CSA-311

ISA Security Compliance Institute — Component Security Assurance

Functional security assessment for components

Version 2.3

December 2022

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.

CSA-311 Component Security Assurance - Functional security assessment for components, Version 2.3

version	date	changes
1.11	2019.08.03	initial version published to https://www.isasecure.org
2.3	2022.12.07	incorporated errata from CSA-102 v2.2; add not relevant case where no essential functions in FSA-CCSC 1A, CCSC 1B, CCSC 1C, CCSC 1F, FSA-CR 2.10A, FSA-CR 7.1; modify scope of validation FSA-CR 2.12; add outcomes to FSA-HDR 3.2 RE(1); clarifications FSA-EDR|HDR|NDR 3.14, EDR|HDR|NDR 3.14 RE(1), FSA-CR 4.1B; add not relevant case to FSA-CR 4.2 RE(1); refer to ICSA-500 in FSA-CR 4.3; correct SDLPA to SDA in FSA-CR 7.1 RE(1) and FSA-CR 7.6; editorial changes in validation activities for FSA-CR 1.9B, FSA-NDR 1.13, FSA-NDR 1.13 RE(1)

Summary of Worksheets:

Overview	**Overview** - this worksheet providing summary information about each worksheet
Tree	**Tree Structure** - hierarchical summary of all requirements organized by the 7 Foundational Requirements
CCSC	**Common component security constraints** - detailed requirements for common component security constraints
FR 1	**Identification & authentication control** - detailed requirements for 1st Foundational Requirement
FR 2	**Use control** - detailed requirements for 2nd Foundational Requirement
FR 3	**System integrity** - detailed requirements for 3rd Foundational Requirement
FR 4	**Data confidentiality** - detailed requirements for 4th Foundational Requirement
FR 5	**Restricted data flow** - detailed requirements for 5th Foundational Requirement
FR 6	**Timely response to events** - detailed requirements for 6th Foundational Requirement
FR 7	**Resource availability** - detailed requirements for 7th Foundational Requirement

Common structure used for all requirement worksheets:

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance

Software Application - indicates whether each requirement applies to a software application
Embedded Device - indicates whether each requirement applies to an embedded device
Host Device - indicates whether each requirement applies to a host device
Network Device - indicates whether each requirement applies to a network device
Requirement ID - unique ID number assigned to each requirement within this document
Reference Name - name for each requirement that provides an indication of the scope / content (using names from IEC 62443-4-2, with name extensions to designate parts of requirements)
Requirement Description - text of the requirement from IEC 62443-4-2
Validation Activity - defines activity that must be performed as part of the evaluation audit
Validation by Independent Test Required - indicates whether the auditor is required to perform independent testing as part of the validation activity
Source of Requirement - Reference in IEC 62443-4-2 for the requirement
Capability Security Level - specifies those capability security levels to which the requirement applies in IEC 62443-4-2
Rationale and Supplemental Guidance - additional information on the requirement from sub clause with this title in IEC 62443-4-2

Normative references - The following pairs of references provide the same technical standard, as published by the organizations ANSI/ISA and IEC.

ANSI/ISA-62443-4-2-2018 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components
IEC 62443-4-2:2019 Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components

ANSI/ISA-62443-4-1-2018 Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements
IEC 62443-4-1:2018 Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements

Software Application	Embedded Device	Host Device	Network Device	Section	Requirement ID and Reference Name	Capability Security Level
				CCSC - Common Component Security Constraints		
x	x	x	x		FSA-CCSC 1A Support of essential functions - account lock out	1, 2, 3, 4
x	x	x	x		FSA-CCSC 1B Support of essential functions - non-repudiation	1, 2, 3, 4
x	x	x	x		FSA-CCSC 1C Support of essential functions - failure of certificate authority	1, 2, 3, 4
	x				FSA-CCSC 1D Support of essential functions - I&A and SIF initiation	1, 2, 3, 4
	x				FSA-CCSC 1E Support of essential functions - authorization and SIF initiation	1, 2, 3, 4
x	x	x	x		FSA-CCSC 1F Support of essential functions - incorrect timestamps	1, 2, 3, 4
					FSA-CCSC 1G Support of essential functions - zone isolation	
	x				FSA-CCSC 1H Support of essential functions - DoS and SIF initiation	1, 2, 3, 4
x	x	x	x		FSA-CCSC 2 Compensating countermeasures	1, 2, 3, 4
x	x	x	x		FSA-CCSC 3 Least privilege	1, 2, 3, 4
x	x	x	x		FSA-CCSC 4 Software development process	1, 2, 3, 4
				FR 1 - Identification & Authentication Control		
x	x	x	x		FSA-CR 1.1 Human user identification and authentication	1, 2, 3, 4
x	x	x	x		FSA-CR 1.1 RE(1) Unique identification and authentication	2, 3, 4
x	x	x	x		FSA-CR 1.1 RE(2) Multifactor authentication for all interfaces	3, 4
x	x	x	x		FSA-CR 1.2 Software process and device identification and authentication	2, 3, 4
x	x	x	x		FSA-CR 1.2 RE(1) Unique identification and authentication	3, 4
x	x	x	x		FSA-CR 1.3 Account management	1, 2, 3, 4
x	x	x	x		FSA-CR 1.4 Identifier management	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5A Authenticator management - initialize authenticator content	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5B Authenticator management - change default authenticators	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5C Authenticator management - change/refresh all authenticators periodically	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5D Authenticator management - protect authenticators	1, 2, 3, 4
x	x	x	x		FSA-CR 1.5 RE(1) Hardware security for authenticators	3, 4
			x		FSA-NDR 1.6 Wireless access management	1, 2, 3, 4
			x		FSA-NDR 1.6 RE(1) Unique identification and authentication	2, 3, 4
x	x	x	x		FSA-CR 1.7 Strength of password-based authentication	1, 2, 3, 4
x	x	x	x		FSA-CR 1.7 RE(1) Password generation and lifetime restrictions for human users	3, 4
x	x	x	x		FSA-CR 1.7 RE(2) Password lifetime restrictions for all users (human, software process, or device)	4
x	x	x	x		FSA-CR 1.8 Public key infrastructure (PKI) certificates	2, 3, 4
x	x	x	x		FSA-CR 1.9A Strength of public key-based authentication - check validity of signature of a given certificate	2, 3, 4
x	x	x	x		FSA-CR 1.9B Strength of public key-based authenticationn -validate certificate chain	2, 3, 4
x	x	x	x		FSA-CR 1.9C Strength of public key-based authentication - check certificate's revocation status	2, 3, 4
x	x	x	x			2, 3, 4

Software Application	Embedded Device	Host Device	Network Device	Section	Requirement ID and Reference Name	Capability Security Level
x	x	x	x		FSA-CR 1.9E Strength of public key-based authentication - map authenticated identity to a user	2, 3, 4
x	x	x	x		FSA-CR 1.9F Strength of public key-based authentication - use of cryptography	2, 3, 4
x	x	x	x		FSA-CR 1.9 RE(1) Hardware security for public key-based authentication	3, 4
x	x	x	x		FSA-CR 1.10 Authenticator feedback	1, 2, 3, 4
x	x	x	x		FSA-CR 1.11A Unsuccessful login attempts - limit number	1, 2, 3, 4
x	x	x	x		FSA-CR 1.11B Unsuccessful login attempts - response	1, 2, 3, 4
x	x	x	x		FSA-CR 1.12 System use notification	1, 2, 3, 4
			x		FSA-NDR 1.13 Access via untrusted networks	1, 2, 3, 4
			x		FSA-NDR 1.13 RE(1) Explicit access request approval	3, 4
x	x	x	x		FSA-CR 1.14A Strength of symmetric key-based authentication - establish trust	2, 3, 4
x	x	x	x		FSA-CR 1.14B Strength of symmetric key-based authentication - secure storage for shared secret	2, 3, 4
x	x	x	x		FSA-CR 1.14C Strength of symmetric key-based authentication - restrict access to shared secret	2, 3, 4
x	x	x	x		FSA-CR 1.14D Strength of symmetric key-based authentication - use of cryptography	2, 3, 4
x	x	x	x		FSA-CR 1.14 RE(1) Hardware security for symmetric key-based authentication	3, 4
				FR 2 - Use Control		
x	x	x	x		FSA-CR 2.1 Authorization enforcement	1, 2, 3, 4
x	x	x	x		FSA-CR 2.1 RE(1) Authorization enforcement for all users (humans, software processes and devices)	2, 3, 4
x	x	x	x		FSA-CR 2.1 RE(2) Permission mapping to roles	2, 3, 4
x	x	x	x		FSA-CR 2.1 RE(3) Supervisor override	3, 4
x	x	x	x		FSA-CR 2.1 RE(4) Dual approval	4
x	x	x	x		FSA-CR 2.2 Wireless use control	1, 2, 3, 4
					FSA-CR 2.3 Use control for portable and mobile devices	NA
x					FSA-SAR 2.4A Mobile code - control execution	1, 2, 3, 4
x					FSA-SAR 2.4B Mobile code - control transfer by user	1, 2, 3, 4
x					FSA-SAR 2.4C Mobile code - integrity check	1, 2, 3, 4
x					FSA-SAR 2.4 RE(1) Mobile code authenticity check	2, 3, 4
	x				FSA-EDR 2.4A Mobile code - control execution	1, 2, 3, 4
	x				FSA-EDR 2.4B Mobile code - control upload by user	1, 2, 3, 4
	x				FSA-EDR 2.4C Mobile code - integrity check	1, 2, 3, 4
	x				FSA-EDR 2.4 RE(1) Mobile code authenticity check	2, 3, 4
		x			FSA-HDR 2.4A Mobile code - control execution	1, 2, 3, 4
		x			FSA-HDR 2.4B Mobile code - control upload by user	1, 2, 3, 4
		x			FSA-HDR 2.4C Mobile code - integrity check	1, 2, 3, 4
		x			FSA-HDR 2.4 RE(1) Mobile code authenticity check	2, 3, 4
			x		FSA-NDR 2.4A Mobile code - control execution	1, 2, 3, 4

Software Application	Embedded Device	Host Device	Network Device	Section	Requirement ID and Reference Name	Capability Security Level
			x		FSA-NDR 2.4B Mobile code - control transfer by user	1, 2, 3, 4
			x		FSA-NDR 2.4C Mobile code - integrity check	1, 2, 3, 4
			x		FSA-NDR 2.4 RE(1) Mobile code authenticity check	2, 3, 4
x	x	x	x		FSA-CR 2.5A Session lock- initiation	1, 2, 3, 4
x	x	x	x		FSA-CR 2.5B Session lock- removal	1, 2, 3, 4
x	x	x	x		FSA-CR 2.6 Remote session termination	2, 3, 4
x	x	x	x		FSA-CR 2.7 Concurrent session control	3, 4
x	x	x	x		FSA-CR 2.8A Auditable events - categories	1, 2, 3, 4
x	x	x	x		FSA-CR 2.8B Auditable events - data fields	1, 2, 3, 4
x	x	x	x		FSA-CR 2.9A Audit storage capacity - allocation	1, 2, 3, 4
x	x	x	x		FSA-CR 2.9B Audit storage capacity - exceeded	1, 2, 3, 4
x	x	x	x		FSA-CR 2.9 RE(1) Warn when audit record storage capacity threshold reached	3, 4
x	x	x	x		FSA-CR 2.10A Response to audit processing failures - maintain essential functions	1, 2, 3, 4
x	x	x	x		FSA-CR 2.10B Response to audit processing failures - actions taken	1, 2, 3, 4
x	x	x	x		FSA-CR 2.11 Timestamps	1, 2, 3, 4
x	x	x	x		FSA-CR 2.11 RE(1) Time synchronization	2, 3, 4
x	x	x	x		FSA-CR 2.11 RE(2) Protection of time source integrity	4
x	x	x	x		FSA-CR 2.12 Non-repudiation	1, 2, 3, 4
x	x	x	x		FSA-CR 2.12 RE(1) Non-repudiation for all users	4
	x				FSA-EDR 2.13 Use of physical diagnostic and test interfaces	2, 3, 4
	x				FSA-EDR 2.13 RE(1) Active monitoring	3, 4
		x			FSA-HDR 2.13 Use of physical diagnostic and test interfaces	2, 3, 4
		x			FSA-HDR 2.13 RE(1) Active monitoring	3, 4
			x		FSA-NDR 2.13 Use of physical diagnostic and test interfaces	2, 3, 4
			x		FSA-NDR 2.13 RE(1) Active monitoring	3, 4
				FR 3 - System Integrity		
x	x	x	x		FSA-CR 3.1 Communication integrity	1, 2, 3, 4
x	x	x	x		FSA-CR 3.1 RE(1) Communication authentication	2, 3, 4
x					FSA-SAR 3.2 Protection from malicious code	1, 2, 3, 4
	x				FSA-EDR 3.2 Protection from malicious code	1, 2, 3, 4
		x			FSA-HDR 3.2 Protection from malicious code	1, 2, 3, 4
		x			FSA-HDR 3.2 RE(1) Report version of code protection	2, 3, 4
			x		FSA-NDR 3.2 Protection from malicious code	1, 2, 3, 4
x	x	x	x		FSA-CR 3.3 Security functionality verification	1, 2, 3, 4
x	x	x	x		FSA-CR 3.3 RE(1) Security functionality verification during normal operation	4

