 5.3)
- a list of program requirement changes by category, noting relevant references and those types of organizations that may be affected by each change (Section 5.4).

5.2 Change categories

Categories of change involved in the transition from the certification program SSA 2014.1 to SSA 2.0.0 are as follows.

- **17065:** Replace ISO/IEC Guide 65 compliance to ISO/IEC 17065 compliance, for ISASecure certification bodies (chartered laboratories). This document does not analyze detailed changes in requirements due to this transition.
- **EDSA 2.0.0:** SSA 2014.1 documents refer to EDSA 2010.1 specifications. SSA 2.0.0 documents refer to EDSA 2.0.0 specifications, and thus incorporate all relevant changes described in Section 4 of the present document.
- **Jitter:** Further detail the specification for detecting excessive jitter, which determines pass/fail for robustness tests.
- **Test coverage:** Add additional tests and test details in the SRT (system robustness testing) specifications.

- **CB process:** General process requirements on ISASecure certification bodies (CBs), known as chartered laboratories. Note that the numbered requirements in EDSA-200 v3.2 and SSA-200 v1.9 are the same, except for personnel qualifications in 6.4.3.1 of those documents, and wording changes to refer to systems vs. embedded devices.
- **Tool recognition:** General requirements for CRT tool recognition not related to a specific CRT test, that are unique to the SSA program.
- **ASCI Lab:** The prior version of SSA-200 incorporated requirements from [ASCI Lab] by reference. SSA 2.0.0 directly incorporated most requirements from [ASCI Lab] into SSA-200. Those not incorporated were either not applicable or already covered by ISO/IEC 17025.
- **Report content:** Substantive changes to the technical content of the sample SSA certification report.
- **Report admin:** Add administrative information and a few technical corrections to sample certification report SSA-303.

The list of specific changes in each of these categories is provided in 5.4, with the exception of the category EDSA 2.0.0. Those changes are detailed in 4.5.

5.3 Terminology and notation changes

Terminology and notation changes parallel to those described in Section 4.3 for EDSA 2.0.0, apply for SSA 2.0.0.

5.4 List of changes to program requirements

The following table enumerates changes to program requirements when moving from ISASecure SSA 2014.1 to SSA 2.0.

- The first column is a reference number for the purposes of this document.
- The second column indicates whether the change places *additional* requirements on one or more organizations participating in the program (+), whether it *changes* a requirement already present (C), or whether it *deletes* a requirement previously present (-).
- The third column shows the change category and describes the change.
- The references in the fourth column refer to SSA 2.0.0 document versions listed in Section 7 of this document.
- The last three columns indicate which participating organizations are expected to find a difference in their requirements for participating in the program, due to this requirement change.

Table 2. Certification program changes SSA 2014.1 to SSA 2.0.0

Number	Add/Delete /Change	Description	References	System supplier	Chartered laboratory	CRT Tool supplier
56.	C	**17065:** Change from ISO/IEC Guide 65 compliance to ISO/IEC 17065 compliance for chartered laboratories. SSA-200 is restructured in accordance	SSA-100 SSA-200		X	

Number	Add/Delete /Change	Description	References	System supplier	Chartered laboratory	CRT Tool supplier
		with the new standard.				
57.	+	**Jitter:** Require submission of maximum jitter tolerance and at least 95% confidence level (as for EDSA)	SSA-310 SRT.R10	X	X	
58.	C	**Jitter:** Changed maximum permitted measurement jitter (as for EDSA)	SSA-310 SRT.R38		X	X
59.	+	**Jitter:** Added specification detail for determining excessive jitter (as for EDSA)	SSA-310 SRT.R38, text after NOTE 2	X	X	X
60.	+	**Test coverage:** add definition of operational mode and add requirements for testing in modes that support control	SSA-310 3.1.14 SSA-310 SRT.R45 SSA-310 SRT.R49	X	X	
61.	-	**Test coverage:** Asset discovery and CRT on perimeter firewall not required	SSA-300 6.3.5.4. Table 5 SSA-310 SRT.R49 SSA-303 Table 1, 9.4, 9.5	X	X	
62.	-	**Test coverage:** Downward essential functions do not need to be monitored for NST	SSA-310 SRT.R56, 13.3, 13.4		X	
63.	C	**Test coverage:** Clarify placement for test devices for CRT and NST	SSA-310 SRT.R49 SSA-310 SRT.R54		X	
64.	C	**Test coverage:** Changed treatment of redundant units for testing	SSA-310 4.1.1, removed sentences in subsections about redundant partner SSA-310 12.1, SRT.R48 reference to ERT.R37, and NOTE 1	X	X	
65.	C	**CB process:** Made reproducibility criterion the same for Asset Discovery Testing and VIT as for other test types	SSA-310 SRT.R41, SRT.R47		X	

