SSA-102
ISA Security Compliance Institute – System Security Assurance –

Baseline document versions and errata for SSA 4.0.0 specifications

Version 5.0

April 2023

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
1.2	2015.04.23	Initial version published to https://www.ISASecure.org
1.4	2015.06.22	Require full CRT tool version number and hash mechanism to verify version; update version of 17025; clarify definition of operational mode
1.5	2016.02.16	Measurement jitter 1% to 2%, broaden spec for detection of transitions
1.6	2016.03.09	Add reference to 62443-3-3 to SSA-204, 205 certificate format
2.0	2018.02.06	In SSA-200: add CACE and CACS as certifications for auditors, permit any bachelor-level degree with sufficient industry experience; in SSA-311: correct applicable levels for session ID requirements under FSA-S-SI-8; scalability updates for SSA-100, 200, 204, 205, 300, 310
3.0	2018.02.21	Update errata for SSA 2.1.0: remove all prior errata from SSA-102 v2.0, since they are implemented in the SSA 2.1.0 document set, except correction of applicable levels for session ID requirements under SSA-311 FSA-S-SI-8
3.1	2018.03.19	Modify requirements for SRT of redundant devices in SSA-310
3.3	2018.04.17	In SSA-310: modify 4.1.1.6 regarding definition of adequately maintain essential history data; modify SRT.R8 regarding submission of definition of essential history data
3.4	2018.10.11	In SSA-310: modify VIT pass criterion for consistency with SDLA-312 DM-4
3.8	2019.09.09	In SSA-300: remove requirement for component compliance with 62443-4-1; in SSA-311: add validation activity for requirements IAC-7, SI-1, SI-2, SI-3, SI-8, RA-1; clarify validation activity for SI-3.1; modify reason for no validation of RDF-1; modify validation for RDF-2 to cover all interfaces; delete erratum on SI-8.1 and 8.2
3.9	2019.11.18	In SSA-311, editorial correction to FSA-S-IAC 9.1, 9.3 and 9.4
4.0	2019.12.14	Update for SSA 4.0.0: remove all errata except for editorial correction from SSA-102 v3.9; add text regarding baseline versions
4.3	2021.03.07	In SSA-300, add definitions of human interface and accessible human interface; in SSA-311, modify selected validations for Identification and Authentication Control and Use Control to use these definitions, correct editorial errors in validation activities for FSA-S-IAC-8 and FSA-S-IAC-9.4, add validation for support of least privilege concept in FSA-S-UC-1; For SDLA-312 v5.5, consider accessible points of entry in threat model
4.5	2021.07.08	Add errata for SSA-311 to include not applicable case for requirements FSA-S-UC-3.1, 3.2, 3.3
4.7	2022.03.15	Update baseline version of SSA-200 in table 1, from v2.8 to v2.9, where v2.9 incorporates changes to assessor qualifications
4.8	2022.05.27	Change baseline version of SDLA-312 to v5.7 and reference errata as issued on that document; correct reference to zone in SSA-300 system example; correct typos in SSA-311 requirement IDs FSA-S-UC-3.3 and FSA-S-UC-3.4
4.9	2022.12.27	In SSA-200 section 4.2 clarify ISCI policy for certificate status and posting (5.3.1, 5.3.2, 5.3.3); in SSA-300 address certifier review of supplier submissions (5.5.3) and add requirement ISASecure_SY.R17 clarifying meaning of independent test (5.5.4); in SSA-301 address case of known vulnerability found after initial certification and not fixed (5.6.1); in present document clause 4: change baseline version of SSA-420 from v3.2 to v4.5, change baseline version of SDLA-312 from v5.7 to v6.3 (SDLA update is incorporation of errata, no net effect on SSA); format for unique section number and title per erratum
5.0	2023.04.21	Update Table 1 baseline version of SSA-204 from 2.0 to 3.0, to reflect policy to not permit placement of ISASecure logo on physical control system

Contents

FOREWORD

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

1 Scope

This document lists baseline versions and all approved changes to all ISASecure SSA 4.0.0 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 SSA specifications will result in a new issue of the relevant specification. This document maintains a list of changes which of themselves do not merit a new version of the specification which is changed. These changes may address typographical errors, cut and paste errors, or technical inaccuracies which are clearly non-controversial in the context of the overall intent of the specification.