Software Application	Embedded Device	Host Device	Network Device	Section	Requirement ID and Reference Name	Capability Security Level
x	x	x	x		FSA-CR 3.4 Software and information integrity	1, 2, 3, 4
x	x	x	x		FSA-CR 3.4 RE(1) Authenticity of software and information	2, 3, 4
x	x	x	x		FSA-CR 3.4 RE(2) Automated notification of integrity violations	3, 4
x	x	x	x		FSA-CR 3.5 Input validation	1, 2, 3, 4
x	x	x	x		FSA-CR 3.6 Deterministic output	1, 2, 3, 4
x	x	x	x		FSA-CR 3.7 Error handling	1, 2, 3, 4
x	x	x	x		FSA-CR 3.8A Session integrity - invalidate session identifiers	2, 3, 4
x	x	x	x		FSA-CR 3.8B Session integrity - generate and recognize session identifiers	2, 3, 4
x	x	x	x		FSA-CR 3.8C Session integrity - random session identifiers	2, 3, 4
x	x	x	x		FSA-CR 3.9 Protection of audit information	2, 3, 4
x	x	x	x		FSA-CR 3.9 RE(1) Audit records on write-once media	4
	x				FSA-EDR 3.10 Support for updates	1, 2, 3, 4
	x				FSA-EDR 3.10 RE(1) Update authenticity and integrity	2, 3, 4
		x			FSA-HDR 3.10 Support for updates	1, 2, 3, 4
		x			FSA-HDR 3.10 RE(1) Update authenticity and integrity	2, 3, 4
			x		FSA-NDR 3.10 Support for updates	1, 2, 3, 4
			x		FSA-NDR 3.10 RE(1) Update authenticity and integrity	2, 3, 4
	x				FSA-EDR 3.11 Physical tamper resistance and detection	2, 3, 4
	x				FSA-EDR 3.11 RE(1) Notification of a tampering attempt	3, 4
		x			FSA-HDR 3.11 Physical tamper resistance and detection	2, 3, 4
		x			FSA-HDR 3.11 RE(1) Notification of a tampering attempt	3, 4
			x		FSA-NDR 3.11 Physical tamper resistance and detection	2, 3, 4
			x		FSA-NDR 3.11 RE(1) Notification of a tampering attempt	3, 4
	x				FSA-EDR 3.12 Provisioning product supplier roots of trust - protection	2, 3, 4
		x			FSA-HDR 3.12 Provisioning product supplier roots of trust - protection	2, 3, 4
			x		FSA-NDR 3.12 Provisioning product supplier roots of trust - protection	2, 3, 4
	x				FSA-EDR 3.13A Provisioning asset owner roots of trust - protection	2, 3, 4
	x				FSA-EDR 3.13B Provisioning asset owner roots of trust - inside zone	2, 3, 4
		x			FSA-HDR 3.13A Provisioning asset owner roots of trust - protection	2, 3, 4
		x			FSA-HDR 3.13B Provisioning asset owner roots of trust - inside zone	2, 3, 4
			x		FSA-NDR 3.13A Provisioning asset owner roots of trust - protection	2, 3, 4
			x		FSA-NDR 3.13B Provisioning asset owner roots of trust - inside zone	2, 3, 4
	x				FSA-EDR 3.14 Integrity of the boot process	1, 2, 3, 4
	x				FSA-EDR 3.14 RE(1) Authenticity of the boot process	2, 3, 4
		x			FSA-HDR 3.14 Integrity of the boot process	1, 2, 3, 4

Software Application	Embedded Device	Host Device	Network Device	Section	Requirement ID and Reference Name	Capability Security Level
		x			FSA-HDR 3.14 RE(1) Authenticity of the boot process	2, 3, 4
			x		FSA-NDR 3.14 Integrity of the boot process	1, 2, 3, 4
			x		FSA-NDR 3.14 RE(1) Authenticity of the boot process	2, 3, 4
				FR 4 - Data Confidentiality		
x	x	x	x		FSA-CR 4.1A Information confidentiality - at rest	1, 2, 3, 4
x	x	x	x		FSA-CR 4.1B Information confidentiality - in transit	1, 2, 3, 4
x	x	x	x		FSA-CR 4.2 Information persistence	2, 3, 4
x	x	x	x		FSA-CR 4.2 RE(1) Erase of shared memory resources	3, 4
x	x	x	x		FSA-CR 4.2 RE(2) Erase verification	3, 4
x	x	x	x		FSA-CR 4.3 Use of cryptography	1, 2, 3, 4
				FR 5 - Restricted Data Flow		
x	x	x	x		FSA-CR 5.1 Network segmentation	1, 2, 3, 4
			x		FSA-NDR 5.2 Zone boundary protection	1, 2, 3, 4
			x		FSA-NDR 5.2 RE(1) Deny all, permit by exception	2, 3, 4
			x		FSA-NDR 5.2 RE(2) Island mode	3, 4
			x		FSA-NDR 5.2 RE(3) Fail close	3, 4
			x		FSA-NDR 5.3 General purpose person-to-person communication restrictions	1, 2, 3, 4
					FSA-CR 5.4 Application partitioning	
				FR 6 - Timely Response to Event		
x	x	x	x		FSA-CR 6.1 Audit log accessibility	1, 2, 3, 4
x	x	x	x		FSA-CR 6.1 RE(1) Programmatic access to audit logs	3, 4
x	x	x	x		FSA-CR 6.2 Continuous monitoring	2, 3, 4
				FR 7 - Resource Availability		
x	x	x	x		FSA-CR 7.1 Denial of service protection	1, 2, 3, 4
x	x	x	x		FSA-CR 7.1 RE(1) Manage communication load from component	2, 3, 4
x	x	x	x		FSA-CR 7.2 Resource management	1, 2, 3, 4
x	x	x	x		FSA-CR 7.3 Control system backup	1, 2, 3, 4
x	x	x	x		FSA-CR 7.3 RE(1) Backup integrity verification	2, 3, 4
x	x	x	x		FSA-CR 7.4 Control system recovery and reconstitution	1, 2, 3, 4
					FSA-CR 7.5 Emergency power	
x	x	x	x		FSA-CR 7.6 Network and security configuration settings	1, 2, 3, 4
x	x	x	x		FSA-CR 7.6 RE(1) Machine-readable reporting of current security settings	3, 4
x	x	x	x		FSA-CR 7.7 Least functionality	1, 2, 3, 4
x	x	x	x		FSA-CR 7.8 Control system component inventory	2, 3, 4

