EDSA-102
ISA Security Compliance Institute – Embedded Device Security Assurance –
Errata for EDSA 2.0.0 Specifications

Version 3.4

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	2011.04.05	Initial version published to http://www.ISASecure.org
2.3	2015.04.22	Update to "Ethernet," ARP, ICMPv4 and UDP errata; remove SDSA, EDSA-310, TCP and IPv4 errata; 2 minutes for load test duration; EDSA-201 gateway address for SSA CRT; EDSA-201 information for user guide
2.5	2015.06.10	Require CRT for modes that permit control in EDSA-310; clarify definition of operational mode; clarify point in time for holding SDLA certification in EDSA-300; update version of 17025
2.6	2015.08.21	EDSA-100 typographical error SDA-S should be SDA-E
2.7	2016.02.15	Measurement jitter 1% to 2%, broaden spec for detection of transitions
3.1	2017.04.07	In EDSA-200, for auditors, add CACE and CACS as certifications and permit any bachelor-level degree with sufficient industry experience; modify wording in EDSA-201 for SSA support feature for CRT tools; EDSA-310 correct reference error; EDSA-403 correct protocol description, clarify IPv4.T12 test definition, and correct IPv4.T13 test procedure; EDSA-406 editorial correction to undefined reference
3.3	2018.03.19	EDSA-310, revise ERT.R37 redundancy testing requirement
3.4	2018.03.20	In EDSA-310: modify ERT.R9 regarding submission of definition of essential history data; modify 7.1.4.2.6 regarding definition of adequately maintain essential history data

Contents

FOREWORD

This is one of a series of documents that defines ISASecure® certification for embedded devices. The ISASecure Embedded Device Security Assurance (EDSA) 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 EDSA 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 EDSA 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 EDSA specifications is provided in the following highest level document.

[EDSA-100] *ISA Security Compliance Institute – Embedded device security assurance – ISASecure Certification Scheme,* as specified at http://www.ISASecure.org

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

[EDSA-100] *ISCI Embedded Device Security Assurance – ISASecure certification scheme,* as specified at http://www.ISASecure.org

[EDSA-200] *ISCI Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation,* as specified at http://www.ISASecure.org

[EDSA-201] *ISCI Embedded Device Security Assurance –Recognition process for communication robustness testing tools,* as specified at http://www.ISASecure.org

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

[EDSA-300] *ISCI Embedded Device Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

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

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

[EDSA-312] *ISA Security Compliance Institute Embedded Device Security Assurance – Security development artifacts for embedded devices*, as specified at http://www.ISASecure.org

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

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

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

[EDSA-405] *ISA Security Compliance Institute 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

The EDSA 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 EDSA.

[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

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 EDSA 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 EDSA Errata Index

Document ID	Document Title	Version	Errata	Reference in this document
EDSA-100	*ISA Security Compliance Institute – Embedded device security assurance – ISASecure Certification Scheme*	2.8	Yes	5.2
EDSA-200	*ISCI Embedded Device Security Assurance – ISASecure EDSA chartered laboratory operations and accreditation*	3.3	Yes	5.3
EDSA-201	*ISCI Embedded Device Security Assurance – Recognition process for communication robustness testing tools*	2.1	Yes	5.4
EDSA-204	*ISCI Embedded Device Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*	2.1	Yes	5.5