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

2 Normative references

All documents listed below in Table 1 are normative references for this document.

Errata on SDLA-312 are provided separately in the following normative 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

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

4 Baseline document versions and index to errata

This clause lists all ISASecure SSA 4.0.0 baseline documents that may be the subject of errata, and indicates for each document whether errata apply to this document. 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 SSA, and are published separately in [SDLA-102].

Table 1 - ISASecure SSA 4.0.0 Baseline and Errata Index

Document ID	Document Title	Baseline Version	Errata	Reference in this document
SSA-100	*ISA Security Compliance Institute – System Security Assurance – ISASecure Certification Scheme*	3.1	Yes	5.2
SSA-200	*ISCI System Security Assurance – ISASecure SSA Chartered laboratory operations and accreditation*	2.9	Yes	5.3
SSA-204	*ISCI System Security Assurance – Instructions and Policies for Use of the ISASecure Symbol and Certificates*	3.0	No	5.4

Document ID	Document Title	Baseline Version	Errata	Reference in this document
SSA-205	*ISCI System Security Assurance – Certificate Document Format*	2.0	No	5.4
SSA-300	*ISCI System Security Assurance – ISASecure certification requirements*	3.1	Yes	5.5
SSA-301	*ISCI System Security Assurance – Maintenance of ISASecure certification*	3.1	Yes	5.6
SSA-311	*ISCI System Security Assurance – Functional security assessment for systems*	2.1	Yes	5.7
SSA-312	*ISCI System Security Assurance – Security development artifacts for systems*	1.6	No	5.8
SSA-420	*ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification*	4.5	No	5.9
SDLA-312	*ISCI Security Development Lifecycle Assurance – Security development lifecycle assessment*	6.3	No	5.10

5 Errata by document

5.1 General

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

5.2 SSA-100 ISASecure certification scheme

The following errata apply to SSA-100 version 3.1.

5.2.1 Add reference to SSA-102

In clause 2, add the sentence “A list of baseline document version numbers and errata on the baseline documents is published in [SSA-102].” In 2.3.1, after [SSA-303], add the reference “[SSA-102] *ISCI System Security Assurance – Baseline document versions and errata for SSA 4.0.0 specifications*, as specified at https://www.ISASecure.org.”

5.2.2 SSA-102 not shown in Figure 1

In 4.6.1, 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 [SSA-102],* the application form [ISASecure-202], the certificate form [SSA-205], and the policy document [ISASecure-117] regarding the ISASecure transition to SSA 4.0.0.”

5.3 SSA-200 Chartered laboratory operations and accreditation

The following errata apply to SSA-200 version 2.9.

5.3.1 Posting certificate status

Replace the following existing sentence in section 4.2, with the paragraph and note following:

Existing sentence: "At the request of system suppliers, systems that are issued certifications are registered on this same ISCI website."

Replacement paragraph and note: "A chartered laboratory reports new certificates and status changes (terminations and withdrawals) to ISCI (see Requirement_SSA.R39.) Certificates granted and status changes are posted on the ISCI website. ISCI will post certificates and status changes upon receipt from a chartered laboratory, except that for certificates granted, a supplier may request that posting be delayed up to 90 days. ISCI will provide a facility via which a product user may determine if a SSA certification has been granted, terminated, or withdrawn.

NOTE A supplier may request a delay in posting a certificate granted to receive advantageous timing for planned announcements."

5.3.2 Refer to SSA-301 regarding validity of certification

Replace Requirement_SSA.R38 by the following text:

"Requirement_SSA.R38 Withdrawal or termination of certification A SSA product certification SHALL remain valid for a product and its updates, or be withdrawn in accordance with [SSA-301] Requirement ISASecure_SYM.R2.

The certification body SHALL terminate a certification if the supplier reports to them that the product has left support status under the ISASecure SDLA-certified SDL process, or if the supplier otherwise requests termination of the certification for any reason.