Number	Add/Delete /Change	Description	References	System supplier	Chartered laboratory	CRT Tool supplier
66.	+	**CB process:** Added detail regarding submission of rate limiting information (as for EDSA)	SSA-310 SRT.R14	X	X	
67.	+	**CB process:** Clarifying note regarding submission of essential functions, converted to requirement	SSA-310 SRT.R7	X	X	
68.	C	**CB process:** SSA Credit for VIT done under EDSA certification	SSA-300 5.3 ISASecure_SY.R4 NOTE 2, 6.3.5.3 SSA-303 9.1 last paragraph SSA-310 SRT.R45	X	X	
69.	C	**CB process:** Clarify time when SDLA certification must be in place, to be referenced by SSA certification	SSA-300 5.3 ISASecure_SY.R4, NOTE 3	X	X	
70.	C	**CB process:** Changed definitions for adequately maintain alarms, history (as for EDSA) and external communication	SSA-310 4.1.1.5, 4.1.1.6, 4.1.1.7 SSA-310 SRT.R21	X	X	
71.	+	**CB process:** Clarified impartiality requirements for chartered laboratory, revising requirements previously found in [ASCI Lab] section III, and referenced from SSA-200. (as for EDSA)	SSA-200 6.3.3		X	
72.	C	**CB process:** No calibration is required for the CRT tool. (as for EDSA)	SSA-200 SSA.R28		X	
73.	C	**CB process:** GICSP certification added as option for professional certification. (as for EDSA)	SSA-200 6.4.3.1 Tables 4 and 6		X	
74.	+	**CB process:** Confirmation of full software version of CRT tool on reports is required (as for EDSA)	SSA-200 SSA.R19		X	X
75.	C, -	**CB process:** Process for determining equipment supplier applicant eligibility; clarifies responsibilities and escalation. Otherwise, I.C.8 in [ASCI Lab] does not	SSA-200 SSA.R15	X	X	

Number	Add/Delete /Change	Description	References	System supplier	Chartered laboratory	CRT Tool supplier
		apply and these requirements are deleted. (as for EDSA)				
76.	+	**CB process:** Requirement related to withdrawal of certification (as for EDSA)	SSA-200 SSA.R38	X	X	
77.	+	**Tool recognition:** support gateway address for testing through firewalls and routers, required for SSA but not EDSA	EDSA-102 5.2, erratum on EDSA-201			X
78.	C	**ASCI Lab:** Document *ASCI Chartered Testing Laboratory 2009 Approval Process*, no longer a reference for SSA-200; requirements directly incorporated into SSA-200, if not already covered by ISO/IEC 17025 (as for EDSA).	SSA-100 SSA-200		X	
79.	-	**ASCI Lab:** Specific requirements regarding calibration and estimated accuracy of results deemed not applicable, so no longer included in SSA-200, were [ASCI Lab] I.D.5, 6, 8 and IV.A.h (as for EDSA).	SSA-200		X	
80.	-	**ASCI Lab:** Employee safety program requirement deleted, so no longer included in SSA-200, was [ASCI Lab] I.G.6 (as for EDSA).	SSA-200		X	
81.	-	**ASCI Lab:** Follow-up and field inspection requirements not applicable, so no longer included in SSA-200, were [ASCI Lab] II.B.1-8, 9b,c,e (as for EDSA).	SSA-200		X	
82.	+	**Report content:** Revised material regarding FSA-E for consistency with specifications	SSA-303 Section 7.2		X	
83.	+	**Report content:** guidance regarding level of detail needed for system description version numbers	SSA-303 Section 6		X	
84.	+	**Report content:** regarding how to report SDLPA results performed under SSA, points to SDLA-303	SSA-303 Section 8.1		X	