Document ID	Document Title	Version	Errata	Reference in this document
EDSA-205	*ISCI Embedded Device Security Assurance – Certificate Document Format*	2.1	No	
EDSA-300	*ISCI Embedded Device Security Assurance – ISASecure Certification Requirements*	2.8	Yes	5.6
EDSA-301	*ISCI Embedded Device Security Assurance – Maintenance of ISASecure Certification*	2.1	No	
EDSA-310	*ISCI Embedded Device Security Assurance – Requirements for embedded device robustness testing*	2.2	Yes	5.7
EDSA-311	*ISCI Embedded Device Security Assurance – Functional security assessment*	1.4	Yes	5.8
EDSA-312	*ISCI Embedded Device Security Assurance – Security development artifacts for embedded devices*	2.0	No	
EDSA-401	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of two common "Ethernet" protocols*	2.01	Yes	5.9
EDSA-402	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ARP protocol over IPv4*	2.31	Yes	5.10
EDSA-403	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF IPv4 network protocol*	1.6	Yes	5.11
EDSA-404	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF ICMPv4 network protocol*	1.3	Yes	5.12
EDSA-405	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF UDP transport protocol over IPv4 or IPv6*	2.6	Yes	5.13
EDSA-406	*ISCI Embedded Device Security Assurance – Testing the robustness of implementations of the IETF TCP transport protocol over IPv4 or IPv6*	2.01	Yes	5.14

5 Errata by document

5.1 General

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

5.2 EDSA-100 Certification scheme

The follow erratum applies to EDSA-100 version 2.8.

- **Update reference**: In 2.4.2, change the date on reference [ISO/IEC 17025] to 15 May 2005.
- **Typographical error:** In 4.1, third paragraph, change SDA-S to SDA-E.

5.3 EDSA-200 Chartered laboratory

The follow errata apply to EDSA-200 version 3.3.

- **Update reference**: In 2.2, change the date on reference [ISO/IEC 17025] to 15 May 2005.
- **Update abbreviations:** In 3.2, add the following entries to the table:
  - CACE, an abbreviation for Certified Automation Cyber Security Expert
  - CACS, an abbreviation for Certified Automation Cyber Security Specialist
- **Accept CACE and CACS professional certifications:**
  - In 6.4.3.1, Requirement EDSA.R10, Table 4 - FSA-E and SDA-E and SDLPA auditor qualifications, replace the row for Professional certification to add 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 EDSA.R12, Table 4 - 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 bachelors degree:** In 6.4.3.1, Requirement EDSA.R10, Table 4 - FSA-E and SDA-E 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 in other subject, if individual has sufficient experience in computer technology field as specified below	• 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 in other subject, if individual has sufficient experience in computer technology field as specified below

Work experience in field	• Minimum four years of post-degree experience in computer technology field, if individual has degree in one of the specific subjects identified above, or has an equivalent science or engineering degree • Minimum eight years of post-degree experience in computer technology field, if individual has a bachelors or equivalent level degree in other subject	• Minimum four years of post-degree experience in computer technology field, if individual has degree in one of the specific subjects identified above, or has an equivalent science or engineering degree • Minimum eight years of post-degree experience in computer technology field, if individual has a bachelors or equivalent level degree in other subject

5.4 EDSA-201 Tool recognition

The following errata apply to the specification EDSA-201 version 2.1.

- **User documentation requirements:** In Table 3, revise the column "Guidelines for Demonstration by Tool Supplier" as follows:
    - ERT.R14, replace "Provide pointers to user or design documentation" by "Provide pointers to user documentation (which may be augmented by design documentation)"
    - ERT.R21, replace "Show how this functionality can be used" by "Show in the user documentation how this functionality can be used"
    - ERT.R30, replace "describe the measurement accuracy" by " describe the measurement accuracy in user documentation"
    - EDSA.R57, replace "Show" in both sentences, by "Show and describe in the user documentation"
    - ERT.R60, replace "Show that" by " Show and describe in the user documentation, how"
    - ERT.R61, replace "Show" by " Show and describe in the user documentation"
    - ERT.R64, replace "Show that" by "Show and describe in the user documentation how"
    - ERT.R65, replace "Show that" by "Show and describe in the user documentation how"
    - ERT.R73, replace "Show that" by "Show and describe in the user documentation how"
    - ERT.R74, replace "Show that" by "Show and describe in the user documentation how"
    - ERT.R75, replace "Describe" by "Describe in the user documentation"
- **Distinguish EDSA vs. SSA CRT tool recognition:** Add the following paragraph at the end of Section 3.2:

  "A tool feature to allow testing through devices that route, is required for System Robustness Testing (SRT), which is an element of ISASecure SSA certification, as described in Section 5.4 below. A CRT tool that has this feature is recognized for EDSA and SSA; a tool that does not have this feature is recognized for EDSA. The scope for tool recognition will be included in the ISCI web site posting for a recognized tool."