If the certifier determines the supplier has not participated in good faith in the certification process, the certifier SHALL withdraw the certification."

5.3.3 Notification of certification status change

Replace Requirement_SSA.R39 by the following text and note:

"Requirement_SSA.R39 Notification of certification status change The chartered laboratory SHALL inform ISCI of any withdrawal or termination of an ISASecure product certification at the time it occurs. The chartered laboratory SHALL inform the supplier that ISCI posts certificates granted, upon receipt from the chartered laboratory, except that the supplier may request a delay of up to 90 days from the grant date for posting of certificates granted.

NOTE The action to terminate or withdraw a certificate that is granted, but not yet posted on the ISCI website, will not be posted by ISCI."

5.4 SSA 204/205 Symbol and certificate

No errata apply to the specifications SSA-204 version 2.0 or SSA-205 version 2.0.

5.5 SSA-300 ISASecure certification requirements

The following errata apply to SSA-300 version 3.1.

5.5.1 Add definitions of human interface and accessible human interface

In 3.1, add the following definitions, which are used in SSA-311 errata found in sections 5.7.2 and 5.7.5 of the present document.

human interface
interface on a component, via which input from a human can flow to/from the component

NOTE The following is from the IEC 62443-4-2 rationale for CR 1.1: “Interfaces capable of human user access are local user interfaces such as touchscreens, push buttons, keyboards, etc. as well as network protocols designed for human user interactions such as hypertext transfer protocol (HTTP), HTTP secure (HTTPS), file transfer protocol (FTP), secure FTP (SFTP), protocols used for device configuration tools (which are sometimes proprietary and other times use open protocols).”

accessible human interface
human interface such that use of this interface can occur without physical or logical reconfiguration, when the system is configured in accordance with security guidelines

NOTE As examples, for a switch HMI where the switch has an interface supporting http, but is recommended in the security guidelines to be placed in a locked cabinet, this is not an accessible human interface. Likewise, if security guidelines recommend that an http interface be logically disabled during normal operations and maintenance, using security settings, then it is not an accessible human interface.

5.5.2 Correct reference to zone in system example

In 6.2, change “process operations zones” in the following sentence, to “process control zones.” **“**The two control system servers in the *process operations zones* on C-LAN 2 and C-LAN 3, are also accessible from C-LAN 1, the process operations zone.”

5.5.3 Add certifier review of supplier submissions

In 5.4, at the end of ISASecure_SY.R6, as a part of that requirement, add the following text: “The certifier SHALL in the course of certification activities, review the supplier submissions upon which these activities depend. The review SHALL verify completeness and consistency of these submissions with definitions in the SSA specifications and with the product as presented for certification. The supplier SHALL make revisions to these submissions if found necessary in this review.”

5.5.4 Meaning of validation by independent test

Add the following additional requirement after ISASecure_SY.R16:

“Requirement ISASecure_SY.R17 – Validation by independent test

If a validation activity for a requirement in [SSA-311] specifies that validation by independent test is required (identified by a “Yes” in the column titled “Validation by Independent Test Required (Yes/No)”) this means that the assessor SHALL BE fully responsible for the testing described. In particular this SHALL include responsibility for the appropriateness and quality of the test, and witnessing the execution of the test. The assessor MAY at their discretion use tools created by the supplier and assistance from supplier personnel in carrying out the test.”

5.6 SSA-301 Maintenance of ISASecure certification

The following errata apply to the specification SSA-301 version 3.1.

5.6.1 Known vulnerability found and not fixed

- Add the following two terms and definitions, and accompanying notes, to section 3.1:

“fix (for a product security issue)
modification of a product and/or its documented security guidance to address a security issue, such that the resulting product version would meet certification criteria specified for initial product certification

NOTE 1 This definition is based upon the usage of the term in IEC 62443-4-1 requirement DM-4, part a).