Number	Add/Delete /Change	Description	References	System supplier	Chartered laboratory	CRT Tool supplier
85.	+	**Report content:** add results of IP protocol scan during Asset Discovery Test	SSA-303 9.4		X	
86.	+	**Report admin:** Add restriction on reproduction of report; use ISASecure certification body logo	SSA-303 title page		X	
87.	+	**Report admin:** Add dates of assessment	SSA-303 Management Summary SSA-303 Technical Summary		X	
88.	+	**Report admin:** Add address of chartered laboratory	SSA-303 5.1		X	
89.	+	**Report admin:** Report version of Asset Discovery Test tool	SSA-303 9.2.1		X	

6 Appendix 1: EDSA 2010.1 and EDSA 2.0.0 specification versions

The following specifications define the EDSA program, together with the most current errata documents SDLA-102 and SSA-102, posted on the ISCI website.

Table 3. EDSA 2010.1 and EDSA 2.0.0 specification versions

Document ID	Document Title	EDSA 2010.1 Version	EDSA 2.0.0 Version
EDSA-100	*ISA Security Compliance Institute – Embedded device Security Assurance – ISASecure Certification Scheme*	2.0	2.8
EDSA-102	*ISCI Embedded Device Security Assurance – Errata for EDSA specifications*	1.2	2.3 or later; most current version
EDSA-200	*ISCI Embedded device security assurance – ISASecure EDSA chartered laboratory operations and accreditation*	2.1	3.3
EDSA-201	*ISCI Embedded device security assurance –Recognition process for communication robustness testing tools*	1.21	2.1
EDSA-204	*ISCI Embedded device security assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*	2.0	2.1
EDSA-205	*ISCI Embedded Device Security Assurance – Certificate Document Format*	2.0	2.1
EDSA-206	*ISCI Embedded Device Security Assurance – ISASecure EDSA CRT laboratory operations and accreditation*		
EDSA-300	*ISCI Embedded Device Security Assurance – ISASecure Certification Requirements*	2.0	2.8
EDSA-301	*ISCI Embedded Device Security Assurance – Maintenance of ISASecure Certification*	1.0	2.1
EDSA-303	*ISASecure Embedded Device Security Assurance - Assessment report sample*	1.3	2.1
EDSA-310	*ISCI Embedded Device Security Assurance - Common requirements for communication robustness testing of IP based protocol implementations* (for EDSA 2010.1) Upon adding VIT to EDSA, title and scope changed to: *ISCI Embedded Device Security Assurance – Requirements for embedded device robustness testing* (for EDSA 2.0.0)	1.7	2.2

Document ID	Document Title	EDSA 2010.1 Version	EDSA 2.0.0 Version
EDSA-311	*ISCI Embedded Device Security Assurance – Functional security assessment*	1.4	1.4
EDSA-312	*ISCI Embedded Device Security Assurance - Software development security assessment* (for EDSA 2010.1) Due to development of SDLA-312 to be referenced by all certifications, title and scope have changed to: *ISCI Embedded Device Security Assurance – Security development artifacts for embedded devices* (for EDSA 2.0.0)	1.4	2.0
EDSA-401	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols*	2.01	2.01
EDSA-402	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4*	2.31	2.31
EDSA-403	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol*	1.31	1.6
EDSA-404	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol*	1.3	1.3
EDSA-405	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6*	2.6	2.6
EDSA-406	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6*	1.41	2.01
ISASecure-111	*ISCI ISASecure Certification Programs - Transition to ISO/IEC 17065*	1.1	1.1
SDLA-100	*ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme*	–	1.5
SDLA-312	*ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*	–	3.0
SSA-420	*ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*	–	2.6
	ASCI Chartered Testing Laboratory 2009 Approval Process	April 2009	–

7 Appendix 2: SSA 2014.1 and SSA 2.0.0 specification versions

The following specifications define the SSA program:

- specifications listed in Table 4
- EDSA specifications that are referenced by the SSA specifications. These are listed below. The EDSA 2010.1 versions of these documents shown in Table 3 are associated with SSA 2014.1. The EDSA 2.0.0 versions of these documents shown in Table 3 are associated with SSA 2.0.0.
    - EDSA-201
    - EDSA-206
    - EDSA-301
    - EDSA-310
    - EDSA-311
    - EDSA-401 through 406
- the most current errata documents EDSA-102 and SDLA-102 posted on the ISCI website.