- **SSA CRT tool recognition requirements:** Add the following section to the end of the document:

  "**Section 5.4 Evidence for Compliance with SSA SRT requirements**

  There is one unique tool requirement in support of SSA certification, in addition to the EDSA tool requirements. The table below describes evidence required for tool compliance with this requirement. The last column shows the step of the tool evaluation for which this information is needed. (A tool may be recognized for EDSA, or for both EDSA and SSA, as described in 3.2.)

Table 5 - Evidence for CRT tool compliance with SSA requirements

Requirement Identifier	Requirement Name	Guidelines for Demonstration by Tool Supplier	Step
SSA-310 SRT.R49	Communication robustness testing precedence	Provide a pointer to user documentation that shows how the tool supports testing through devices that route such as firewalls and routers.	1

"

5.5 EDSA-204 Symbols and certificates

The follow erratum applies to EDSA-204 version 2.1.

- **Update reference:** Clause 2, change the date on reference [ISO/IEC 17025] to 15 May 2005.

5.6 EDSA-300 Requirements for certification

The following erratum applies to the specification EDSA-300 version 2.8.

- **Clarify time for holding SDLA certification:** At the end of the first sentence in the requirement column of the table in 5.2, Requirement ISASecure_ED.R5, add the text " at the time of issuance of the EDSA certificate."

5.7 EDSA-310 Requirements for embedded device robustness testing

The following errata apply to the specification EDSA-310 version 2.2.

- **Correct document reference:** In 1.3, replace EDSA-420 by SSA-420.
- **Clarify definition of operational mode:** In 3.1.12, 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 how essential history data may be specified:** In 6.3, replace requirement ERT.R9 by: "A certification applicant that considers maintaining process history an essential function and does not exclude this per Requirement ERT.R8 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."
- **Clarify definition of adequately maintain essential history reporting:** In 7.1.4.2.6, replace the following text "Essential history data is not lost during continuous 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 never reported by the embedded device. 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 7.1.4.2.6, add the following note: "NOTE 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."

- **Require CRT in operational modes that support control:** At the end of the first sentence of the requirement in 7.2.4, ERT.R44, add the text "in all operational modes of the device in which the control function is available."

- **Permit alternative method of transition detection:** In section 7.1.4.3, requirement ERT.R30, 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."

- **Clarify testing requirement for redundant units:** In section 7.2.3.1, requirement ERT.R37, add text (shown here in italics) to the following clause "testing SHALL be applied to the device when one or more of the redundant units are not operational" so that it reads "testing SHALL be applied to the device when *all redundant units are operational and when* one or more of the redundant units are not operational."

- **Change limit on measurement jitter:** In section 7.1.4.3, requirement ERT.R30, 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.

5.8 EDSA-311 Functional Security Assessment

The following erratum applies to the specification EDSA-311 version 1.4.

- **Modify requirement for disabling non-access-controlled services:** In the Comments/Clarifications column of FSA-AC-2.1.11, add the words "able to be" so that the text now reads: "All services should either be secured by access control or *able to be* disabled for normal operation (services that must be disabled also need to be documented for the user)."

5.9 EDSA-401 "Ethernet"

The following errata apply to the specification EDSA-401 version 2.01.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: "Requirements are comprised of all the numbered Requirements in this document

and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence."

- **Update referenced document title:** Clause 2, the title for reference [EDSA-310] is changed from *"Common requirements for communication robustness testing of IP-based protocol implementations"* to "*Requirements for embedded device robustness testing"*

- **Update terminology:** All instances of the term "essential service" are changed to "essential function" and the symbolic tag [CRT.Essential_services] in this document is replaced by [CRT.Essential_functions]. (Symbolic tags are described as a note to the reference [EDSA-310] in Clause 2 of documents that use these tags.)