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CCSC 1A	Support of essential functions - account lock out	The components of the system shall adhere to specific constraints as described in clause 4 of IEC 62443-3-3 [11]. (For reference, the specific items from Clause 4 of IEC 62443-3-3 are copied below in this column, for rows FSA-CCSC 1A through 1H, with the first item following, in this cell.) Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically: - Accounts used for essential functions shall not be locked out, even temporarily (see 5.5, SR 1.3 – Account management, 5.6, SR 1.4 – Identifier management, 5.13, SR 1.11 – Unsuccessful login attempts and 6.7, SR 2.5 – Session lock).	Note that as part of their submissions for certification, the supplier will have identified the essential functions of the component in alignment with the definition in IEC 62443-4-2. Verify in design documentation that accounts used for essential functions shall not be locked out, even temporarily. Verify by testing that accounts used for essential functions are not locked out due to account management actions and locking functions implemented to meet FR 1. Record one of: a. Met b. Not met c. Not relevant - no essential functions	Yes	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
x	x	x	x	FSA-CCSC 1B	Support of essential functions - non-repudiation	Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically: - Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time (see 6.14, SR 2.12 – Non-repudiation).	Verify that the supplier has performed and documented analysis and testing to confirm that verifying and recording operator actions to enforce non-repudiation does not add significant delay to system response time (see FSA-CR 2.12 – Non-repudiation). Record one of: a. Met b. Not met c. Not relevant - no essential functions	No	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
x	x	x	x	FSA-CCSC 1C	Support of essential functions - failure of certificate authority	Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically: - For high availability control systems, the failure of the certificate authority shall not interrupt essential functions (see 5.10, SR 1.8 – Public key infrastructure (PKI) certificates).	If public key authentication is used by the component, determine by asking the supplier, if this is a high availability component. If public key authentication is used by the component and the supplier asserts it is a high availability component, verify that the supplier has a test case to confirm that the component maintains its essential functions upon failure of the certificate authority. Verify that this test has passed (See FSA-CR 1.8 – Public key infrastructure (PKI) certificates). Record one of: a. Met b. Not met If public key authentication is not used by the component, record: c. Not relevant - public key authentication not used If public key authentication is used but the supplier does not assert this is a high availability component, record: d. Not relevant - not high availability component, or no essential functions	No	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
	x			FSA-CCSC 1D	Support of essential functions - I&A and SIF initiation	Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically: - Identification and authentication shall not prevent the initiation of the SIF (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication).	If the component has a safety instrumented function (SIF), verify in design documentation that Identification and authentication does not prevent the initiation of the SIF (see FSA-CR 1.1 – Human user identification and authentication and FSA-CR 1.2 – Software process and device identification and authentication). Verify by testing that initiation of SIF occurs as designed regardless of the authentication state of component users. Record one of: a. Met b. Not met If the component does not have SIF, record: c. Not relevant	Yes	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
	x			FSA-CCSC 1E	Support of essential functions - authorization and SIF initiation	Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically: Authorization enforcement shall not prevent the initiation of the SIF (see 6.3, SR 2.1 – Authorization enforcement).	If the component has a safety instrumented function (SIF), verify in design documentation that authorization enforcement does not prevent the initiation of the SIF (see FSA-CR 2.1 – Authorization enforcement). Record one of: a. Met b. Not met If the component does not have SIF, record: c. Not relevant	No	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
x	x	x	x	FSA-CCSC 1F	Support of essential functions - incorrect timestamps	Incorrectly timestamped audit records (see 6.10, SR 2.8 – Auditable events and 6.13 SR 2.11 – Timestamps) shall not adversely affect essential functions.	Verify using design documentation that incorrectly timestamped audit records do not adversely affect essential functions. (See FSA-CR 2.8 - Auditable events and FSA-CR 2.11 Timestamps.) Record one of: a. Met b. Not met c. Not relevant - no essential functions	No	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
				FSA-CCSC 1G	Support of essential functions - zone isolation	Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode (see 9.4, SR 5.2 – Zone boundary protection).	There is no component level requirement associated with this requirement in IEC 62443-3-3, therefore there is no validation activity.		IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
	x			FSA-CCSC 1H	Support of essential functions - DoS and SIF initiation	A denial of service (DoS) event on the control system or safety instrumented system (SIS) network shall not prevent the SIF from acting (see 11.3, SR 7.1 – Denial of service protection).	If the component has a safety instrumented function (SIF), and requirement FSA-CR 7.1 Denial of service protection has been met, record one of the following as specified for that requirement, for the essential function SIF: a. Met b. Not met If the component does not have SIF, record: c. Not relevant	No	IEC 62443-4-2: CCSC 1	1, 2, 3, 4	
x	x	x	x	FSA-CCSC 2	Compensating countermeasures	There will be cases where one or more requirements specified in the document cannot be met without the assistance of a compensating countermeasure that is external to the component. When this is the case the documentation for that component shall describe the appropriate countermeasures applied by the system to allow the requirement to be met when the component is integrated into a system.	Identify any requirement derived from FR 1 - FR 7 such that: - it is applicable to the certification level, and - the result recorded for the validation activity in the present document is "Met by integration into system." If there are such requirements, verify for each one that the component documentation describes appropriate countermeasures applied by a system to allow the requirement to be met when the component is integrated into that system. Record one of: a. Met b. Not met If there are no requirements that meet these criteria, record: c. Not relevant	No	IEC 62443-4-2: CCSC 2	1, 2, 3, 4	
x	x	x	x	FSA-CCSC 3	Least privilege	When required and appropriate, one or more system components (software applications, embedded devices, host devices and network devices) shall provide the capability for the system to enforce the concept of least privilege. Individual system components shall provide the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability shall be available when required.	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	No	IEC 62443-4-2: CCSC 3	1, 2, 3, 4	
x	x	x	x	FSA-CCSC 4	Software development process	All of the components defined in this document shall be developed and supported following the secure product development processes described in IEC 62443-4-1 [12].	The SDLPA and SDA elements of certification verify this requirement. If those elements have passed per the criteria for those elements described in the certification criteria document for this evaluation (specification numbered 300), record: a. Met Otherwise, record: b. Not met	No	IEC 62443-4-2: CCSC 4	1, 2, 3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.1	Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 [11] SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	If the component has human users, verify that the component can identify and authenticate all users at all accessible interfaces, either locally or by integration into a system. Note that user identification and authentication may be role-based or group-based (such as, for some component interfaces, several users may share the same identity) Record one of: a. Met by component b. Met by integration into system c. Not met If the component has no human users, record: d. Not relevant	No	IEC 62443-4-2: CR 1.1	1, 2, 3, 4	All human users need to be identified and authenticated for all access to the component. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or physically keyed lids etc., and in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process. This requirement should be applied to both local and remote access to the component. This requirement comes in addition to the requirement of having such an authentication and identification at the system level. 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). User identification and authentication may be role-based or group-based (such as, for some component interfaces, several users may share the same identity). User identification and authentication should not hamper fast, local emergency actions. In order to support IAC policies, as defined according to IEC 62443-2-1 [5], the component should verify the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user should be enforced (see 6.3).
x	x	x	x	FSA-CR 1.1 RE(1)	Unique identification and authentication	Components shall provide the capability to uniquely identify and authenticate all human users.	If the component has human users, verify that the component can uniquely identify and authenticate all human users at all user accessible interfaces, either locally or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If the component has no human users, record: d. Not relevant	No	IEC 62443-4-2: CR 1.1 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 1.1 RE(2)	Multifactor authentication for all interfaces	Components shall provide the capability to employ multifactor authentication for all human user access to the component.	If the component has human users, verify that the component can provide the capability of multifactor authentication for all human users, either locally or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If the component has no human users, record: d. Not relevant	No	IEC 62443-4-2: CR 1.1 RE(2)	3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.2	Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to IEC 62443-3-3 [11] SR1.2. If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to IEC 62443-3-3 [11] SR1.1 may be part of the component identification and authentication process towards the other components.	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	No	IEC 62443-4-2: CR 1.2	2, 3, 4	*Note this requirement has been interpreted as intending identification and authentication by the component of other devices, as well as requiring identification and authentication of the component itself to other devices.* *"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 function of identification and authentication is to map a known identity to an unknown software process or device (henceforth referred to as an entity in 5.4.2) so as to make it known before allowing any data exchange. Allowing rogue entities to send and receive control system specific data can result in detrimental behavior of the control system. All entities should be identified and authenticated for all access to the control system. Authentication of the identity of such entities should be accomplished by using methods such as passwords, tokens or location (physical or logical). This requirement should be applied to both local and remote access to the control system. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technically infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied. Special attention needs to be made when identifying and authenticating portable and mobile devices. These types of devices are a known method of introducing undesired network traffic, malware and/or information exposure to control systems, including otherwise isolated networks. Where entities function as a single group, identification and authentication may be role-based, group-based or entity-based. It is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see clause 4 for a more complete discussion). For example, in common protection and control schemes, a group of devices jointly execute the protection functions and communicate with multicast messages among the devices in the group. In these cases, group authentication based on shared accounts or shared symmetric keys are commonly used. In order to support identification and authentication control policies as defined according to IEC 62443-2-1 [5], the control system verifies the identity of all entities as a first step. In a second step, the permissions assigned to the identified entity are enforced (see 6.3, CR 2.1 – Authorization enforcement)
x	x	x	x	FSA-CR 1.2 RE(1)	Unique identification and authentication	Components shall provide the capability to uniquely identify and authenticate itself to any other component.	Vendor shall provide list of all software processes and devices to which the component can connect. Verify that evidence exists that the component can provide a unique identification to each process and device to which the component can connect. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 1.2 RE(1)	3, 4	
x	x	x	x	FSA-CR 1.3	Account management	Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to IEC 62443-3-3 [11] SR 1.3.	If component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify component supports account management functions by an administrator type role to establish, activate, modify, disable and remove accounts, either directly or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If component does not provide the capability to identify and authenticate users of any type as described above, record: d. Not relevant	No	IEC 62443-4-2: CR 1.3	1, 2, 3, 4	A component may provide this capability by integrating into a higher level account management system. If the capability is not integrated into a higher level account management system then the component is expected to provide the capability natively. A common approach meeting this requirement would be a component that delegates the valuation of authentication to a directory server (for example, LDAP or Active Directory) which provides the account management capabilities required by IEC 62443-3-3 [11] SR 1.3. When a component integrates into a higher level system to provide the account management capabilities there needs to be consideration for the impact to the component in the event that the higher level system capability becomes unavailable.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.4	Identifier management	Components shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to IEC 62443-3-3 [11] SR 1.4.	If component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify user documents indicate that component allows managing identifiers by user, group, role and / or interface, either directly or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If component does not provide the capability to identify and authenticate users of any type as described above, record: d. Not relevant	No	IEC 62443-4-2: CR 1.4	1, 2, 3, 4	Accounts created under CR 1.3 – Account management require the use of one or more identifiers to distinctly identify each account. These identifiers must be unique and unambiguous as to the account with which they are associated. Some examples of identifiers in common use are account names, UNIX user ids, Microsoft Windows account globally unique identifiers (GUID), and bound X.509 certificates. A component may provide a local capability to associate identifiers with accounts. If the component is integrated into a system that enforces a system-wide security policy it is highly recommended that identifiers be associated with the same account across all components in the system. In order to accomplish this a component must be able to integrate into a system-wide identifier management capability.
x	x	x	x	FSA-CR 1.5A	Authenticator management - initialize authenticator content	Components shall provide the capability to support the use of initial authenticator content.	If component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify user documents indicate ability to define initial authenticator content. Record one of: a. Met b. Not met If component does not provide the capability to identify and authenticate users of any type as described above, record: c. Not relevant	No	IEC 62443-4-2: CR 1.5(a)	1, 2, 3, 4	In addition to an identifier (see 5.6) an authenticator is required to prove identity. Control system authenticators include, but are not limited to, tokens, symmetric keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys and key cards. There should be security policies in place instructing that human users must take reasonable measures to safeguard authenticators, including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others and reporting lost or compromised authenticators immediately. Authenticators have a lifecycle. When an account is created automatically a new authenticator needs to be created, in order for the account owner to be able to authenticate. For example, in a password-based system, the account has a password associated with it. Definition of the initial authenticator content could be interpreted as the administrator defining the initial password that the account management system sets for all new accounts. Being able to configure these initial values makes it harder for an attacker to guess the password between account creation and first account use (which should involve the setting of a new password by the account owner). Some control systems are installed with unattended installers that create all necessary accounts with default passwords and some embedded devices are shipped with default passwords. Over time, these passwords often become general knowledge and are documented on the Internet. Being able to change the default passwords protects the system against unauthorized users using default passwords to gain access. Passwords can be obtained from storage or from transmission when used in network authentication. The complexity of this can be increased by cryptographic protections such as encryption or hashing or by handshake protocols that do not require transmission of the password at all. Still, passwords might be subject to attacks, for example, brute force guessing or breaking the cryptographic protection of passwords in transit or storage. The window of opportunity can be reduced by changing/refreshing the passwords periodically. Similar considerations apply to authentication systems based on cryptographic keys. Enhanced protection can be achieved by using hardware mechanisms such as hardware security modules like trusted platform modules (TPMs). The management of authenticators should be specified in applicable security policies and procedures, for example, constraints to change default authenticators, refresh periods, specification of the protection of authenticators or firewall procedures. Besides the capabilities for authenticator management specified in this requirement, the strength of the authentication mechanism depends on the strength of the chosen authenticator (for example, password complexity or key length in public key authentication) and the policies for validating the authenticator in the authentication process (for example, how long a password is valid or which checks are performed in public key certificate validation). For the most common authentication mechanisms, password-based and public key authentication, 5.9, 5.10 and 5.11 provide further requirements. Use of components for some operations may be restricted, requiring additional authentication (such as, tokens, keys and certificates) in order to perform some functions.
x	x	x	x	FSA-CR 1.5B	Authenticator management - change default authenticators	Components shall provide the capability to support the recognition of changes to default authenticators made at installation time.	If component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify user documents indicate ability to change default authenticators (such as default passwords) at installation time. Verify by testing that the component recognizes these changes after installation as expected. Record one of: a. Met b. Not met If component does not provide the capability to identify and authenticate users of any type as described above, record: c. Not relevant	Yes	IEC 62443-4-2: CR 1.5(b)	1, 2, 3, 4	See FSA-CR 1.5A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.5C	Authenticator management - change/refresh all authenticators periodically	Components shall provide the capability to function properly with periodic authenticator change/refresh operation.	If component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify user documents indicate ability to function properly with changed/refreshed authenticators. Record one of: a. Met b. Not met If component does not provide the capability to identify and authenticate users of any type as described above, record: c. Not relevant	No	IEC 62443-4-2: CR 1.5(c)	1, 2, 3, 4	See FSA-CR 1.5A
x	x	x	x	FSA-CR 1.5D	Authenticator management - protect authenticators	Components shall provide the capability to protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.	If component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify design or user documents indicate ability to protect authenticators from unauthorized disclosure and modification when stored, used or transmitted by the component. Record one of: a. Met b. Not met If component does not provide the capability to identify and authenticate users of any type as described above, record: c. Not relevant	No	IEC 62443-4-2: CR 1.5(d)	1, 2, 3, 4	See FSA-CR 1.5A
x	x	x	x	FSA-CR 1.5 RE(1)	Hardware security for authenticators	The authenticators on which the component rely shall be protected via hardware mechanisms.	Verify user or design documents indicate ability to protect relevant authenticators with hardware mechanisms. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 1.5 RE(1)	3, 4	
			x	FSA-NDR 1.6	Wireless access management	A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	If the network device supports wireless access management, verify that the network device can identify and authenticate all users (humans, software processes, or devices) engaged in wireless communication. Note that user identification and authentication may be role-based or group-based (such as, for some component interfaces, several users may share the same identity). Record one of: a. Met b. Not met If the network device does not support wireless access management, record: c. Not relevant	No	IEC 62443-4-2: NDR 1.6	1, 2, 3, 4	Any wireless technology can, and in most cases should, be considered just another communication protocol option. Thus, it should be subject to the same IACS security requirements as any other communication type utilized by the IACS. However, from a security point of view, there is at least one significant difference between wired and wireless communications. Physical security countermeasures are typically less effective when using wireless.
			x	FSA-NDR 1.6 RE(1)	Unique identification and authentication	The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	If the network device supports wireless communication, verify that the network device can uniquely identify and authenticate all users (humans, software processes, or devices) engaged in wireless communication. Record one of: a. Met b. Not met If the network device does not support wireless communication, record: c. Not relevant	No	IEC 62443-4-2: NDR 1.6 RE(1)	2, 3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.7	Strength of password-based authentication	For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.	If the component utilizes password-based authentication, verify user documents indicate that configurable password strength can be enforced that meets internationally recognized and proven guidelines, either directly or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If the component does not utilize password-based authentication, record: d. Not relevant	No	IEC 62443-4-2: CR 1.7	1, 2, 3, 4	The ability to enforce configurable password strength, whether it is based on minimum length, variety of characters, or duration of time (the minimum being a one-time password) is necessary to assist in increasing the overall security of user chosen passwords. Generally accepted practices and recommendations can be found in documents such as NIST SP800-63-2, *Electronic Authentication Guideline* [27].
x	x	x	x	FSA-CR 1.7 RE(1)	Password generation and lifetime restrictions for human users	Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.	If the component utilizes password-based authentication, verify user documents indicate that password use for human users can be limited to a specified lifetime, and re-use can be limited to a configurable number of generations, either directly or by integration into a system. Verify a source for the commonly accepted practices followed. Record one of: a. Met by component b. Met by integration into system c. Not met If the component does not utilize password-based authentication, record: d. Not relevant	No	IEC 62443-4-2: CR 1.7 RE(1)	3, 4	
x	x	x	x	FSA-CR 1.7 RE(2)	Password lifetime restrictions for all users (human, software process, or device)	Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.	If the component utilizes password-based authentication, verify user documents indicate that the component supports the capability to enforce password minimum and maximum lifetime restrictions for all types of users that support password based authentication (humans, software processes, devices), either directly or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If the component does not utilize password-based authentication, record: d. Not relevant	No	IEC 62443-4-2: CR 1.7 RE(2)	4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.8	Public key infrastructure (PKI) certificates	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3-3 [11] SR1.8.	Review user documentation and determine if public key authentication is used by the component. This includes use of X509 certificates or other trust models (e.g. PGP). For reference, IEC 62443-3-3 SR 1.8 states: "Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI." SR 1.8 has accompanying rationale also included in IEC 62443-4-2 for CR 1.8, and shown in the present document in the "Rationale and Supplemental Guidance" column to the right. If public key authentication is used, for certificates not obtained from an existing PKI, verify user documents indicate that the required public key infrastructure practices per SR 1.8 are supported, either directly or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If public key authentication is not used by the component, record: d. Not relevant	No	IEC 62443-4-2: CR 1.8	2, 3, 4	The selection of an appropriate PKI should consider the organization's certificate policy which should be based on the risk associated with a breach of confidentiality of the protected information. Guidance on the policy definition can be found in commonly accepted standards and guidelines, such as the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 [31] for X.509-based PKI. For example, the appropriate location of a certification authority (CA), whether within the control system versus on the Internet, and the list of trusted CAs should be considered in the policy and depends on the network architecture (see also IEC 62443‑2‑1 [5]).
x	x	x	x	FSA-CR 1.9A	Strength of public key-based authentication - check validity of signature of a given certificate	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to 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 public key authentication is used, verify in user documentation that signature validity can be determined, either directly or by integration into a system, without communicating outside the same IACS environment, such as out to the Internet or to a less secure IACS zone. If the component directly supports the capability, also verify with the following test in an environment without an Internet connection. Provide a certificate with an invalid signature to the component. Verify that this problem is detected and reported to the user. Record one of: a. Met by component b. Met by integration in system c. Not met If public key authentication is not used, record: d. Not relevant	Yes	IEC 62443-4-2: CR 1.9(a)	2, 3, 4	To meet the requirements in 5.11.1 does not necessarily require a real time connection to a certificate authority. Alternative out-of-band methods may be used to meet the requirements in 5.11.1. For example, a disconnected system could install and update certifications using manual out-of-band processes. Public/private key cryptography strongly depends on the secrecy of a given subject's private key and proper handling of the trust relationships. When verifying a trust between two entities based on public key authentication, it is essential to trace the public key certificate to a trusted entity. A common implementation error in certificate validation is to only check the validity of a certificate's signature, but not checking the trust in the signer. In a PKI setting, a signer is trusted if they are a trusted CA or have a certificate issued by a trusted CA, thus all verifiers need to trace certificates presented to them back to a trusted CA. If such a chain of trusted CAs cannot be established, the presented certificate should not be trusted. If self-signed certificates are used instead of a PKI, the certificate subject itself signed its certificate, thus there never is a trusted third-party or CA. This should be compensated by deploying the self-signed public key certificates to all peers that need to validate them via an otherwise secured mechanism (for example, configuration of all peers in a trusted environment). Trusted certificates need to be distributed to peers through secure channels. During the validation process, a self-signed certificate should only be trusted if it is already present in the list of trusted certificates of the validating peer. The set of trusted certificates should be configured to the minimum necessary set. In both cases, validation needs to also consider the possibility that a certificate is revoked. In a PKI setting this is typically done by maintaining certificate revocation lists (CRLs) or running an online certificate status protocol (OCSP) server. When revocation checking is not available due to control system constraints, mechanisms such as a short certificate lifetime can compensate for the lack of timely revocation information. Note that short lifetime certificates can sometimes create significant operational issues in a control system environment. It is expected that most components will integrate into an IACS and leverage the key authentication mechanisms provided by the underlying IACS. When implementing public key authentication at the component-level of an IACS, protection of the key becomes a primary concern and objective of key storage on that component. Care should be taken in the implementation to assure that any private keys stored within the component cannot be retrieved or tampered with (See 5.7, CR 1.5 – Authenticator management). NOTE Tamper resistant design methodologies and technologies are available to assist with designing a secure private key protection mechanism.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.9B	Strength of public key-based authentication -validate certificate chain	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued.	Review user documentation and determine if public key authentication is used. If public key authentication is used, review design documentation and determine if the component has the capability, either directly or by integration into a system, to validate the certificate chain without communicating outside the same IACS environment or in the case of self-signed certificates, by deploying leaf certificates to all nodes which communicate with the subject to which the certificate is issued. Examples of communication outside the same IACS environment are communication to the Internet or to a less secure IACS zone. Record one of: a. Met by component b. Met by integration with system c. Not met If public key authentication is not used, record: d. Not relevant	No	IEC 62443-4-2: CR 1.9(b)	2, 3, 4	See FSA-CR 1.9A
x	x	x	x	FSA-CR 1.9C	Strength of public key-based authentication - check certificate's revocation status	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to validate certificates by checking a given certificate's revocation status.	Review user documentation and determine if public key authentication is used. If public key authentication is used, verify in user documentation that the component has the capability, either directly or by integration into a system, to check certification revocation status without communication outside the same IACS environment, such as to the Internet or a less secure IACS zone. If the component directly supports the capability, also verify with the following test in an environment without an Internet connection. Provide a certificate with a revoked status. Verify that the problem is detected and reported to the user. Record one of: a. Met by component b. Met by integration into system c. Not met If public key authentication is not used, record: d. Not relevant	Yes	IEC 62443-4-2: CR 1.9(c)	2, 3, 4	See FSA-CR 1.9A
x	x	x	x	FSA-CR 1.9D	Strength of public key-based authentication - establish user control of private key	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to 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 public key authentication is used, examine user documents to verify that key pairs may be generated either directly or by integration into a system, without communicating outside the same IACS environment, such as to the Internet or a less trusted IACS zone. Verify by review of user and design documents that corresponding private keys are only accessible by the owner of the key, whether human, software process, or device. Record one of: a. Met by component b. Met by integration into system c. Not met If public key authentication is not used, record: d. Not relevant	No	IEC 62443-4-2: CR 1.9(d)	2, 3, 4	See FSA-CR 1.9A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.9E	Strength of public key-based authentication - map authenticated identity to a user	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to map the authenticated identity to a user (human, software process or device).	Review user documentation and determine if public key authentication is used. If public key authentication is used, examine user documents to verify that an identity authenticated by public key authentication is mapped to a component user (human, software process, or device), without communicating outside the same IACS environment, such as to the Internet or a less trusted IACS zone. Record one of: a. Met by component b. Met by integration into system c. Not met If public key authentication is not used, record: d. Not relevant	No	IEC 62443-4-2: CR 1.9(e)	2, 3, 4	See FSA-CR 1.9A
x	x	x	x	FSA-CR 1.9F	Strength of public key-based authentication - use of cryptography	For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to ensure that the algorithms and keys used for the public key authentication comply with CR 4.3 – Use of cryptography.	Review user documentation and determine if public key authentication is used. If public key authentication is used, review design documentation to verify that the component provides the capability either directly or by integration into a system, and without communication outside the same IACS environment, to ensure that algorithms and keys used for this comply with FSA-CR 4.3 - Use of cryptography. Examples of communication outside the same IACS environment are communication to the Internet or to a less secure IACS zone. Record one of: a. Met by component b. Met by integration into system c. Not met If public key authentication is not used, record: d. Not relevant	No	IEC 62443-4-2: CR 1.9(f)	2, 3, 4	See FSA-CR 1.9A
x	x	x	x	FSA-CR 1.9 RE(1)	Hardware security for public key-based authentication	Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms.	Review user documentation and determine if public key authentication is used. If public key authentication is used, review design documentation to verify that hardware mechanisms are used to protect critical long-lived private keys, either directly by the component or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met If public key authentication is not used, record: d. Not relevant	No	IEC 62443-4-2: CR 1.9 RE(1)	3, 4	
x	x	x	x	FSA-CR 1.10	Authenticator feedback	When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authenticator information during the authentication process.	If the component locally provides an authentication capability, verify component is capable of obscuring feedback of authentication information. Record one of: a. Met b. Not met If the component does not locally provide an authentication capability record: c. Not relevant	No	IEC 62443-4-2: CR 1.10	1, 2, 3, 4	Obscuring feedback protects the information from possible exploitation by unauthorized individuals, for example, displaying asterisks or other random characters when a human user types in a username and/or password obscures feedback of authentication information. Other examples include the entry of secure socket shell (SSH) token entry and one-time passwords. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as "unknown user name."