Table 4. SSA 2014.1 and SSA 2.0.0 specification versions

Document ID	Document Title	SSA 2014.1 Version	SSA 2.0.0 Version
SSA-100	*ISA Security Compliance Institute – System device security assurance – ISASecure Certification Scheme*	1.5	1.7
SSA-102	*ISA Security Compliance Institute – System device security assurance – errata for SSA specifications*	-	1.2 or later; most current version
SSA-200	*ISCI System Security Assurance – ISASecure SSA Chartered laboratory operations and accreditation*	1.2	1.9
SSA-204	*ISCI System Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*	1.1	1.2
SSA-205	*ISCI System Security Assurance – Certificate Document Format*	1.1	1.2
SSA-300	*ISCI System Security Assurance – ISASecure certification requirements*	1.1	1.4
SSA-301	*ISCI System Security Assurance – Maintenance of ISASecure certification*	1.4	1.6
SSA-303	*ISASecure System Security Assurance - Assessment report sample*	1.3	2.0

Document ID	**Document Title**	**SSA 2014.1 Version**	**SSA 2.0.0 Version**
SSA-310	*ISCI System Security Assurance – Requirements for system robustness testing*	1.02	2.0
SSA-311	*ISCI System Security Assurance – Functional security assessment for systems*	1.82	1.82
SSA-312	*ISCI System Security Assurance – Security development artifacts for systems*	1.01	1.01
SSA-420	*ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*	2.4	2.6
SDLA-100	*ISCI Security Development Lifecycle Assurance – ISASecure Certification Scheme*	1.5	1.5
SDLA-312	*ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*	3.0	3.0
	ASCI Chartered Testing Laboratory 2009 Approval Process	April 2009	–

8 Appendix 3: EDSA-310 v2.3 to EDSA-310 v1.7 requirements mapping

Note that those EDSA-310 v2.3 requirements with no associated EDSA-201 v1.7 requirement, also have no associated CRT Tool requirements per EDSA-201 v2.1.

Table 5. EDSA 310 v2.3 to EDSA-310 v1.7 requirements mapping

EDSA-310 v2.3 Requirement Identifier	EDSA-310 v1.7 Requirement Identifier	Version 2.3 Requirement Name	
ERT.R1	CRT.R1	Types of CRT tests	
ERT.R2	CRT.R2	Applicable protocols for CRT	
ERT.R3	CRT.R3	Interface surface tests precedence	
ERT.R4	CRT.R4	Core protocol tests precedence	
ERT.R5		Types of ERT tests	
ERT.R6	CRT.R5	Criterion for ERT pass	
ERT.R7	CRT.R6	Single configuration DUT	
ERT.R8	CRT.R7	Submission of essential functions	
ERT.R9	CRT.R8	Submission of definition of essential history data	
ERT.R10	CRT.R9	Submission of upward essential function monitoring criteria	
ERT.R11	CRT.R10	Submission of method to achieve maximum recommended device load	
ERT.R12	CRT.R11	Submission of control jitter tolerance	
ERT.R13	CRT.R12	Submission of device hardware and software	
ERT.R14	CRT.R13	Submission of monitoring hardware and software for downward essential functions	
ERT.R15	CRT.R14	Submission of monitoring hardware and software for upward essential functions	
ERT.R16	CRT.R15	Submission of end user device documentation	
ERT.R17	CRT.R16	Submission of list of accessible network interfaces	
ERT.R18	CRT.R17	Submission of implemented protocols	
ERT.R19	CRT.R18	Submission of description of intended embedded device defensive behavior	
ERT.R20	CRT.R29	Basic interface surface test configuration	
ERT.R21	CRT.R30	Configuration for downward essential functions monitoring during interface surface test	
ERT.R22	CRT.R31	Configuration for firewalls during interface surface test	
ERT.R23	CRT.R32	UDP port scan	
ERT.R24	CRT.R33	TCP port scan	