- **Correct protocol description:** Figure 1 – IEEE 802.3 frame structure with IEEE 802.2 Type 1 and IEEE 802 SNAP states that the SNAP header should start with 0xAA0003. This is not correct. It should start with 0xXX 0xYY 0x03, where 0xXX and 0xYY are in {0xAA, 0xAB}.

- **Correct protocol description**: Subclause 4.3, M4, modify the text "(0xFF FF FF FF FF FF) is classified as a group address even though its first bit is zero" to read "(0xFF FF FF FF FF FF) is classified as globally unique even though its second bit is a one."

- **Clarify terminology**: Clarify the meaning of the term "load" in the following instances:

    - Subclause 6.2 a), replace "low load" by "low network communications load"

    - Subclause 6.2 Note 4, replace "receiver load" by "receiver network communications load"

    - Clause 7 Table 1, last column heading, replace "Maximum load" by "Maximum network communications load"

- **Correct required protocols for testing:** Replace the paragraph in subclause 6.3.2 by: "ARP is used to test that the DUT is receiving and can generate Ethernet frames, in particular ARP request/ARP reply."

- **Clarify requirement intent:** Add a sentence as a third paragraph of subclause 6.6.2, Requirement "Ethernet".R5, "During basic robustness testing, lower level PDUs employed to convey a protocol under test SHALL be valid."

- **Increase duration of tests:** Subclause 6.7.2, Requirement "Ethernet".R10, replace "at least tens of seconds" by "two minutes."

- **Require pseudo random test generation**: Subclause 6.7.2, Requirement "Ethernet".R11, in both paragraphs, replace text enclosed in parentheses by " (which SHALL be a seeded pseudo-random process where applicable)."

- **Clarify pass/fail criteria:** Clause 7, Requirement "Ethernet".R14, append sentence as follows. "Tests where *Results* are indicated as Pass or Fail, SHALL pass if the indicated *Expected response* is observed."

- **Broaden test description:** Clause 7, Table 2 - "Ethernet".T00, in the Test description row, after "The basic operational aspects of the protocol under test", add the text "and of any inferior or selected superior supporting protocols used in the testing."

- **Correct test name:** Clause 7**,** Table 7 - "Ethernet".T05, replace the test name "IEEE 802 multicast destination address tolerance" by "IEEE 802 unicast destination address tolerance."

- **Correct test name:** Clause 7**,** Table 8 - "Ethernet".T06 replace the test name "IEEE 802 multicast destination address tolerance" by "IEEE 802 broadcast destination address tolerance."

- **Remove ramp down requirement on high load test procedure:** Clause 7, Table 10 – “Ethernet”.T08: Maintenance of service under high load, including network saturation: Raw DPDU flood, in the Test procedure row, states that the TD “then gradually reduces its sending rate to zero.” This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

- **Increase test duration:** Clause 7, Table 10 – "Ethernet".T08: Maintenance of service under high load, including network saturation: Raw DPDU flood, in the Test procedure row, replace "a few seconds" by "two minutes."

- **Add test:** In Clause 7, add test as follows:

Table 11 – “Ethernet”.T09: Inconsistent frame length

Test ID	“Ethernet”.T09
Test name	Inconsistent frame length
Test description	“Ethernet” frames with pad length field values inconsistent with the actual frame lengths are sent to the DUT to evaluate the DUT’s ability to withstand receipt of such frames
Reference requirements	6.6.3, Requirement "Ethernet".R5, considering permitted lengths per 6.6.3c
Test type	Basic robustness
Test status	Mandatory
Expected DUT behavior	The DUT SHALL protect itself against receipt of “Ethernet” frames with incorrect values in the pad length field.
Test object	To probe the robustness of the DUT’s ability to withstand receipt of “Ethernet” frames with actual length inconsistent with the value in the pad length field.
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2].
Test procedure	The TD sends otherwise-valid “Ethernet” frames addressed to the DUT, but with actual frame length larger or smaller than the value indicated by the pad length field of the frame.
Expected response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	This test applies to Ethernet 802.3 only, since Ethernet II does not have a field that indicates length of the frame.