NOTE 2 Changes that eliminate a security issue may or may not fall under this definition of “fix.” For example, recommending use of the user’s choice of an external firewall to protect against exploitation of a critical vulnerability is not a “fix.” Since the firewall is not part of the product, the product still has a critical vulnerability and so does not meet initial certification criteria. On the other hand, incorporating a specific firewall into the product and satisfying IEC 62443-4-1 requirements for that firewall as a third party component. would count as a fix. As a second example, suppose that a flawed security capability was removed from the product and replaced by instructions for integration with an external system to achieve the security capability. This would be considered a fix if IEC 62443-4-2 explicitly permitted the capability to be achieved by integration into a system, but would not be a fix if IEC 62443-4-2 did not permit this.”

“version (of system)
well defined release of a system”

- At the end of requirement ISASecure_SYM.R2, add this paragraph to that requirement:

“After initial certification, it is possible that previously unknown vulnerabilities may become known in the product version initially certified, or in one of its updates. It is possible that the severity of such a vulnerability exceeds the risk threshold established for the product per SDLA-312 requirement SDLA-DM-4, or that the vulnerability prevents the product from meeting one or more functional requirements for certification. In these situations, if the supplier concludes that it is infeasible or impractical to fix the issue with a product update, the supplier SHALL inform the certifying chartered laboratory, who SHALL withdraw the certification. The certification body SHALL reasonably coordinate with the supplier so that the supplier may communicate with product users before the certification is withdrawn, but in all cases SHALL withdraw the certification at most 90 days after being informed by the supplier that the vulnerability will not be fixed by a product update. The supplier SHALL communicate with product users regarding the vulnerability as required by IEC 62443-4-1 Requirement DM-5 Disclosing security-related issues.”

5.7 SSA-311 Functional Security Assessment for systems

The following errata apply to SSA-311 version 2.1.

5.7.1 Correct letters that identify evaluation options in FSA-S-IAC 9.1, 9.3, 9.4

For requirements FSA-S-IAC 9.1, 9.3 and 9.4, in the validation activity column, identify selectable options by the letters “a, b, c” instead of “a, a, b.”

5.7.2 Clarify interfaces subject to Identification and Authentication control requirements

For requirements shown in Table 2 below, apply modifications to text in the column titled “Validation Activity” as shown in red italic font. Requirement rows greyed out have no changes but are included for convenience.

5.7.3 Add missing words in validation activity for FSA-S-IAC-8

For the requirement FSA-S-IAC-8, in text for validation activity, change “required public key authentication” to “required practices for public key authentication,” as shown in Table 2 below.

5.7.4 Correct typographical error in validation activity for FSA-S-IAC-9.4

For the requirement FSA-S-IAC-9.4, in text for validation activity, change “an” to “a” as shown in Table 2 below.

Table 2 - Modifications to Identification and Authentication Control validation activities