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.11A	Unsuccessful login attempts - limit number	When a component provides an authentication capability the component 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.	If the component locally provides an authentication capability, verify component is capable of enforcing a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. Record one of: a. Met b. Not met If the component does not locally provide an authentication capability, record: c. Not relevant	No	IEC 62443-4-2: CR 1.11(a)	1, 2, 3, 4	Due to the potential for denial of service, the number of consecutive invalid access attempts may be limited. If enabled, the application or device may automatically reset to zero the number of access attempts after a predetermined time period established by the applicable security policies and procedures. Resetting the access attempts to zero will allow users (human, software process or device) to gain access if they have the correct login credentials. Automatic denial of access for control system operator workstations or nodes should not be used when immediate operator responses are required in emergency situations. All lockout mechanisms should consider functional requirements for continuous operations so as to mitigate adverse denial of service operating conditions which could result in system failures or compromising the safety of the system. Allowing interactive logins to an account used for critical services could provide a potential for denial of service or other abuse.
x	x	x	x	FSA-CR 1.11B	Unsuccessful login attempts - response	When a component provides an authentication capability the component shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.	If the component locally provides an authentication capability, verify component is capable of denying access for a specified period of time or until unlocked by an administrator when a configured limit for unsuccessful login attempts has been reached. Record one of: a. Met b. Not met If the component does not locally provide an authentication capability, record: c. Not relevant	No	IEC 62443-4-2: CR 1.11(b)	1, 2, 3, 4	See FSA-CR 1.11A
x	x	x	x	FSA-CR 1.12	System use notification	When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.	If component provides local human use access/HMI, verify component is capable of displaying user configurable system use notifications before authenticating. Record one of: a. Met b. Not met If the component does not provide local human use access/HMI, record: c. Not relevant	No	IEC 62443-4-2: CR 1.12	1, 2, 3, 4	Privacy and security policies and procedures need to be consistent with applicable laws, directives, policies, regulations, standards and guidance. Often, the main justification for this requirement is legal prosecution of violators and proving intentional breach. This capability is thus necessary to support policy requirements, and might improve IACS security because it can be used as a deterrent. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the control system. A warning banner implemented as a posted physical notice in the control system facility does not protect against remote login issues. Examples of elements for inclusion in the system use notification message are: a) that the individual is accessing a system owned by the asset owner; b) that system usage may be monitored, recorded and subject to audit; c) that unauthorized use of the system is prohibited and subject to criminal and/or civil penalties; and d) that use of the system indicates consent to monitoring and recording.
			x	FSA-NDR 1.13	Access via untrusted networks	The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.	Unless the supplier has documented that a network device is not intended to support access into a network via an untrusted network, verify that the network device has the capability to inspect all network traffic that accesses the device, where that inspection determines whether the network device takes action to control the traffic. Examples of control actions supported may include rerouting the traffic or dropping it. Methods of access to the network device subject to this requirement shall include but are not limited to, dial-up, broadband, and wireless. Record one of: a. Met b. Not met If the supplier has documented that a network device may not be used to support access into a network, record: c. Not relevant	No	IEC 62443-4-2: NDR 1.13	1, 2, 3, 4	The network device should protect against unauthorized connections or subversion of authorized connections. Examples of access to the network device via untrusted networks typically include remote access methods (such as, dial-up, broadband and wireless) as well as connections from a company's office (non-control system) network. The network device may provide ACL (Access Control List) functionality to restrict access by: Layer 2 forwarding devices such as Ethernet switches: a) MAC address b) VLAN Layer 3 forwarding devices such as routers, gateways and firewalls: a) IP address b) Port and protocol c) Virtual Private Networks
			x	FSA-NDR 1.13 RE(1)	Explicit access request approval	The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.	Verify by test that: the network device may assign a user to a role approving untrusted networks for access to the network device, and that networks so approved are permitted access, and other networks are not.	Yes	IEC 62443-4-2: NDR 1.13 RE(1)	3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 1.14A	Strength of symmetric key-based authentication - establish trust	For components that utilize symmetric keys, the component shall provide the capability to establish the mutual trust using the symmetric key.	Review user documentation and determine if symmetric key authentication is used. If symmetric key authentication is used, verify user documents indicate ability for the component to establish mutual trust using the symmetric key. Record one of: a. Met b. Not met If symmetric key authentication is not used, record: c. Not relevant	No	IEC 62443-4-2: CR 1.14(a)	2, 3, 4	Means should be defined for installing the keys into the component. This may include installing and managing the component key using out-of-band methods. This is necessary since a compromise of any symmetric keys that are stored within the component could lead to a full compromise of the system using those keys. In practice, there are two basic ways to perform the secure authentication of a device to another: either using asymmetric cryptography (see 5.11) or by using symmetric cryptography. The choice between asymmetric and symmetric is dictated by several criteria, like key management, trust provisioning, legacy support and efficiency. Examples of symmetric key authentication schemes are Needham-Schröder or Kerberos. When symmetric key authentication is used, the party uses a secret key they have learned in the past (for example, through trust provisioning). The party proves their claimed identity by proving knowledge of the secret key (for example, by answering a challenge submitted by the other party, the examiner). The examiner has the knowledge of the same secret (also learned in the past through trust provisioning) and is able to compute the answer to the challenge performing the same cryptographic operations as the prover. The examiner can then compare the answer of the prover with its own computation. If they match, the examiner is convinced that the prover is the one they claim to be and the process can be conducted the other way around, switching roles, to achieve mutual-authentication. This mechanism is secure only if the shared secret is only known by the prover and the examiner and if the secret is diversified per prover. One instance of such a mechanism is the proper use of cipher-based message authentication code (CMAC) computations or alternatively the Galois counter mode (GCM)/Galois message authentication code (GMAC) operation modes.
x	x	x	x	FSA-CR 1.14B	Strength of symmetric key-based authentication - secure storage for shared secret	For components that utilize symmetric keys, the component shall provide the capability to store securely the shared secret (the authentication is valid as long as the shared secret remains secret).	Review user documentation and determine if symmetric key authentication is used. If symmetric key authentication is used, verify user and design documents indicate ability to protect the shared secret from unauthorized disclosure. Record one of: a. Met b. Not met If symmetric key authentication is not used, record: c. Not relevant	No	IEC 62443-4-2: CR 1.14(b)	2, 3, 4	See FSA-CR 1.14A
x	x	x	x	FSA-CR 1.14C	Strength of symmetric key-based authentication - restrict access to shared secret	For components that utilize symmetric keys, the component shall provide the capability to restrict access to the shared secret.	Review user documentation and determine if symmetric key authentication is used. If symmetric key authentication is used, verify design and user documents indicate ability to protect the shared secret from unauthorized use or modification Record one of: a. Met b. Not met If symmetric key authentication is not used, record: c. Not relevant	No	IEC 62443-4-2: CR 1.14(c)	2, 3, 4	See FSA-CR 1.14A
x	x	x	x	FSA-CR 1.14D		For components that utilize symmetric keys, the component shall provide the capability to ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3 – Use of cryptography Subclause 8.5.	Review user documentation and determine if symmetric key authentication is used. If symmetric key authentication is used, review design documentation to verify that the component provides the capability to ensure that algorithms and keys used for this comply with FSA-CR 4.3 - Use of cryptography. Record one of: a. Met b. Not met If symmetric key authentication is not used, record: c. Not relevant	No	IEC 62443-4-2: CR 1.14(d)	2, 3, 4	See FSA-CR 1.14A
x	x	x	x	FSA-CR 1.14 RE(1)	Hardware security for symmetric key-based authentication	Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.	Review user documentation and determine if symmetric key authentication is used. If symmetric key authentication is used, review design documentation to verify that hardware mechanisms are used to protect critical long-lived symmetric keys. Record one of: a. Met b. Not met If symmetric key authentication is not used, record: c. Not relevant	No	IEC 62443-4-2: CR 1.14 RE(1)	3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 2.1	Authorization enforcement	Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.	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	No	IEC 62443-4-2: CR 2.1	1, 2, 3, 4	Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains). After the control system has verified the identity of a user (human, software process or device) (see 5.3, CR 1.1 – Human user identification and authentication and 5.4, CR 1.2 – Software process and device identification and authentication), it also has to verify that a requested operation is actually permitted according to the defined security policies and procedures. For example, in a role-based access control policy, the control system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system. Planned or unplanned changes to control system components can have significant effects on the overall security of the control system. Accordingly, only qualified and authorized individuals should obtain the use of control system components for purposes of initiating changes, including upgrades and modifications.
x	x	x	x	FSA_CR 2.1	Authorization enforcement		Further notes on above validation activity: 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	NA	IEC 62443-4-2: CR 2.1	1,2,3,4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA_CR 2.1	Authorization enforcement		Further notes on above validation activity, continued: •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)	NA	IEC 62443-4-2: CR 2.1	1, 2, 3, 4	
x	x	x	x	FSA-CR 2.1 RE(1)	Authorization enforcement for all users (humans, software processes and devices)	Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.	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	No	IEC 62443-4-2: CR 2.1 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 2.1 RE(2)	Permission mapping to roles	Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.	If the component provides the capability to identify and authenticate users of any type (humans, software processes or devices), either directly or by integration into a system, verify component provides the capability to map permissions to roles for these users by an authorized supervisory level account, either directly or through a compensating security mechanism. Record one of: a. Met by component b. Met by a compensating security mechanism c. Not met If the component does not provide the capability to identify and authenticate users of any type as described, record: d. Not relevant	No	IEC 62443-4-2: CR 2.1 RE(2)	2, 3, 4	
x	x	x	x	FSA-CR 2.1 RE(3)	Supervisor override	Components shall support a supervisor manual override for a configurable time or sequence of events.	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	No	IEC 62443-4-2: CR 2.1 RE(3)	3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 2.1 RE(4)	Dual approval	Components shall support dual approval when action can result in serious impact on the industrial process.	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	No	IEC 62443-4-2: CR 2.1 RE(4)	4	
x	x	x	x	FSA-CR 2.2	Wireless use control	If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.	If the component supports usage through wireless interfaces, verify with user documentation that the component can integrate into a system to authorize usage, monitor, and enforce usage restrictions for wireless connectivity to the component per commonly accepted security practices. Record one of: a. Met b. Not met If the component does not support usage through wireless interfaces, record: c. Not relevant	No	IEC 62443-4-2: CR 2.2	1, 2, 3, 4	Wireless use control may be implemented in different devices that make up the system. Network devices may be one of the devices that assist with use control through controls such as network admission control. For devices and applications that utilize wireless networks those devices should be able to properly utilize wireless network protection such as network admission control. Components may also implement different limitations on access based on whether the access is from wireless devices or wired devices. This does place a need that the component be able to distinguish whether the interface is through wireless or not. Some network devices provide the capability to scan for unauthorized wireless network activity in the wireless spectrum. In order to prevent a negative impact on the performance of the control system functionality, it is a good practice to deploy dedicated devices to perform checks for unauthorized network activity.
				FSA-CR 2.3	Use control for portable and mobile devices	There is no component level requirement associated with IEC 62443-3-3 SR 2.3.	No validation activity		IEC 62443-4-2: CR 2.3		
x				FSA-SAR 2.4A	Mobile code - control execution	In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the software application, action to control execution of mobile code.	Review user documentation and determine if the software application uses mobile code technologies. If the software application uses mobile code technologies, review user documentation and verify that the application provides the capability to enforce a security policy for the usage of mobile code technologies. Verify that a policy is supported at a minimum, that prevents each mobile code technology used, from being executed, when initiated by the software application, on the hosting device. Record one of: a. Met b. Not met If the software application does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: SAR 2.4(a)	1, 2, 3, 4	Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.
x				FSA-SAR 2.4B	Mobile code - control transfer by user	In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the software application, action to control which users (human, software process, or device) are allowed to transfer mobile code to/from the application.	Review user documentation and determine if the software application uses mobile code technologies. If the software application uses mobile code technologies, review component documentation and verify that there is a mechanism to control, for each mobile code technology, which users (human, software process, or device) are allowed to transfer mobile code to/from the application. Record one of: a. Met b. Not met If the software application does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: SAR 2.4(b)	1, 2, 3, 4	See FSA-SAR 2.4A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x				FSA-SAR 2.4C	Mobile code - integrity check	In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the software application, action to control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Review user documentation and determine if the software application uses mobile code technologies. If the software application uses mobile code technologies, review component documentation and verify that there is a policy mechanism to require that an integrity check must run and pass prior to mobile code execution, for each mobile technology used. Record one of: a. Met b. Not met If the software application does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: SAR 2.4(c)	1, 2, 3, 4	See FSA-SAR 2.4A
x				FSA-SAR 2.4 RE(1)	Mobile code authenticity check	The application shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Review user documentation and determine if the software application uses mobile code technologies. If the software application uses mobile code technologies, review component documentation and verify that there is that there is a policy mechanism to require that an authenticity check must run and pass prior to mobile code execution. Record one of: a. Met b. Not met If the software application does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: SAR 2.4 RE(1)	2, 3, 4	
	x			FSA-EDR 2.4A	Mobile code - control execution	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the embedded device, action to control execution of mobile code.	Review user documentation and determine if the embedded device uses mobile code technologies. If the embedded device uses mobile code technologies, review user documentation and verify that the embedded device provides the capability to enforce a security policy for the usage of mobile code technologies. Verify that a policy is supported at a minimum, that prevents each mobile code technology used from being executed on the device. Record one of: a. Met b. Not met If the embedded device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: EDR 2.4(a)	1, 2, 3, 4	Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.
	x			FSA-EDR 2.4B	Mobile code - control upload by user	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the embedded device, action to control which users (human, software process, or device) are allowed to upload mobile code to the device.	Review user documentation and determine if the embedded device uses mobile code technologies. If the embedded device uses mobile code technologies, review component documentation and verify that there is a mechanism to control, for each mobile code technology, which users (human, software process, or device) are allowed to upload mobile code to the device. Record one of: a. Met b. Not met If the embedded device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: EDR 2.4(b)	1, 2, 3, 4	See FSA-EDR 2.4A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
	x			FSA-EDR 2.4C	Mobile code - integrity check	In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the embedded device, action to control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Review user documentation and determine if the embedded device uses mobile code technologies. If the embedded device uses mobile code technologies, review component documentation and verify that there is a policy mechanism to require that an integrity check must run and pass prior to mobile code execution, for each mobile technology used. Record one of: a. Met b. Not met If the embedded device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: EDR 2.4(c)	1, 2, 3, 4	See FSA-EDR 2.4A