5.10 EDSA-402 ARP

The following errata apply to the specification EDSA-402 version 2.31.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: “Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence.”

- **Update referenced document title:** Clause 2, the title for reference [EDSA-310] is changed from *"Common requirements for communication robustness testing of IP-based protocol implementations"* to "*Requirements for embedded device robustness testing"*

- **Update terminology:** All instances of the term "essential service" are changed to "essential function" and the symbolic tag [CRT.Essential_services] in this document is replaced by [CRT.Essential_functions]. (Symbolic tags are described as a note to the reference [EDSA-310] in Clause 2 of documents that use these tags.)

- **Clarify terminology**: Clarify the meaning of the term "load" in the following instances:

    - Subclause 6.2 a), replace "low load" by "low network communications load"

- Subclause 6.2 Note 3, replace "receiver load" by "receiver network communications load"
- Clause 7 Table 1, last column heading, replace "Maximum load" by "Maximum network communications load"

- **Clarify requirement intent:** Add a sentence as a third paragraph of subclause 6.6.3, Requirement ARP.R6, "During basic robustness testing, lower level PDUs employed to convey a protocol under test SHALL be valid."
- **Increase test duration:** Subclause 6.7.2, Requirement ARP.R10, replace "at least tens of seconds" by "two minutes."
- **Require pseudo random test generation**: Subclause 6.7.2, Requirement ARP.R11, in both paragraphs, replace text enclosed in parentheses by " (which SHALL be a seeded pseudo-random process where applicable)."
- **Clarify pass/fail criteria:** Clause 7, Requirement ARP.R14, append sentence as follows. "Tests where *Results* are indicated as Pass or Fail, SHALL pass if the indicated *Expected DUT response* is observed."
- **Clarify meaning of Results row:** Clause 7**,** insert this sentence before Table 2: “If the Results row in a table does not indicate “Pass/Fail,” this means that the test provides security-relevant information about the DUT to be included in the test report, but cannot cause a device to fail certification as long as related documentation of compensating controls is provided by the vendor as indicated.”
- **Typographical error:** Clause 7, Table 2 – ARP.T01: DUT cache poisoning, in the Test description and the Test procedure rows, the first instance of “ARP request DPDUs” is changed to correctly read “ARP reply DPDUs.”
- **Clarify terminology:** Clause 7, Table 3 - ARP.T01: DUT cache poisoning, Test description field, change the terms "churn" and "churning" to "repeatedly update" and "attempt to repeatedly update."
- **Clarify test intent:** Clause 7, Table 4 - ARP.T02, Truncated DPDU, replace existing fields in the table with the following text shown in italics. These changes are not intended to modify the test, but rather to describe it more accurately.

Table 4 – ARP.T02: Truncated DPDU

Test ID	ARP.T02
Test name	Truncated DPDU
Test description	*An ARP DPDU is sent as an "Ethernet" MAC frame payload, where the payload is a properly formed ARP DPDU that has been deliberately truncated to be less than (HLN+PLN)×2+8 octets in length, but where the "Ethernet" MAC FCS is correct for the truncated DPDU as conveyed in the Ethernet frame*
Reference requirements	Requirement ARP.R6, violating 4.3, M5 or M6
Test type	Basic robustness: PDU structural violations
Test status	Mandatory
Expected DUT behavior	*The DUT checks the ARP DPDU's specified length before checksum validation and determines that the last portion of the DPDU is absent from the conveying Ethernet frame*
Test object	To evaluate the DUT's consistency checks and processing order for received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	*The TD sends an invalid ARP DPDU such that the ARP DPDU length is less than 28 octets but the conveying "Ethernet" MAC frame payload is a valid ARP DPDU (except for its premature truncation). If possible, the ARP DPDU is chosen so that ARP DPDU acceptance will lead to incorrect ARP processing on DPDU receipt. The TD MAY monitor for any response from the DUT*
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	*If the DUT fails to validate that the conveying Ethernet frame contains a complete ARP DPDU, so that the length of the ARP DPDU = 28 octets, then the "Ethernet" MAC FCS may be incorrectly interpreted as part of the ARP DPDU's TPA field. If this corrupt target protocol address is inserted into the DUT ARP translation cache, it will become an unused entry and will subsequently be flushed by the DUT's validation mechanism for out-of-date ARP information. However, the desired entry (of the correct target protocol address) will not be made, resulting in the TD needing to generate a retry of the ARP request to elicit an ARP reply from the DUT*