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-1	Human user identification and authentication	The SUT shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the SUT to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Verify that the SUT can uniquely identify and authenticate all *human* users at all accessible *human* interfaces and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human interfaces*	IEC 62443-3-3: SR1.1
FSA-S-IAC-1.1	Unique identification and authentication	The SUT shall provide the capability to uniquely identify and authenticate all human users.	Verify that the SUT can uniquely identify and authenticate all *human* users at all ~~*user*~~ accessible *human* interfaces and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human interfaces*	IEC 62443-3-3: SR1.1 (1)
FSA-S-IAC-1.2	Multifactor authentication for untrusted networks	The SUT shall provide the capability to employ multifactor authentication for human user access to the SUT via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).	Verify that the SUT can provide the capability of multifactor authentication for remote access and record results as: a. Supported, or b. Not Supported	IEC 62443-3-3: SR1.1 (2)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-1.3	Multifactor authentication for all networks	The SUT shall provide the capability to employ multifactor authentication for all human user access to the SUT.	Verify that the SUT can require multifactor authentication for local access *to accessible human interfaces* (e.g. access within the zone) and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human interfaces*	IEC 62443-3-3: SR1.1 (3)
FSA-S-IAC-2	Software process and device identification and authentication	The SUT shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the SUT to support least privilege in accordance with applicable security policies and procedures.	Vendor shall provide list of all software processes and devices that can connect to the SUT *via an accessible network interface*. Verify that evidence exists that identification and authentication is done for each listed process and device and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible network interfaces*	IEC 62443-3-3: SR1.2
FSA-S-IAC-2.1	Unique identification and authentication	The SUT shall provide the capability to uniquely identify and authenticate all software processes and devices.	Vendor shall provide list of all software processes and devices that can connect to the SUT *via an accessible network interface*. Verify that evidence exists that each process and device that can connect to the SUT has a unique identification and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible network interfaces*	IEC 62443-3-3: SR1.2 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-3	Account management	The SUT shall provide the capability to support the management of all accounts, including establishing, activating, modifying, disabling and removing accounts.	*Where user accounts are supported for accessible human and network interfaces,* verify SUT supports account management functions by an administrator type role to establish, activate, modify, disable and remove accounts, and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces* *Therefore if an accessible human or network interface supports only a fixed set of user accounts, this requirement is not supported.*	IEC 62443-3-3: SR1.3
FSA-S-IAC-3.1	Unified account management	The SUT shall provide the capability to support unified account management	Verify SUT supports unified account management functions to establish, activate, modify, disable and remove accounts. Verify that performing these functions on an account is applicable to all components of the system that support user accounts *for accessible human and network interfaces* and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.3 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-4	Identifier management	The SUT shall provide the capability to support the management of identifiers (e.g. user ID) by user, group, role and/or SUT interface	Verify user documents indicate that *for accessible human or network interfaces*, the SUT allows managing identifiers by user, group, role and / or interface and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.4
FSA-S-IAC-5	Authenticator management	The SUT shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon SUT installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	See child requirements	IEC 62443-3-3: SR1.5
FSA-S-IAC-5.1	Initialize authenticator content	The SUT shall provide the capability to define initial authenticator content;	Verify user documents indicate ability to define initial authentication content *for accessible human and network interfaces* and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.5 (a)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-5.2	Change default authenticators	The SUT shall provide the capability to change default authenticators upon SUT installation;	Verify user documents indicate ability to change default authenticators *for users at accessible human and network interfaces* and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.5 (b)
FSA-S-IAC-5.3	Change/ refresh all authenticators periodically	The SUT shall provide the capability to change/refresh authenticators periodically; and	Verify user documents indicate ability to change/refresh authenticators *for users at accessible human and network interfaces* and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.5 (c)
FSA-S-IAC-5.4	Protect authenticators	The SUT shall provide the capability to protect authenticators from unauthorized disclosure and modification when stored and transmitted.	Verify user documents indicate ability to protect authenticators *for users at accessible human and network interfaces* from unauthorized disclosure and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.5 (d)
FSA-S-IAC-5.5	Hardware security for software process identity credentials	For software process and device users, the SUT shall provide the capability to protect the relevant authenticators via hardware mechanisms.	Verify user documents indicate ability to protect relevant authenticators with hardware mechanisms and record results as: a. Supported, or b. Not Supported	IEC 62443-3-3: SR1.5 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-6	Wireless access management	The SUT shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Review user documentation and determine if wireless communication is supported on the SUT. If not record the result as: a. Not Applicable If wireless is communication is supported vendor shall provide list of all software processes and devices that can connect to the SUT via the wireless connection. Verify that evidence exists that identification and authentication is done for each listed process and device and for human users and record results as: a. Supported, or b. Not Supported	IEC 62443-3-3: SR1.6
FSA-S-IAC-6.1	Unique identification and authentication	The SUT shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Review user documentation and determine if wireless communication is supported on the SUT. If not record the result as: a. Not Applicable If wireless is communication is supported vendor shall provide list of all software processes and devices that can connect to the SUT via the wireless connection. Verify that evidence exists that each process and device that can connect to the SUT has a unique identification and record results as: a. Supported, or b. Not Supported	IEC 62443-3-3: SR1.6 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-7	Strength of password-based authentication	For SUT utilizing password-based authentication, the SUT shall provide the capability to enforce password strength restrictions	If the SUT utilizes password-based authentication *for accessible human or network interfaces*, verify *that* user documents indicate that configurable password strength can be enforced. Record results as: a. Supported, or b. Not supported, or c*. Not applicable – if the SUT has no accessible human or network interfaces that use password-based authentication*	IEC 62443-3-3: SR1.7
FSA-S-IAC-7.1	Password generation and lifetime restrictions for human users	The SUT shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the SUT shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices.	*For accessible human or network interfaces that utilize password-based authentication,* verify user documents indicate that password re-use can be limited for a specified number of generations and record results as: a. Supported, or b. Not Supported*, or* *c. Not Applicable – if the SUT has no accessible human or network interfaces that use password-based authentication*	IEC 62443-3-3: SR1.7 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-7.2	Password lifetime restrictions for all users	For SUT utilizing password-based authentication, the SUT shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users	*For accessible human or network interfaces that utilize password-based authentication*, verify user documents indicate that the SUT provides the capability to enforce password minimum and maximum lifetime restrictions for all users and record results as: a. Supported, or b. Not Supported*, or* *c. Not Applicable – if the SUT has no accessible human or network interfaces that use password-based authentication*	IEC 62443-3-3: SR1.7 (2)
FSA-S-IAC-8	Public key infrastructure (PKI) certificates	Where PKI is utilized, the SUT shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.	Verify user documents indicate that the required *practices for* public key authentication are supported if public key functionality is offered and record results as: a. Supported, or b. Not Supported, or c. NA - if public key is not supported	IEC 62443-3-3: SR1.8