	x			FSA-EDR 2.4 RE(1)	Mobile code authenticity check	The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Review user documentation and determine if the embedded device uses mobile code technologies. If the embedded devices uses mobile code technologies, review component documentation and verify that there is that there is a policy mechanism to require that an authenticity check must run and pass prior to mobile code execution. Record one of: a. Met b. Not met If the embedded device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: EDR 2.4 RE(1)	2, 3, 4	
		x		FSA-HDR 2.4A	Mobile code - control execution	In the event that a host device utilizes mobile code technologies, the host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the host device, action to control execution of mobile code.	Review user documentation and determine if the host device uses mobile code technologies. If the host device uses mobile code technologies, review user documentation and verify that the host device provides the capability to enforce a security policy for the usage of mobile code technologies. Verify that a policy is supported at a minimum, that prevents each mobile code technology used from being executed on the host device. Record one of: a. Met b. Not met If the host device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: HDR 2.4(a)	1, 2, 3, 4	Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the host device resides. For example, mobile code exchanges may be disallowed directly with the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.
		x		FSA-HDR 2.4B	Mobile code - control upload by user	In the event that a host device utilizes mobile code technologies, the host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the host device, action to control which users (human, software process, or device) are allowed to upload mobile code to the host device.	Review user documentation and determine if the host device uses mobile code technologies. If the host device uses mobile code technologies, review component documentation and verify that there is a mechanism to control, for each mobile code technology, which users (human, software process, or device) are allowed to upload mobile code to the host device. Record one of: a. Met b. Not met If the host device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: HDR 2.4(b)	1, 2, 3, 4	See FSA-HDR 2.4A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
		x		FSA-HDR 2.4C	Mobile code - integrity check	In the event that a host device utilizes mobile code technologies, the host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the host device, action to control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Review user documentation and determine if the host device uses mobile code technologies. If the host device uses mobile code technologies, review component documentation and verify that there is a policy mechanism to require that an integrity check must run and pass prior to mobile code execution, for each mobile technology used. Record one of: a. Met b. Not met If the host device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: HDR 2.4(c)	1, 2, 3, 4	See FSA-HDR 2.4A
		x		FSA-HDR 2.4 RE(1)	Mobile code authenticity check	The host device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Review user documentation and determine if the host device uses mobile code technologies. If the host devices uses mobile code technologies, review component documentation and verify that there is that there is a policy mechanism to require that an authenticity check must run and pass prior to mobile code execution. Record one of: a. Met b. Not met If the host device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: HDR 2.4 RE(1)	2, 3, 4	
			x	FSA-NDR 2.4A	Mobile code - control execution	In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the network device, action to control execution of mobile code.	Review user documentation and determine if the network device uses mobile code technologies. If the network device uses mobile code technologies, review user documentation and verify that the network device provides the capability to enforce a security policy for the usage of mobile code technologies. Verify that a policy is supported at a minimum, that prevents each mobile code technology used from being executed on the network device. Record one of: a. Met b. Not met If the network device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: NDR 2.4(a)	1, 2, 3, 4	Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel. Mobile code could be secured by adding integrity, authenticity, and authorization checks to the code itself (application layer), or for “just-in-time” code execution through transmitting the mobile code via a secure communications tunnel which provides these attributes, or any mechanism equivalent to these options.
			x	FSA-NDR 2.4B	Mobile code - control transfer by user	In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the network device, action to control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device.	Review user documentation and determine if the network device uses mobile code technologies. If the network device uses mobile code technologies, review component documentation and verify that there is a mechanism to control, for each mobile code technology, which users (human, software process, or device) are allowed to transfer mobile code to/from the network device. Record one of: a. Met b. Not met If the network device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: NDR 2.4(b)	1, 2, 3, 4	See FSA-NDR 2.4A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 2.4C	Mobile code - integrity check	In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, for each mobile code technology used on the network device, action to control the execution of mobile code based on the results of an integrity check prior to the code being executed.	Review user documentation and determine if the network device uses mobile code technologies. If the network device uses mobile code technologies, review component documentation and verify that there is a policy mechanism to require that an integrity check must run and pass prior to mobile code execution, for each mobile technology used. Record one of: a. Met b. Not met If the network device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: NDR 2.4(c)	1, 2, 3, 4	See FSA-NDR 2.4A
			x	FSA-NDR 2.4 RE(1)	Mobile code authenticity check	The network device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.	Review user documentation and determine if the network device uses mobile code technologies. If the network devices uses mobile code technologies, review component documentation and verify that there is that there is a policy mechanism to require that an authenticity check must run and pass prior to mobile code execution. Record one of: a. Met b. Not met If the network device does not use mobile code technologies, record: c. Not relevant	No	IEC 62443-4-2: NDR 2.4 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 2.5A	Session lock - initiation	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device).	Review user documentation and determine if the component provides a human user interface, which may be accessed locally or via a network. If the component provides a user interface, verify user documents include evidence that the component provides the capability to initiate a session lock for a human user triggered by one of: session inactivity longer than a configurable time period or manual initiation by the human user owning the session. Record one of: a. Met b. Not met If the component does not provide a human user interface, record: c. Not relevant	No	IEC 62443-4-2: CR 2.5(a)	1, 2, 3, 4	Session locks are used to prevent access to specified workstations or nodes. Components should activate session lock mechanisms automatically after a configurable time period. In most cases, the session locks are configured at the system level. Session locks implemented as part of this requirement may be pre-empted or limited by remote session termination, as defined in CR 2.6 – Remote session termination.
x	x	x	x	FSA-CR 2.5B	Session lock - removal	If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.	Review user documentation and determine if the component provides a human user interface, which may be accessed locally or via a network. If the component provides a human user interface, verify user documents include evidence that the component provides the capability for a session lock, once initiated for any type of user session (human, software process, or device), to remain in effect until either a human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures. Record one of: a. Met b. Not met If the component does not provide a human user interface, record: c. Not relevant	No	IEC 62443-4-2: CR 2.5(b)	1, 2, 3, 4	See FSA-CR 2.5A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 2.6	Remote session termination	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.	Review user documentation and determine if the component supports remote sessions. If the component supports remote sessions, verify the component has at least one of these capabilities: it is able to be configured to automatically terminate a remote session after a configurable time period of inactivity, or a local authority may terminate a remote session. Record one of: a. Met b. Not met If the component does not support remote sessions, record: c. Not relevant	No	IEC 62443-4-2: CR 2.6	2, 3, 4	A remote session is initiated whenever a component is accessed across the boundary of a zone defined by the asset owner based on their risk assessment. This requirement may be limited to sessions that are used for component monitoring and maintenance activities (not critical operations) based on the risk assessment of the control system and security policies and procedures. Some components may not allow sessions to be terminated as the session might be part of an essential function of the component.
x	x	x	x	FSA-CR 2.7	Concurrent session control	Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	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	Yes	IEC 62443-4-2: CR 2.7	3, 4	A resource starvation DoS might occur if a limit is not imposed. There is a trade-off between potentially locking out a specific user versus locking out all users and services due to a lack of resources. Product supplier and/or system integrator guidance is likely required to provide sufficient information as to how the number of concurrent sessions value should be assigned.
x	x	x	x	FSA-CR 2.8A	Auditable events - categories	Components shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, control system events, backup and restore event, configuration changes, and audit log events.	Verify via user documentation that the component supports capability to generate audit records relevant to security for the following categories: access control, request errors, control system events, backup and restore events, configuration changes, and audit log events. Verify via sample logs that some records from each of these categories are generated. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 2.8(a)-(f) first sentence	1, 2, 3, 4	Devices may contain either embedded firmware or run an OS. While the intent of the requirement is to cover categories of events, at least all events from the above categories that can be generated by the firmware or OS are to be included. NOTE Security event categories are only applicable if functionality itself is provided by the component.
x	x	x	x	FSA-CR 2.8B	Auditable events - data fields	Individual audit records shall include timestamp, source (originating device, software process or human user account), category, type, event ID, and event result.	Verify via user documentation that all audit records in the categories listed in FSA-CR 2.8A include timestamp, source (originating device, software process or human user account), category, type, event ID, and event result. Verify via sample logs that all of these fields have values present for all categories of records. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 2.8(a)-(f) second sentence	1, 2, 3, 4	See FSA-CR 2.8A
x	x	x	x	FSA-CR 2.9A	Audit storage capacity - allocation	Components shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management.	Verify that the capacity for audit record storage on the device is documented, and that the device provides this capacity. Verify that evidence exists that the supplier performed analysis to confirm that the capacity will meet business and regulatory requirements of users. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 2.9(a)	1, 2, 3, 4	Components should provide sufficient audit storage capacity, taking into account retention policy, the auditing to be performed and the online audit processing requirements. Components may rely on the system into which they are integrated to provide the majority of audit storage capacity. However, the components should provide enough local storage to buffer audit data until it can be sent to the system. Guidelines to be considered may include NIST Special Publication (SP) 800-92 [26]. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.
x	x	x	x	FSA-CR 2.9B	Audit storage capacity - exceeded	Components shall provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.	Review design documentation or perform testing to verify that all functions of the component are maintained when it reaches or exceeds audit storage capacity. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 2.9(b)	1, 2, 3, 4	See FSA-CR 2.9A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 2.9 RE(1)	Warn when audit record storage capacity threshold reached	Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.	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	No	IEC 62443-4-2: CR 2.9 RE(1)	3, 4	
x	x	x	x	FSA-CR 2.10A	Response to audit processing failures - maintain essential functions	Components shall provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure.	Verify via design documentation that software or hardware errors related to audit processing, or failures in the audit capturing mechanisms, do not cause loss of essential functions of the component. Record: a. Met b. Not met c. Not relevant - no essential functions Note that validation for FSA-CR 2.9B separately validates another aspect this requirement.	No	IEC 62443-4-2: CR 2.10(a)	1, 2, 3, 4	Audit generation typically occurs at the source of the event. Audit processing involves transmission, possible augmentation (such as, the addition of a timestamp) and persistent storage of the audit records. Audit processing failures include, for example, software or hardware errors, failures in the audit capturing mechanisms and audit storage capacity being reached or exceeded. Guidelines to be considered when designing appropriate response actions may include the NIST SP 800-92, *Guide to Computer Security Log Management* [26]. It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information. Also alerting personnel could be an appropriate supporting action in response to an audit processing failure.
x	x	x	x	FSA-CR 2.10B	Response to audit processing failures - actions taken	Components shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.	Verify user documents include evidence that the audit function supports one or more common accepted industry practices and recommendations upon lack of storage space to record new events, for example overwrite oldest audit records or stop generating audit records. Verify via testing that the device takes the action under these conditions as described in the user documentation. Verify in design documentation that in the event of software or hardware errors related to audit processing, one or more actions are taken in accordance with common accepted industry practices and recommendations, for example logging the event or generating a notification. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 2.10(b)	1, 2, 3, 4	See FSA-CR 2.10A
x	x	x	x	FSA-CR 2.11	Timestamps	Components shall provide the capability to create timestamps (including date and time) for use in audit records.	Verify by reviewing sample audit records in each category, that audit records include timestamps. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 2.11	1, 2, 3, 4	A good reference for the format of timestamps is ISO/IEC 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times* [15]. Care should be taken when designing a system that periodic time-shift events, such as daylight savings time in some locations, are taken into account.
x	x	x	x	FSA-CR 2.11 RE(1)	Time synchronization	Components shall provide the capability to create timestamps that are synchronized with a system wide time source.	Verify using user documentation that the component can be configured to synchronize time stamps with a system wide time source. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 2.11 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 2.11 RE(2)	Protection of time source integrity	The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.	Verify user documents include evidence that unauthorized alteration of time synchronization is detected and creates an audit event record. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 2.11 RE(2)	4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 2.12	Non-repudiation	If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action. Control elements that are not able to support such capability shall be listed in component documents.	Review user documentation and determine if the component provides a human user interface that permits actions by human users. If the component provides such a human user interface, verify component requirements documentation states that actions taken by human users, and the human user responsible for those actions, are logged in the audit records. At a minimum, this applies to actions related to security functions required by this standard and to example actions shown under Rationale and Supplemental Guidance." Further verify that supplier test cases are mapped to this requirement and have passed. Record one of: a. Met b. Not met If a component does not provide a such a human user interface, verify that the user manual for the component documents that the component does not have the ability to log user actions. If this can be verified, record: a. Not relevant If this cannot be verified, record: b. Not met	No	IEC 62443-4-2: CR 2.12	1, 2, 3, 4	Examples of particular actions taken by a user include performing operator actions, changing control system configurations, creating information, sending a message, approving information (such as, indicating concurrence) and receiving a message. Non-repudiation protects against later false claims by a user of not having taken a specific action, by an author of not having authored a particular document, by a sender of not having transmitted a message, by a receiver of not having received a message or by a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from a user, if a user took specific actions (for example, sending an email and approving a work order) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (for example, user identification and authorization, digital signatures, digital message receipts and timestamps).
x	x	x	x	FSA-CR 2.12 RE(1)	Non-repudiation for all users	Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Review user and design documentation and determine if the component permits actions by other than human users (software processes or devices). If the component permits such actions, verify requirements for the component state that all actions taken by a given user (software process or device), and the user responsible for those actions, are logged in the audit records. Further verify that supplier test cases are mapped to this requirement and have passed. Record one of: a. Met b. Not met If a component does not permit such actions, record: c. Not relevant (Note that the case for human users is covered by FSA-CR 2.12.)	No	IEC 62443-4-2: CR 2.12 RE(1)	4	