- **Clarify test intent**: Clause 7, Table 6 - ARP.T04, Excessive DPDU length, replace existing fields in the table with the following text shown in italics. These changes is not intended to modify the test, but rather to describe it more accurately.

Table 6 – ARP.T04: Excessive DPDU length

Test ID	ARP.T04
Test name	Excessive DPDU length
Test description	*An ARP DPDU is sent whose length is extended beyond the expected (HLN+PLN)×2+8 octets by having the length indicated by the conveying "Ethernet" MAC frame be greater than that required to convey the ARP DPDU. (In other words, there are extra octets after the ARP DPDU within the conveying Ethernet frame.)*
Reference requirements	Requirement ARP.R6, violating 4.3, M5 or M6
Test type	Basic robustness: content semantic violations
Test status	Mandatory
Expected DUT behavior	The DUT uses the ARP DPDU's specified length rather than the size of the conveying "Ethernet" MAC frame
Test object	To evaluate the DUT's consistency checks for received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	*The TD sends a valid ARP DPDU, where the conveying "Ethernet" MAC frame length field value is greater than that required for the ARP DPDU, so that DPDU acceptance may lead to incorrect ARP DPDU length processing on DPDU receipt. The TD MAY monitor for any response from the DUT*
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	*This test MAY expose whether "Ethernet" MAC payload length or the ARP DPDU's specified length is being used by the DUT to determine the length of the received ARP DPDU, and whether the TD properly discards any unanticipated extra octets*

- **Clarify test intent:** Clause 7, Table 8 - ARP.T06, Incorrect specified lengths for address fields, in the Test procedure field, add the text "This SHALL be performed for various invalid values of both the HLN and PLN fields separately, and MAY be performed with both invalid."

- **Correct requirement cross reference:** Clause 7, Table 9 - ARP.T07: in the Reference requirements field, delete the text ", and d)".

- **Correct requirement cross reference:** Clause 7, Table 10 - ARP.T08: in the Reference requirements field, delete the text ", and d)".

- **Remove ramp down requirement on high load test procedure:** Clause 7, Table 12 – ARP.T10: Maintenance of service under high load, including network saturation, in the Test procedure row, states that the TD "then gradually reduces its sending rate to zero." This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

- **Increase test duration:** Clause 7, Table 12 – ARP.T10: Maintenance of service under high load, including network saturation, in the Test procedure row, replace "a few seconds" by "two minutes."

- **Add requirement cross reference:** Clause 7, Table 12 - ARP.T10, in the Reference requirements field of the table, add ARP.R10.

- **Add test:** In Clause 7, add test as follows:

Table 13 – ARP.T11: Invalid hardware or protocol type

Test ID	ARP.T11
Test name	Invalid hardware or protocol type
Test description	Correctly formed ARP DPDUs are sent with invalid hardware or protocol type values
Reference requirements	Requirement ARP.R6, violating 4.3, M2
Test type	Basic robustness: content semantic violations
Test status	Mandatory
Expected DUT behavior	The DUT validates the ARP DPDU hardware type (HRD) and protocol type (PRO) fields on receipt and performs per requirement M2
Test object	To evaluate the DUT's semantic processing of received ARP DPDUs
Test configuration	A TD is connected to the DUT by an underlying non-switched network that uses IEEE 802 and IP addressing, as specified in [CRT.Test_configuration_2]
Test procedure	The TD sends a properly formed ARP DPDU to the DUT containing an invalid hardware type and/or protocol value. The TD MAY monitor for any response from the DUT. This SHALL be performed for various invalid values of both the HRD and PRO fields separately, and MAY be performed with both fields invalid.
Expected DUT response	The DUT continues to adequately maintain essential services
Results	Pass or fail
Remarks	This test MAY expose failures to ignore invalid hardware and protocol types.