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-9	Strength of public key authentication	For SUTs utilizing public key authentication, the SUT shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted certification authority (CA)CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).	See child requirements	IEC 62443-3-3: SR1.9
FSA-S-IAC-9.1	Check validity of signature of a given certificate	validate certificates by checking the validity of the signature of a given certificate	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, provide a certificate with an invalid signature to a test system. Verity that the system detects this problem and reports this problem to the user. Verify that the connection is denied unless the user chooses to allow the connection anyway and record results as: a. Supported b. Not Supported	IEC 62443-3-3: SR1.9 (a)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-9.2	Construct a certification path to an accepted CA	validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued;	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, review design documentation and determine if the system validates certificates by construction a certification path to an accepted CA or in the case of self-signed certificates, by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued and record results as: b. Supported c. Not Supported	IEC 62443-3-3: SR1.9 (b)
FSA-S-IAC-9.3	Check a given certificates revocation status	validate certificates by checking a given certificate's revocation status;	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, provide a certificate with a revoked status. verify that the system detects this problem and reports this problem to the user. Verify that the connection is denied unless the user chooses to allow the connection anyway and record results as: a. Supported b. Not Supported	IEC 62443-3-3: SR1.9 (c)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-9.4	Establish user control of private key	establish user (human, software process or device) control of the corresponding private key	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, provide a certificate with a~~n~~ valid signature and non-revoked status to a test system. verify that the system allows this connection and accepts the data from this server and record results as: a. Supported b. Not Supported	IEC 62443-3-3: SR1.9 (d)
FSA-S-IAC-9.5	Map authenticated identity to a user	map the authenticated identity to a user (human, software process or device)	Test for FSA-S-IAC-9.4 covers this item as well	IEC 62443-3-3: SR1.9 (e)
FSA-S-IAC-9.6	Hardware security for public key authentication	The SUT shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, review design documentation if hardware mechanisms according to commonly accepted security industry practices and recommendations are used to protect the relevant private keys and record results as: b. Supported c. Not Supported	IEC 62443-3-3: SR1.9 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-10	Authenticator feedback	The SUT shall provide the capability to obscure feedback of authentication information during the authentication process	Verify SUT is capable of obscuring feedback of authentication information *at accessible human or network interfaces* and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.10
FSA-S-IAC-11	Unsuccessful login attempts	The SUT shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The SUT shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the SUT shall provide the capability to disallow interactive logons.	Verify SUT is capable of monitoring of unsuccessful login attempts *at accessible human or network interfaces* with configurable ability to deny access permanently or for a configurable time period based on repeated unsuccessful attempts and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR1.11
FSA-S-IAC-12	System use notification	The SUT shall provide the capability to display a configurable system use notification message before authenticating.	Verify SUT is capable of displaying user configurable system use notifications *at accessible human interfaces* and records results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human interfaces*	IEC 62443-3-3: SR1.12