	x			FSA-EDR 2.13	Use of physical diagnostic and test interfaces	Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG Debugging).	Examine the embedded device hardware, and design documentation for all device models in scope for the certification, and the threat model, to identify any diagnostic and test interfaces that provide an ability to control the embedded device or to access non-public information. If there are such interfaces, review user or design documents to verify that authorization of an authenticated user assigned to a role authorized to use them, is required to access them (in which case they would be subject for FR 1 requirements), or that they are otherwise protected against unauthorized access. Record one of: a. Met b. Not met If there are no such interfaces, record: c. Not relevant	No	IEC 62443-4-2: EDR 2.13	2, 3, 4	Factory diagnostic and test interface(s) are created at various locations within the embedded device to assist the embedded device's developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the embedded device . However, these same interfaces must be carefully protected from access by unauthorized entities to protect the essential functionality provided by the embedded device to the IACS. If a diagnostic and test interface does not provide an ability to control the embedded device or to access non-public information, then it will not need an authentication mechanism. This shall be determined via a threat and risk assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information). There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
	x			FSA-EDR 2.13 RE(1)	Active monitoring	Embedded devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	If diagnostic or test interfaces that provide the ability to control the device or access to non-public information are found in validation of FSA-EDR 2.13, verify by testing that an audit log entry is generated when an attempt is made to access any of these interfaces. Record one of: a. Met b. Not met If such interfaces are not found in validation of FSA-EDR 2.13, then record: c. Not relevant	Yes	IEC 62443-4-2: EDR 2.13 RE(1)	3, 4	
		x		FSA-HDR 2.13	Use of physical diagnostic and test interfaces	Host devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	Examine the host device hardware, and design documentation for all device models in scope for the certification, and the threat model, to identify any diagnostic and test interfaces that provide an ability to control the host device or to access non-public information. If there are such interfaces, review user or design documents to verify that authorization of an authenticated user assigned to a role authorized to use them, is required to access them (in which case they would be subject to FR 1 requirements), or that they are otherwise protected against unauthorized access. Record one of: a. Met b. Not met If there are no such interfaces, record: c. Not relevant	No	IEC 62443-4-2: HDR 2.13	2, 3, 4	Factory diagnostic and test interface(s) are created at various locations within the host device to assist the component's developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the component. However, these same interfaces must be carefully protected from access by unauthorized entities to protect the essential functionality provided by the component to the IACS. There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document. If a diagnostic and test interface does not provide an ability to control the host device or to access non-public information, then it will not need an authentication mechanism. This shall be determined via a threat and risk assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).
		x		FSA-HDR 2.13 RE(1)	Active monitoring	Host devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	If diagnostic or test interfaces that provide the ability to control the device or access to non-public information are found in validation of FSA-HDR 2.13, verify by testing that an audit log entry is generated when an attempt is made to access any of these interfaces. Record one of: a. Met b. Not met If such interfaces are not found in validation of FSA-HDR 2.13, then record: c. Not relevant	Yes	IEC 62443-4-2: HDR 2.13 RE(1)	3, 4	
			x	FSA-NDR 2.13	Use of physical diagnostic and test interfaces	Network devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).	Examine the network device hardware, and design documentation for all device models in scope for the certification, and the threat model, to identify any diagnostic and test interfaces that provide an ability to control the network device or to access non-public information. If there are such interfaces, review user or design documents to verify that authorization of an authenticated user assigned to a role authorized to use them, is required to access them (in which case they would be subject to FR 1 requirements), or that they are otherwise protected against unauthorized access. Record one of: a. Met b. Not met If there are no such interfaces, record: c. Not relevant	No	IEC 62443-4-2: NDR 2.13	2, 3, 4	Factory diagnostic and test interface(s) are created at various locations within the component to assist the component's developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the component. However, these same interfaces must be carefully protected from access by unauthorized entities to protect the essential functionality provided by the component to the IACS. There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document. Note that if a diagnostic and test interface does not provide the ability to control the product, or to access non-public information, then it will not need an authentication mechanism. This should be determined via a threat assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 2.13 RE(1)	Active monitoring	Network devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.	If diagnostic or test interfaces that provide the ability to control the device or access to non-public information are found in validation of FSA-NDR 2.13, verify by testing that an audit log entry is generated when an attempt is made to access any of these interfaces. Record one of: a. Met b. Not met If such interfaces are not found in validation of FSA-NDR 2.13, then record: c. Not relevant	Yes	IEC 62443-4-2: NDR 2.13 RE(1)	3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 3.1	Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Examine design and user documents and determine if the component provides the capability to protect the data it transmits against changes to message content. Protection provided shall be beyond that provided by the transport layer. An example is the use of cryptographic hashes. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.1	1, 2, 3, 4	Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a control system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator. Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol (TCP) / internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well (see 7.6, CR 3.4 – Software and information integrity), while on a network distributed in areas with regular physical presence of staff or on a wide area network physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for communication integrity (for example because of legal restrictions). When it is infeasible or impractical to meet the necessary security requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk. Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. Many times the environment contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution.
x	x	x	x	FSA-CR 3.1 (ADV)	Communication integrity	Components shall provide the capability to protect integrity of transmitted information.	Examine design and user documents and determine if the component provides the capability to protect the data it transmits against changes to message content. Protection provided shall be beyond that provided by the transport layer. An example is the use of cryptographic hashes. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.1	1, 2, 3, 4	Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a control system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator. Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol (TCP) / internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well (see 7.6, CR 3.4 – Software and information integrity), while on a network distributed in areas with regular physical presence of staff or on a wide area network physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for communication integrity (for example because of legal restrictions). When it is infeasible or impractical to meet the necessary security requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk. Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. Many times the environment contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 3.1 RE(1)	Communication authentication	Components shall provide the capability to verify the authenticity of received information during communication.	Examine design and user documents and determine whether the origin of data received by the component can be validated by the component. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.1 RE(1)	2, 3, 4	
x				FSA-SAR 3.2	Protection from malicious code	The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.	Verify that design or user documents contain evidence that the software application is compatible with at least one mechanism for protection from installation and execution of malicious code on its hosting device. Verify that these documents note any special configuration requirements applicable for that mechanism. Verify that the supplier can provide evidence that the mechanism was qualified by testing or other means. Record one of: a. Met b. Not met	No	IEC 62443-4-2: SAR 3.2	1, 2, 3, 4	Protection from malicious code (for example, viruses, worms, Trojan horses and spyware) may be provided by the control system application or by an external service or application. Control system applications need to be compatible with mechanisms designed to protect them from malicious code. This requirement does not imply that the product supplier is to qualify and document all malicious code protection mechanisms which are compatible with the application but implies that the product supplier is to qualify and document at least one mechanism.
	x			FSA-EDR 3.2	Protection from malicious code	The embedded device shall provide the capability to protect from installation and execution of unauthorized software.	Verify that design or user documents contain evidence that the embedded device supports protections from installation and execution of unauthorized software. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.2	1, 2, 3, 4	Unauthorized software may contain malicious code and thus be harmful to the component. If an embedded device is able to utilize a compensating control, it need not directly support protection from malicious code. It is assumed that the IACS will be responsible for providing the required safeguards. However, for scenarios such as having a local universal serial bus (USB) host access, the need for protection from malicious code should be determined by a risk assessment. Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques. Prevention techniques may include, but are not limited to, removable media control, sandbox techniques and specific computing platforms mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection and mandatory access controls. See 10.4 for an associated requirement involving control system monitoring tools and techniques.
		x		FSA-HDR 3.2	Protection from malicious code	There shall be mechanisms on host devices that are qualified by the IACS product supplier to provide protection from malicious code. The IACS product supplier shall document any special configuration requirements related to protection from malicious code.	Verify that design or user documents contain evidence that the host device supports use of ~~at~~ one or more mechanisms for protection from installation and execution of malicious code, covering all interfaces via which code may be introduced. Verify that these documents note any special configuration requirements related to the mechanism(s). Verify that the supplier can provide evidence that the mechanism(s) was qualified by testing or other means. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.2	1, 2, 3, 4	Host devices need to support the use of malicious code protection (against, for example, viruses, worms, Trojan horses and spyware) . The product supplier should qualify and document the configuration of protection from malicious code mechanisms so that the primary mission of the control system is maintained.
		x		FSA-HDR 3.2 RE(1)	Report version of code protection	The host device shall automatically report the software and file versions of protection from malicious code in use (as part of overall logging function).	Verify by test that the host device reports the software and file versions of protection from malicious code in use. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: HDR 3.2 RE(1)	2, 3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 3.2	Protection from malicious code	The network device shall provide for protection from malicious code.	Verify that design or user documents contain evidence that the network device provides, directly or using one or more compensating mechanisms, protection from installation and execution of malicious code. The mechanisms shall cover all interfaces via which code may be introduced. Verify that these documents note any special configuration requirements related to the protection mechanisms. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.2	1, 2, 3, 4	If a network device is able to utilize a compensating control, it need not directly support protection from malicious code. One such possible compensating control would be the use of network packet filtering devices to identify and remove malicious code while in transit. It is assumed that the IACS will be responsible for providing the required safeguards. However, for scenarios such as having a local USB host access, the need for protection from malicious code should be evaluated.
x	x	x	x	FSA-CR 3.3	Security functionality verification	Components shall provide the capability to support verification of the intended operation of security functions according to IEC 62443-3-3 [11] SR3.3.	Verify component provides methods to test security functions during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in the IEC 62443-4-2 standard. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.3	1, 2, 3, 4	The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations. Details of the execution of these verifications need to be specified with careful consideration of the requirements for continuous operations (for example, scheduling or prior notification). Examples of security verification functions include: • Verification of antivirus countermeasures by European Institute for Computer Antivirus Research (EICAR) testing of the control system file system. Antivirus software should detect the EICAR test samples and appropriate incident handling procedures should be triggered. • Verification of the identification, authentication and use control countermeasures by attempting access with an unauthorized account (for some functionality this could be automated). • Verification of intrusion detection systems (IDSs) as a security control by including a rule in the IDS that triggers on irregular, but known non-malicious traffic. The test could then be performed by introducing traffic that triggers this rule and the appropriate IDS monitoring and incident handling procedures. • Confirmation that audit logging is occurring as required by security policies and procedures and has not been disabled by an internal or external entity.
x	x	x	x	FSA-CR 3.3 RE(1)	Security functionality verification during normal operation	Components shall provide the capability to support verification of the intended operation of security functions during normal operations.	Verify component provides methods to test security functions during normal operation. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.3 RE(1)	4	
x	x	x	x	FSA-CR 3.4	Software and information integrity	Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.	Verify that user documentation describes manual or automated integrity mechanisms (such as cryptographic hashes) to verify the integrity of component software and configuration information as well as the recording and reporting of the results of these checks, either directly or by integration into a system. Record one of: a. Met by component b. Met by integration into system c. Not met	No	IEC 62443-4-2: CR 3.4	1, 2, 3, 4	Integrity verification methods are employed to detect, record, report and protect against software and information tampering that may occur if other protection mechanisms (such as authorization enforcement) have been circumvented. Components should employ formal or recommended integrity mechanisms (such as cryptographic hashes). For example, such mechanisms could be used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 3.4 RE(1)	Authenticity of software and information	Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.	Verify that user documentation describes manual or automated authenticity mechanisms (such as digital signatures) to authenticate the origin of component software and configuration information as well as the recording and reporting of the results of these checks. Record one of: a. Met by component b. Met by integration into system c. Not met	No	IEC 62443-4-2: CR 3.4 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 3.4 RE(2)	Automated notification of integrity violations	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.	If component directly supports the capability under FSA-CR 3.4, verify component provides automated methods to verify software and configuration integrity and to provide automated notification to a configurable entity. Record one of: a. Met b. Not met If the component does not directly support the capability under FSA-CR 3.4, record: c. Not relevant	No	IEC 62443-4-2: CR 3.4 RE(2)	3, 4	
x	x	x	x	FSA-CR 3.5	Input validation	Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	No validation activity for the FSA element of certification. This requirement is covered in the SDA element of certification, by the validations for IEC 62443-4-1 requirements SVV-1 and SI-2, defined in the ISASecure document SDLA-312 as requirements SDLA-SVV-1C and SDLA-SI-2E.	No	IEC 62443-4-2: CR 3.5	1, 2, 3, 4	Rules for checking the valid syntax of input data such as set points should be in place to verify that this information has not been tampered with and is compliant with the specification. Inputs passed to interpreters should be pre-screened to prevent the content from being unintentionally interpreted as commands. Note that this is a security CR, thus it does not address human error, for example supplying a legitimate integer number which is outside the expected range. Generally accepted industry practices for input data validation include out-of-range values for a defined field type, invalid characters in data fields, missing or incomplete data and buffer overflow. Additional examples where invalid inputs lead to system security issues include SQL injection attacks, cross-site scripting or malformed packets (as commonly generated by protocol fuzzers). Guidelines to be considered should include well-known guidelines such as the Open Web Application Security Project (OWASP) Code Review Guide [28].