5.11 EDSA-403 IPv4

The following errata apply to the specification EDSA-403 version 1.6.

- **Correct protocol description:** In 4.2.5:
    - Replace " RR =0b1000 0111" by "RR=0b0000 0111."
    - Replace the table before Note 3 with the following table:

```
LSRR   +--------+--------+--------+---------//--------+
SSRR   |0000XYZ1| length | offset |     routeData     |
  RR   +--------+--------+--------+---------//--------+
       |   1B   |   1B   |   1B   |        4n B       |
```

- **Clarify test description and procedure:** In Table 20 for test IPv4.T12:
    - In the test description, replace the clause **"**The TD sends a large fragmented ICMP echo NPDU of 65,535 bytes or larger" by "The TD sends large fragmented ICMP echo NPDUs of 65,535 bytes and larger"
    - In the test procedure, replace the word "or" by the word "and " in the sentence "The TD sends several, large fragmented ICMP echo request NPDUs of 65,535 bytes or larger in size,"
- **Correct test procedure:** In Table 21 for test IPv4.T13, change the last sentence to: **"**Test sequences include those described in 6.7.3 b)."

5.12 EDSA-404 ICMPv4

The following errata apply to the specification EDSA-404 version 1.3.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: “Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence.”

- **Update referenced document title:** Clause 2, the title for reference [EDSA-310] is changed from *"Common requirements for communication robustness testing of IP-based protocol implementations"* to "*Requirements for embedded device robustness testing"*

- **Update terminology:** All instances of the term "essential service" are changed to "essential function" and the symbolic tag [CRT.Essential_services] in this document is replaced by [CRT.Essential_functions]. (Symbolic tags are described as a note to the reference [EDSA-310] in Clause 2 of documents that use these tags.)

- **Clarify terminology**: Clarify the meaning of the term "load" in the following instances:

    - Subclause 6.2 a), replace "low load" by "low network communications load"

    - Clause 7 Table 5, last column heading, replace "Maximum load" by "Maximum network communications load"

- **Delete duplicate information:** Subclause 6.6.2.1, Requirement ICMPv4.R5, delete the last paragraph, as this is duplicated in Requirement ICMPv4.R8.

- **Correct typographical error:** Subclause 6.6.2.1, in the title of Requirement ICMPv4.R8, replace "inappropriate" by "appropriate."

- **Clarify requirement intent:** Add a sentence as a third paragraph of subclause 6.6.3, Requirement ICMPv4.R9, "During basic robustness testing, lower level PDUs employed to convey a protocol under test SHALL be valid."

- **Increase test duration:** Subclause 6.7.2, Requirement ICMPv4.R13, replace "at least tens of seconds" by "two minutes."

- **Require pseudo random test generation**: Subclause 6.7.2, Requirement ICMPv4.R14, in both paragraphs, replace text enclosed in parentheses by " (which SHALL be a seeded pseudo-random process where applicable)."

- **Clarify pass/fail criteria:** Clause 7, Requirement ICMP.R17, append sentence as follows. "Tests where *Results* are indicated as Pass or Fail, SHALL pass if the indicated *Expected DUT response* is observed."

- **Add missing detail to test description**: Clause 7, Table 8 - ICMPv4.T02, in Test procedure, replace text in parentheses that currently reads "or where a variable size structure," with "or where a conveyed variable-size structure within the PDU is intentionally malformed as to length or contents."

- **Add requirement cross references:** Clause 7, in the Reference requirements fields of the following tables, add requirement references as follows:

    - Table 10 - ICMPv4.T04: in the Reference requirements field of the table, add ICMPv4.R8.

    - Table 14 - ICMPv4.T08: in the Reference requirements field of the table, add ICMPv4.R13.