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-IAC-13	Access via untrusted networks	The SUT shall provide the capability to monitor and control all methods of access to the SUT via untrusted networks.	Verify user documents include the capability to monitor and control all forms of remote access via untrusted networks is supported and records results as: a. Supported, or b. Not Supported	IEC 62443-3-3: SR1.13
FSA-S-IAC-13.1	Explicit access request approval	The SUT shall provide the capability to deny ~~remote~~ access requests by default (e.g. access via untrusted networks) unless explicitly approved by an assigned role.	Verify user documents include the capability to deny remote access by default and record results as: a. Supported, or b. Not Supported	IEC 62443-3-3: SR1.13 (1)

5.7.5 Clarify interfaces subject to Use control requirements

For requirements shown in Table 3 below, apply modifications to text in the column titled “Validation Activity,” as shown in red italic font.

5.7.6 Add validation of support for least privilege concept under FSA-S-UC-1

Add second paragraph to the description of the validation activity for FSA-S-UC-1 as shown in red italic font in Table 3 below.

Table 3 - Modifications to validation activity for Use Control requirements

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-UC-1	Authorization enforcement	On all interfaces, the SUT shall provide the capability to enforce authorizations assigned to all human users for controlling use of the SUT to support segregation of duties and least privilege.	*For all accessible human interfaces*, verify SUT enforces authorizations for human users to control use of the SUT as configured by account management. *The SDA certification element under requirement SDLA-SG-6 in document SDLA-312, requires*	IEC 62443-3-3: SR2.1

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
			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 system. 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. *Considering both verifications,* record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human interfaces*	
FSA-S-UC-1.1	Authorization enforcement for all users	On all interfaces, the SUT shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the SUT to support segregation of duties and least privilege.	*For all accessible human and network interfaces,* verify SUT enforces authorizations for processes and devices to control use of the SUT as configured by account management and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human or network interfaces*	IEC 62443-3-3: SR2.1 (1)

Requirement ID	Reference Name	Requirement Description	Validation Activity	Source of Requirement
FSA-S-UC-1.2	Permission mapping to roles	The SUT shall provide the capability for an authorized user or role to modify the mapping of permissions to roles for human users	*For all accessible human interfaces,* verify SUT provides the capability to map permissions to roles if authorized by a supervisory level account and record results as: a. Supported, or b. Not Supported*, or* *c. Not applicable – if the SUT has no accessible human interfaces*	FSA-S-UC-1.2

5.7.7 Add validation outcome of “Not applicable” for FSA-S-UC 3.1, 3.2, and 3.3

For requirements FSA-S-UC 3.1, FSA-S-UC 3.2, and FSA-S-UC 3.3, append the following to the text of the validation activity:

“c. Not applicable if portable and mobile devices cannot connect to the system”

5.7.8 Correct typographical error in Tree list requirement ID for FSA-S-UC 3.3

Change the requirement ID currently shown as “FSA-S-UC-3-3” in the Tree summary list of requirements, to replace the fourth dash with a period, so that it reads “FSA-S-UC-3.3.”

5.7.9 Correct typographical error in Requirement ID for FSA-S-UC-3.4

Change the requirement ID currently shown as “FSA-S-UC-3, 4” to replace the comma with a period so that it reads “FSA-S-UC-3.4”.

5.7.10 Change device to system in FSA-S-UC-4.3, 4.4, 4.5

In the validation activities for FSA-S-UC-4.3, 4.4, and 4.5, change the text for option c) from “Not applicable if the device does not allow any mobile code to execute” to “Not applicable if the system does not allow any mobile code to execute.”

5.8 SSA-312 Security Development Artifacts

No errata apply to the specification SSA-312 version 1.6.

5.9 SSA-420 Vulnerability Identification Testing

No errata apply to the specification SSA-420 version 4.5.

5.10 SDLA-312 Security development lifecycle assessment

Any errata for SDLA-312 are found in the document [SDLA-102].

— — — — — —