x	x	x	x	FSA-CR 3.6	Deterministic output	Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.	Review user documentation and determine if the component can physically or logically connect to an automation process. If the component can physically or logically connect to an automation process, review user documentation and verify that the component will set outputs of an automation process to a predetermined state if normal operation can not be maintained. Record one of: a. Met b. Not met If the component can not physically or logically connect to an automation process, record: c. Not relevant	No	IEC 62443-4-2: CR 3.6	1, 2, 3, 4	The deterministic behavior of control system outputs as a result of threat actions against the control system devices and software is an important characteristic to ensure the integrity of normal operations. Ideally, the device continues to operate normally while under attack, but if the control system cannot maintain normal operation, then the control system outputs need to fail to a predetermined state. The appropriate predetermined state of control system outputs is device dependent and could be one of the following user configurable options: • Unpowered – the outputs fail to the unpowered state; • Hold – the outputs fail to the last-known good value; or • Fixed – the outputs fail to a fixed value that is determined by the asset owner or an application; or • Dynamic – the outputs fail to one of the above options based on the current state.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 3.7	Error handling	Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.	Supplier provides a list of all error messages returned to a non administrative user. Verify for samples from this list that component error messages do not reveal sensitive information that could be exploited to attack the component. Verify that the supplier has performed a security expert review of all error messages for such exploitable information. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.7	1, 2, 3, 4	The product supplier and/or system integrator should carefully consider the structure and content of error messages. Error messages generated by the component should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include well-known guidelines such as the OWASP Code Review Guide. NOTE: A good example of an error message that could help adversaries attack an IACS would be to provide details of why authentication with the system failed. For example stating invalid user or invalid password in the feedback would help an adversary attack the IACS and thus should not be provided.
x	x	x	x	FSA-CR 3.8A	Session integrity - invalidate session identifiers	Components shall provide mechanisms to protect the integrity of communications sessions including the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions).	Review user documentation and determine if communication sessions are used. If communication sessions are used, verify that design documentation confirms that 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	No	IEC 62443-4-2: CR 3.8(a)	2, 3, 4	This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking, insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use should be considered in light of requirements for real-time communications. Session hijacking and other man-in-the-middle attacks or injections of false information often take advantage of easy-to-guess session IDs (keys or other shared secrets) or use of session IDs that were not properly invalidated after session termination. Therefore the validity of a session authenticator should be tightly connected to the lifetime of a session. Employing randomness in the generation of unique session IDs helps to protect against brute-force attacks to determine future session IDs.
x	x	x	x	FSA-CR 3.8B	Session integrity - generate and recognize session identifiers	Components shall provide mechanisms to protect the integrity of communications sessions including the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated.	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 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	No	IEC 62443-4-2: CR 3.8(b)	2, 3, 4	See FSA-CR 3.8A
x	x	x	x	FSA-CR 3.8C	Session integrity - random session identifiers	Components shall provide mechanisms to protect the integrity of communications sessions including the capability to generate unique session identifiers with commonly accepted sources of randomness.	Review user documentation and determine if communication sessions are used. If communication sessions are used, verify that 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	No	IEC 62443-4-2: CR 3.8(c)	2, 3, 4	See FSA-CR 3.8A
x	x	x	x	FSA-CR 3.9	Protection of audit information	Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.	Review component documentation and verify that audit information and audit tools (if present) require authorization in order to access, modify or delete, for any interface through which these are accessible. Attempt to delete an audit log as an unauthorized user and verify that access is denied. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 3.9	2, 3, 4	Audit information includes all information (for example, audit records, audit settings and audit reports) needed to successfully audit control system activity. The audit information is important for error correction, security breach recovery, investigations and related efforts. Mechanisms for enhanced protection against modification and deletion include the storage of audit information to hardware-enforced write-once media.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 3.9 RE(1)	Audit records on write-once media	Components shall provide the capability to store audit records on hardware-enforced write-once media.	Review component documentation and verify that the component has the capability to produce audit records on hardware-enforced write-once media. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 3.9 RE(1)	4	
	x			FSA-EDR 3.10	Support for updates	The embedded device shall support the ability to be updated and upgraded.	Verify by examining design documentation and user documentation, that elements of the embedded device can be updated and upgraded. Typical elements are software and firmware. Update and upgrade are defined in IEC 62443-4-2 sub clause 3.1. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.10	1, 2, 3, 4	Embedded devices over their installed lifetime may have the need for installation of updates and upgrades. There will be cases where embedded devices are supporting or executing essential functions as well. When this is the case the embedded device needs to have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2 CCSC 1 Support of essential functions). One example for providing this capability would be to support redundancy within the embedded device.
	x			FSA-EDR 3.10 RE(1)	Update authenticity and integrity	The embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation.	Verify that the component provides measures to verify prior to installation, that software updates and upgrades originate from the supplier. Verify in design and user documentation and by testing that the component provides measures to detect changes to software that have occurred after creation by the supplier and prior to installation. One possible method to meet this requirement is to validate digital signatures and cryptographic hashes. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: EDR 3.10 RE(1)	2, 3, 4	
		x		FSA-HDR 3.10	Support for updates	Host devices shall support the ability to be updated and upgraded.	Verify by examining design documentation and user documentation, that elements of the host device can be updated and upgraded. Typical elements are software and firmware. Update and upgrade are defined in IEC 62443-4-2 sub clause 3.1. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.10	1, 2, 3, 4	Host devices over their installed lifetime may have the need for installation of updates and upgrades. There will be cases where host devices are supporting or executing essential functions as well. When this is the case the host device should have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2 CSSC 1 Support of essential functions). One example for providing this capability would be to support redundancy within the host device.
		x		FSA-HDR 3.10 RE(1)	Update authenticity and integrity	Host devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.	Verify that the component provides measures to verify prior to installation, that software updates and upgrades originate from the supplier. Verify in design and user documentation and by testing that the component provides measures to detect changes to software that have occurred after creation by the supplier and prior to installation. One possible method to meet this requirement is to validate digital signatures and cryptographic hashes. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: HDR 3.10 RE(1)	2, 3, 4	
			x	FSA-NDR 3.10	Support for updates	Network devices shall support the ability to be updated and upgraded.	Verify by examining design documentation and user documentation, that elements of the network device can be updated and upgraded. Typical elements are software and firmware. Update and upgrade are defined in IEC 62443-4-2 sub clause 3.1. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.10	1, 2, 3, 4	Network devices over their installed lifetime may require installation of updates and upgrades. There will be cases where network devices are supporting or executing essential functions as well. When this is the case the network device should have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2 CCSC 1 Support of essential functions). One example for providing this capability would be to support redundancy within the network device.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 3.10 RE(1)	Update authenticity and integrity	Network devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.	Verify that the component provides measures to verify prior to installation, that software updates and upgrades originate from the supplier. Verify in design and user documentation and by testing that the component provides measures to detect changes to software that have occurred after creation by the supplier and prior to installation. One possible method to meet this requirement is to validate digital signatures and cryptographic hashes. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: NDR 3.10 RE(1)	2, 3, 4	
	x			FSA-EDR 3.11	Physical tamper resistance and detection	The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Examine the threat model for the component to verify that it enumerates possible integrity and confidentiality threats to the component due to physical access. Verify for each of these threats, that they are deterred by physical mechanisms and that carrying out the threat creates tamper evidence. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.11	2, 3, 4	The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur. Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals. The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.
	x			FSA-EDR 3.11 RE(1)	Notification of a tampering attempt	The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Verify in the threat model that high risk events of unauthorized physical access are mitigated by automatic notification. Verify that the component provides the capability to automatically provide notification to a configurable set of recipients when such an access is detected, and to create an audit record for this notification. Methods that require human intervention for detection or notification (such as a person noticing disturbed tamper tape) do not meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.11 RE(1)	3, 4	
		x		FSA-HDR 3.11	Physical tamper resistance and detection	Host devices shall provide the capability to support tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Examine the threat model for the component to verify that it enumerates possible integrity and confidentiality threats to the component due to physical access. Verify for each of these threats, that they are deterred by physical mechanisms supported by the component, and that the component supports a mechanism such that carrying out the threat creates tamper evidence. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.11	2, 3, 4	The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur. Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals. The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.
		x		FSA-HDR 3.11 RE(1)	Notification of a tampering attempt	Host devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Verify in the threat model that high risk events of unauthorized physical access are mitigated by automatic notification. Verify that the component provides the capability to automatically provide notification to a configurable set of recipients when such an access is detected, and to create an audit record for this notification. Methods that require human intervention for detection or notification (such as a person noticing disturbed tamper tape) do not meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.11 RE(1)	3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 3.11	Physical tamper resistance and detection	Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.	Examine the threat model for the component to verify that it enumerates possible integrity and confidentiality threats to the component due to physical access. Verify for each of these threats, that they are deterred by physical mechanisms, and that carrying out the threat creates tamper evidence. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.11	2, 3, 4	The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur. Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals. The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.
			x	FSA-NDR 3.11 RE(1)	Notification of a tampering attempt	Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.	Verify in the threat model that high risk events of unauthorized physical access are mitigated by automatic notification. Verify that the component provides the capability to automatically provide notification to a configurable set of recipients when such an access is detected, and to create an audit record for this notification. Methods that require human intervention for detection or notification (such as a person noticing disturbed tamper tape) do not meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.11 RE(1)	3, 4	
	x			FSA-EDR 3.12	Provisioning product supplier roots of trust - protection	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Examine supplier documentation of the component design and manufacturing process to verify that during the process for creating any roots of trust for the device, and thereafter, the product supplier keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity and authenticity of the roots of trust at the time of device manufacture and as used thereafter, and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.12	2, 3, 4	In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it must possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the "root of trust" for the system. This trusted source of data may be a set of cryptographic hashes of "known good" software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a "known good" state in which all security mechanisms are known to be operational and uncompromised. "Root of trust" data is often protected via hardware mechanisms, preventing any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier's provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.
		x		FSA-HDR 3.12	Provisioning product supplier roots of trust - protection	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Examine supplier documentation of the component design and manufacturing process to verify that during the process for creating any roots of trust for the device, and thereafter, the product supplier keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity and authenticity of the roots of trust at the time of device manufacture and as used thereafter, and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.12	2, 3, 4	In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it must possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the "root of trust" for the system. This trusted source of data may be a set of cryptographic hashes of "known good" software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a "known good" state in which all security mechanisms are known to be operational and uncompromised. "Root of trust" data can be protected by software or hardware implemented mechanisms to prevent any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier's provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 3.12	Provisioning product supplier roots of trust - protection	Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more "roots of trust" at the time of manufacture of the device.	Examine supplier documentation of the component design and manufacturing process to verify that during the process for creating any roots of trust for the device, and thereafter, the product supplier keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity and authenticity of the roots of trust at the time of device manufacture and as used thereafter, and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.12	2, 3, 4	In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it must possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the "root of trust" for the system. This trusted source of data may be a set of cryptographic hashes of "known good" software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a "known good" state in which all security mechanisms are known to be operational and uncompromised. "Root of trust" data is often protected by software or hardware implemented mechanisms to prevent any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier's provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.
	x			FSA-EDR 3.13A	Provisioning asset owner roots of trust - protection	Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as "roots of trust".	Examine user documentation to verify that after an asset owner has assumed responsibility for a device, a process exists for the asset owner to create and use roots of trust for the device. Verify in design documentation that the asset owner keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity, and authenticity of the asset owner roots of trust and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.13(a)	2, 3, 4	Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a "known good" state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component's functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins. In order to perform these validations the component must contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore it is important that the product supplier provide a way for the asset owner to securely provision their own "roots of trust" which provide the ability to distinguish between origins allowed by the asset owner's security policy, and those that are not. The authenticity and integrity of these "roots of trust" must be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component. A root of trust can also be used as a basis communications security, such as communications integrity required by CR 3.1 – Communication integrity or communications confidentiality required by CR 4.1 – Information confidentiality. Requirements such as EDR 2.4 – Mobile code require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.
	x			FSA-EDR 3.13B	Provisioning asset owner roots of trust - inside zone	Embedded devices shall support the capability to provision without reliance on components that may be outside of the device's security zone.	Examine user and design documents for evidence to verify that the component process for provisioning asset owner roots of trust can be performed within the component's security zone. Record one of: a. Met b. Not met	No	IEC 62443-4-2: EDR 3.13(b)	2, 3, 4	See FSA-EDR 3.13A