- **Remove ramp down requirement on high load test procedure:** Clause 7, Table 14 – ICMPv4.T08: Maintenance of service under high load, including network saturation: Raw ICMPv4 NPDU flood**,** in the Test procedure row, states that the TD “then gradually reduces its sending rate to zero.” This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

- **Increase test duration:** Clause 7, Table 14 – ICMPv4.T08: Maintenance of service under high load, including network saturation: Raw ICMPv4 NPDU flood, in the Test procedure row, replace "a few seconds" by "two minutes."

5.13 EDSA-405 UDP

The following errata apply to the specification EDSA-405 version 2.6.

- **Clarify requirement sources and precedence:** The following statement is inserted before the notes in Clause 1, Scope: “Requirements are comprised of all the numbered Requirements in this document and any immediately following clarifying information, together with the tables in Clause 7 that describe individual tests. In the event of a conflict between these, the tables in Clause 7 take precedence.”

- **Update referenced document title:** Clause 2, the title for reference [EDSA-310] is changed from *"Common requirements for communication robustness testing of IP-based protocol implementations"* to "*Requirements for embedded device robustness testing"*

- **Update terminology:** All instances of the term "essential service" are changed to "essential function" and the symbolic tag [CRT.Essential_services] in this document is replaced by [CRT.Essential_functions]. (Symbolic tags are described as a note to the reference [EDSA-310] in Clause 2 of documents that use these tags.)

- **Clarify terminology**: Clarify the meaning of the term "load" in the following instances:

    - Subclause 6.2 a), replace "low load" by "low network communications load"

    - Subclause 6.2, Note after c), replace "receiver load" by "receiver network communications load"

    - Clause 7 Table 1, last column heading, replace "Maximum load" by "Maximum network communications load."

- **Correct acronym expansion:** Subclause 3.2, Abbreviations, states that the acronym TPDU is short for “transmission-layer PDU.” This is not correct. The correct expanded form is “transport-layer PDU,” as in ISO/IEC 7498-1, *OSI Basic Reference Model*.

- **Clarify requirement intent:** Add a sentence as a third paragraph of subclause 6.6.2, Requirement UDP.R5, "During basic robustness testing, lower level PDUs employed to convey a protocol under test SHALL be valid."

- **Increase test duration:** Subclause 6.7.2, Requirement UDPv4.R9, replace "at least tens of seconds" by "two minutes."

- **Require pseudo random test generation**: Subclause 6.7.2, Requirement UDP.R10, in both paragraphs, replace text enclosed in parentheses by " (which SHALL be a seeded pseudo-random process where applicable)."

- **Clarify pass/fail criteria:** Clause 7, Requirement UDP.R13, append sentence as follows. "Tests where *Results* are indicated as Pass or Fail, SHALL pass if the indicated *Expected DUT response* is observed."

- **Expand scope of test:** Clause 7, Table 9 - UDP.T07: Rejection of UDP TPDUs addressed to reserved destination ports, replace all instances of the text "reserved" in this table, to "Reserved or Unassigned." Thus in particular the title of the test is changed due to this modification.

- **Add requirement cross reference:** Clause 7, Table 11 - UDP.T09, in the Reference requirements field of the table, add UDP.R9.

- **Remove ramp down requirement on high load test procedure:** Clause 7, Table 11 – UDP.T09: Maintenance of service under high load, including network saturation: Raw TPDU flood, in the Test

procedure row, states that the TD “then gradually reduces its sending rate to zero.” This ramp-down portion of the test procedure in quotes is not required and is deleted from the specification.

- **Increase test duration:** Clause 7, Table 11 – UDP.T09: Maintenance of service under high load, including network saturation: Raw TPDU flood, in the Test procedure row, replace "a few seconds" by "two minutes."

5.14 EDSA-406 TCP

The following erratum applies to the specification EDSA-406 version 2.01.

- **Correct undefined reference:** Sub clause 4.2.3, undefined reference under Figure 2 should read "Figure 3."

— — — — — —