EDSA-310 v2.3 Requirement Identifier	EDSA-310 v1.7 Requirement Identifier	Version 2.3 Requirement Name	
ERT.R25	CRT.R34	Use of DUT- based utilities for determining active ports	
ERT.R26	CRT.R35	IP protocol type scan	
ERT.R27	CRT.R36	Scan coverage of all accessible network interfaces and device modes	
ERT.R28	CRT.R37	High rate port and protocol scans	
ERT.R29	CRT.R38	Reproducibility of determination of ports that may be active	
ERT.R30	CRT.R39	Test criteria for “adequately maintain control capability”	
ERT.R31	CRT.R40	Test criteria for “adequately maintain upward essential functions”	
ERT.R32	CRT.R41	Criteria for “pass interface surface test”	
ERT.R33	CRT.R42	Reproducibility of interface surface test failure	
ERT.R34	CRT.R48	Test configuration 1 – switched IP connection from TD to DUT	
ERT.R35	CRT.R49	Test configuration 2 – non-switched IP connection from TD to DUT	
ERT.R36	CRT.R50	Robustness testing phases	
ERT.R37	CRT.R51	Test coverage for devices with redundant configurations	
ERT.R38	CRT.R52	Test coverage of field values	
ERT.R39	CRT.R55	Required test values used in testing fixed-length fields representing integers or enumerations	
ERT.R40	CRT.R56	Required test values used in testing determined-length fields containing varying-length self-delimiting strings	
ERT.R41	CRT.R57	Testing fields with a varying sequence of fixed-size subfields	
ERT.R42	CRT.R58	Testing fields with substructure and self-defining length	
ERT.R43	CRT.R59	Protocol-specific load testing	
ERT.R44	-	Criterion for protocol-specific CRT pass	
ERT.R45	CRT.R60	Criteria for single protocol specific robustness test pass	
ERT.R46	CRT.R61	Reproducibility of protocol-specific robustness test failure	

EDSA-310 v2.3 Requirement Identifier	EDSA-310 v1.7 Requirement Identifier	Version 2.3 Requirement Name	
ERT.R47	CRT.R62	Generation of reproducible robustness tests	
ERT.R48	CRT.R63	Pseudo-random seed value	
ERT.R49	CRT.R64	Pseudo random seed reuse	
ERT.R50	-	Vulnerability Identification Testing	
ERT.R51	-	Basic vulnerability identification test configuration	
ERT.R52	-	Configuration for downward essential functions monitoring during vulnerability identification test	
ERT.R53	-	Vulnerability identification test coverage of all accessible network interfaces	
ERT.R54	-	Criteria for “pass vulnerability identification test”	
ERT.R55	-	Reproducibility of vulnerability identification test failure	
ERT.R56	CRT.R19	CRT report summary	
ERT.R57	CRT.R20	Test report administrative information	
ERT.R58	CRT.R21	Report CRT test case descriptions	
ERT.R59	CRT.R22	Report CRT methodology summary	
ERT.R60	CRT.R23	Report CRT configuration	
ERT.R61	CRT.R24	Report ISASecure reference for test failure	
ERT.R62	CRT.R25	Report test failure analysis	
ERT.R63	CRT.R26	Report conditional branches of test execution	
ERT.R64	CRT.R27	Report test software version	
ERT.R65	CRT.R28	Report test identification and parameters for reproducibility	

EDSA-310 v2.3 Requirement Identifier	EDSA-310 v1.7 Requirement Identifier	Version 2.3 Requirement Name	
ERT.R66	CRT.R43	Report basic interface surface test information	
ERT.R67	CRT.R44	Report UDP ports that may be active	
ERT.R68	CRT.R45	Report TCP ports that may be active	
ERT.R69	CRT.R46	Report IP protocol types	
ERT.R70	CRT.R47	Report behavior of essential functions during scans	
ERT.R71	CRT.R65	Report basic protocol specific robustness test information	
ERT.R72	CRT.R66	Robustness results summary over all protocols	
ERT.R73	CRT.R67	Report robustness failures	
ERT.R74	CRT.R68	Report robustness failure conditions	
ERT.R75	CRT.R69	Report robustness test case results listing	
ERT.R76	-	Report basic vulnerability identification test information	
ERT.R77	-	Report vulnerability identification failures	
ERT.R78	-	Report accessible interface with identified vulnerability	