CSA-102
ISA Security Compliance Institute – Component Security Assurance –

Baseline document versions and errata for CSA 1.0.0 specifications

Version 2.2

May 2022

Copyright © 2018-2022 ASCI – Automation Standards Compliance Institute, All rights reserved

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, information, 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.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute’s copyright and other proprietary rights.

Revision history

version	date	changes
1.1	2019.12.14	Initial version published to https://www.ISASecure.org
1.2	2020.07.17	Add erratum for CSA-311 FSA-CR 2.1
1.3	2020.09.11	Add erratum for CSA-311 FSA-CR 2.9 RE(1)
1.6	2021.03.07	Add errata for CSA-311 CCSC 3, FSA-CR 2.1 RE(3), and FSA-CR 2.1 RE(4); For SDLA-312 v5.5, consider accessible points of entry in threat model
1.9	2021.10.26	Modify existing errata for CSA-311 CSSC 3 and FSA-CR 2.1; add erratum for CSA-311 FSA-CR 2.1 RE(1); change Table 1 baseline version of CSA-200 to v4.8
1.10	2022.02.11	Add errata for CSA-311 FSA-CR 2.7 and FSA-CR 3.8 to clarify meaning of “session”
2.2	2022.05.27	Change baseline version of SDLA-312 to v5.7 and reference errata as issued on that document; correct typo in CSA-311 requirement ID FSA-EDR 2.4B; add erratum for CSA-311 CR 1.2 to verify incoming as well as outgoing authentication capability

Contents

FOREWORD

This is one of a series of documents that defines the ISASecure® CSA (Component Security Assurance) certification program for software applications, embedded devices, host devices, and network devices. These are the component types defined by the standard IEC 62443-4-2, that are used to build control systems. ISASecure CSA is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). A description of the program and the current list of documents related to ISASecure CSA, as well as other ISASecure certification programs, can be found on the web site https://www.ISASecure.org.

1 Scope

This document lists baseline versions and all approved changes to all ISASecure CSA 1.0.0 specifications published at https://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 CSA 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

Errata in the following CSA specifications are listed in the subsequent clauses of the present document.

[CSA-100] is the highest level document for CSA 1.0.0 and describes all normative references for that certification program.

[CSA-100] *ISA Security Compliance Institute – Component security assurance – ISASecure certification scheme,* as specified at https://www.ISASecure.org

[CSA-300] *ISCI Component Security Assurance – ISASecure certification requirements,* as specified at https://www.ISASecure.org

[CSA-311] *ISCI Component Security Assurance – Functional security assessment for components, as specified at https://www.ISASecure.org*

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

Errata on [SDLA-312] are provided separately in the following document.

[SDLA-102] *ISCI Security Development Lifecycle Assurance – Baseline document versions and errata for SDLA 3.0.0 Specifications*, as specified at https://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 Baseline document versions and index to errata

This clause lists all ISASecure CSA 1.0.0 baseline documents that may be the subject of errata, and indicates for each document whether errata in the present document apply to the document. If so, the table below provides the sub clause reference in the present document that lists specific modifications for these errata. Note that errata on [SDLA-312] may affect CSA and are published separately in [SDLA-102].

Table 1 - ISASecure CSA Baseline and Errata Index

Document ID	Document Title	Baseline Version	Errata	Reference in this document
CSA-100	*ISCI Component Security Assurance - ISASecure certification scheme*	4.3	Yes	5.2
CSA-200	*ISCI Component Security Assurance – ISASecure CSA chartered laboratory operations and accreditation*	4.8	No	
CSA-204/205	*ISCI Component Security Assurance – Instructions and Policies for Use of the ISASecure® Symbol and Certificate (205 is editable certificate template)*	3.3	No	
CSA-300	*ISCI Component Security Assurance – ISASecure certification requirements*	4.2	Yes	5.3
CSA-301	*ISCI Component Security Assurance – Maintenance of ISASecure certification*	3.2	No	
CSA-311	*ISCI Component Security Assurance – Functional security assessment for components*	1.11	Yes	5.4
CSA-312	*ISCI Component Security Assurance – Security development artifacts for components*	3.2	No	
SSA-420	*ISCI System Security Assurance – Vulnerability Identification Testing Specification*	3.2	No	
SDLA-312	*ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*	5.7	No	

5 Errata by document

5.1 General

This clause lists all errata that apply to the documents indicated in Table 1 of the present document.

5.2 CSA-100 ISASecure certification scheme

The following errata apply to CSA-100 version 4.3.

- **Add reference to CSA-102:** In clause 2, add the sentence “A list of baseline document version numbers and errata on the baseline documents is published in [CSA-102].” In 2.3.1, after [CSA-303], add the reference “[CSA-102] *ISCI Component Security Assurance – Baseline document versions and errata for CSA 1.0.0 specifications*, as specified at https://www.ISASecure.org.”

- **Note that CSA-102 is not in Figure 1:** In 4.5.1, note 2, add text as in italics to the note:

  "The figure depicts all documents in Section 2 with the exception of *the baseline/errata document [CSA-102],* the application form [ISASecure-202], the editable certificate template [CSA-205], and the policy document [ISASecure-117] which describes the transition from the prior ISASecure EDSA program to CSA."

5.3 CSA-300 ISASecure certification requirements

The following erratum applies to the specification CSA-300 version 4.2.

- **Certifier carries out VIT:** In Table 1, in the row for VIT-C, replace existing text in the requirement column "The system passes VIT-C, per the pass/fail criteria for capability security level *n,*" with the text "The certifier carries out and the component passes VIT-C, per the pass/fail criteria for capability security level *n*."

5.4 CSA-311 Functional security assessment for components

The following errata apply to the specification CSA-311 version 1.11.

- **Correct typographical error in Requirement ID for FSA-EDR 2.4B:** Change the requirement ID currently shown as "FSA-EDR 2.4.B" to remove the second period so that it reads "FSA-EDR 2.4B".

The following erratum for CCSC 3 incorporates a previous erratum for this requirement in CSA-102 v1.6. That previous erratum improved the wording of the third sentence of the validation activity to be consistent with the standard.

- **Clarify wording and case of external privilege mapping for CCSC 3:** Replace the validation activity for requirement CCSC 3 regarding least privilege, with the text:

  "The SDLPA certification element under requirement SDLA-SG-6 in document SDLA-312, requires information about user account permissions and privileges required to use the product. If the evaluation for SDLA-SG-6 has passed, verify that the supplier has performed and documented an analysis of tasks related to the component. Verify that this analysis shows the permissions provided and mapping capability of permissions to roles support sufficient granularity and flexibility to enforce the concept of least privilege assignment of tasks to users. If requirement CR 2.1 has been met with dependence on external countermeasures, then permission assignment and mapping for human users may take place external to the component using compensating system or component countermeasures and/or procedures documented in the supplier's security guidelines for the component. Examples of external assignment of privileges are: provide a privileged account to use an external configuration tool, or provide an individual with a physical key to an enclosure protecting user access to such a tool. Reliance upon external countermeasures that are not integrated with the system, as in this last example, is permitted for SL-C = 1 only. Record one of:

  a. Met by component (without external countermeasures)
  b. Met with dependence on external countermeasures (CR 2.1 must also be met with dependence on external countermeasures for this option to be chosen)
  c. Not met

  If the evaluation for SDLA-SG-6 has not passed, record:
  c. Not met"

- **Verify incoming authentication capability in addition to outgoing, for FSA-CR 1.2**: Replace the validation activity for FSA-CR 1.2 with the text in quotes below.

  This erratum is in accordance with the ISCI understanding that the intent of IEC 62443-4-2 CR 1.2 is to require identification and authentication by the component of other devices, as well as requiring identification and authentication of the component itself to other devices. This interpretation was verified with members of the ISA99 standards committee.

  "Vendor shall provide a list of all types of software processes and devices with which the component can connect. For all of the listed types of software processes and devices, verify that

evidence exists that the component under evaluation can identify and authenticate itself to an entity of this type, for outgoing connections from the component to such an entity. Further, verify that evidence exists that the component can identify and authenticate each instance of a software process and device of a listed type, for incoming connections from such an entity to the component under evaluation. Identification and authentication of entities making incoming connections can be provided either locally or by integration into a system level identification and authentication system.

Record one of:

a. Met

b. Met by integration into system (for incoming connections)

c. Not met

d. Not relevant – component does not exchange data with any other devices or software processes

"Types" of software processes and devices are defined by the supplier, to distinguish entities with different functions, or that have different incoming or outgoing authentication capabilities that are required to interoperate with those of the component under evaluation. Various brands or models of connecting entities may fall under the same type, and do not need to be individually listed."

The following erratum for CR 2.1 incorporates a previous erratum for this requirement in CSA-102 v1.6. The previous erratum for CR 2.1 was in accordance with ISCI understanding that the intent of IEC 62443-4-2 CR 2.1 is to cover human users, as distinguished from CR 2.1 RE(1), which also covers users that are software processes and devices. This interpretation was verified with members of the ISA99 standards committee.

- **Change scope to human users and clarify authorization enforcement by system FSA-CR 2.1:** Replace the validation activity for FSA-CR 2.1 with the text:

  "For capability security levels 3 and 4, or if the component provides the capability to directly identify and authenticate human users, verify the component directly enforces authorizations for these users to control use of the component as configured. For capability security levels 1 and 2, if the component provides the capability to identify and authenticate human users by integration into a system, then verify that authorizations to access the component are enforced by either the component and/or external countermeasures that are documented in the supplier's security guidelines. These external countermeasures may include mechanisms that may or may not be integrated with the system, and policies/procedures that restrict how human users may connect to the component. Reliance upon external countermeasures not integrated with the system, or reliance upon adherence to policies/procedures that are carried out by non-administrators, is permitted for SL-C=1 only. Record one of:

  a. Met by component (without external countermeasures)
  b. Met with dependence on external countermeasures
  c. Not met
  If the component has no human users, record:
  d. Not relevant

  NOTE 1 Any mechanism via which a human may influence a deployed component, involves a human "user" (per definitions in 62443-1-1-2007 for "user" and "access"). A common scenario is human user access to a component via an intermediate program such as a configuration tool.

  NOTE 2 The following are example countermeasures related to the case of an external configuration tool that has a network connection to the component. These countermeasures might be used in various combinations to enforce restriction of component configuration access to authorized individuals for capability security levels 1 and 2.

Examples of external countermeasures integrated with the system:

- Human user identification/authorization capability of external configuration tool
- Device-level network restriction that only the intended configuration tool workstation can connect to the component configuration port
- Application-level restriction that only configuration tool software can connect to the component configuration interface
- Configuration tool and component are placed in same domain, with domain enforcement of permitted network connections to the component
- Mechanism that detects and/or prevents a second copy of configuration tool software from communicating on the IACS network
- Physical key required to power up the configuration tool workstation

Examples of external countermeasures not integrated with the system:

- Physical key required to gain physical access to enclosure that houses the configuration tool workstation

Examples of policies/procedures for administrators:

- Only one engineering workstation may be placed in domain with component

Examples of policies/procedures for non-administrators:

- Only one instance of engineering workstation software may be connected to IACS (in the case where no mechanisms detect/prevent a non-administrator from setting up such a connection)"

- **Clarify "supported as users" in FSA-CR 2.1 RE(1):** Replace the validation activity for FSA-CR 2.1 with the text:
"Review user documentation and determine if software processes or devices are supported with user accounts on the component.

  If software processes or devices are supported with user accounts, verify component enforces authorizations for processes and device users to control use of the component as configured by account management.

  Record one of:

  a. Met

  b. Not met

  If software processes or devices are not supported with user accounts on the component, record:

  c. Not relevant"

- **Supervisor override only required for operator interface:** Replace the validation activity for FSA-CR 2.1 RE(3) to read:

  "If the component has an operator interface, verify that the component can support supervisor override of role permissions for actions on this interface. Verify that the override can be configured to be in effect for a configurable time or sequence of events. Record one of:

  a. Met

  b. Not met

  Note if the component has an operator interface but roles are not supported for this interface, both this requirement and FSA-CR 2.1 are to be recorded as not met.

  If the component does not have an operator interface, record:

c. Not relevant”

- **Clarify outcomes for dual approval requirement assessment:** Replace the validation activity for FSA-CR 2.1 RE(4) by:

  “If the component has an operator interface, verify that the component supports dual approval for actions on this interface that could impact the industrial process. Record one of:

  a. Met

  b. Not met”

  If the component does not have an operator interface, record:

  c) Not relevant”

The following erratum is in accordance with the ISCI understanding that it was not the intent of IEC 62443-4-2 to require that all types of components support a *configurable* audit storage threshold that would trigger a warning.

- **Permit fixed threshold for audit warning:** Modify the validation activity for FSA-CR 2.9 RE(1) to replace “configurable threshold” with “fixed or configurable threshold,” so that the validation activity now reads: “Review user documents and confirm that the component has the capability to issue a warning when allocated audit record storage volume on the component reaches a fixed or configurable threshold. Record one of:

  a. Met

  b. Not met”

- **Clarify meaning of user vs. communication sessions:** Modify the validation activities for each of the requirements listed in the following table, as shown using italic underline and strikeout:

Requirement ID	Reference name	Validation activity
FSA-CR 2.7	Concurrent session control	Verify the component is able to be configured to limit the number of concurrent *user (login)* sessions per interface, for any given user (human, software process, or device). For all interfaces, verify that the supplier has executed and passed a test to verify this limit is enforced, by attempting to create more than the maximum number of *user* sessions allowed and verifying denial of connection once the threshold is reached. Record one of: a. Met b. Not met

Requirement ID	Reference name	Validation activity
FSA-CR 3.8A	Session integrity - invalidate session identifiers	Review user documentation and determine if *communication* sessions are used. If *communication* sessions are used, verify that design documentation confirms that ~~*user*~~ session identifiers *for communication sessions initiated by a user* are invalidated upon user logout or other session termination. Record one of: a. Met b. Not met If *communication* sessions are not used, record: c. Not relevant
FSA-CR 3.8B	Session integrity - generate and recognize session identifiers	Review user documentation and determine if *communication* sessions are used. If *communication* sessions are used, verify that design documents indicate that the component can generate ~~*user*~~ *communication* session identifiers for each session that are unique and that session IDs not generated by the system are rejected. Record one of: a. Met b. Not met If *communication* sessions are not used, record: c. Not relevant
FSA-CR 3.8C	Session integrity - random session identifiers	Review user documentation and determine if *communication* sessions are used. If *communication* sessions are used, verify that ~~*user*~~ *communication* session identifiers are generated by the system with an accepted level of randomness. Record one of: a. Met b. Not met If *communication* sessions are not used, record: c. Not relevant

— — — — — —