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
		x		FSA-HDR 3.13A	Provisioning asset owner roots of trust - protection	Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”.	Examine user documentation to verify that after an asset owner has assumed responsibility for a device, a process exists for the asset owner to create and use roots of trust for the device. Verify in design documentation that the asset owner keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity, and authenticity of the asset owner roots of trust and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.13(a)	2, 3, 4	Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins. In order to perform these validations the component must contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” must be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component. Requirements such as HDR 2.4 – Mobile code require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute. A root of trust can also be used as a basis communications security, such as communications integrity required by CR 3.1 – Communication integrity or communications confidentiality required by CR 4.1 – Information confidentiality.
		x		FSA-HDR 3.13B	Provisioning asset owner roots of trust - inside zone	Host devices shall support the capability to provision without reliance on components that may be outside of the device’s security zone.	Examine user and design documents for evidence to verify that the component process for provisioning asset owner roots of trust can be performed within the component's security zone. Record one of: a. Met b. Not met	No	IEC 62443-4-2: HDR 3.13(b)	2, 3, 4	See FSA-HDR 3.13A
			x	FSA-NDR 3.13A	Provisioning asset owner roots of trust - protection	Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”.	Examine user documentation to verify that after an asset owner has assumed responsibility for a device, a process exists for the asset owner to create and use roots of trust for the device. Verify in design documentation that the asset owner keys and data to be used as roots of trust, are handled within the device such that they cannot be accessed in any manner other than by the functions in the device that require the usage of this information. Verify that the threat model analyzes threats to the confidentiality, integrity, and authenticity of the asset owner roots of trust and that these threats have been mitigated. Use of a trusted store or a trusted zone are examples of methods to meet this requirement. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.13(a)	2, 3, 4	Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins. In order to perform these validations the component must contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” must be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component. Requirements such as NDR 2.4 – Mobile code require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute. A root of trust is used to provide communications security, such as communications integrity required by CR 3.1 – Communication integrity or communications confidentiality required by CR 4.1 – Information confidentiality.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 3.13B	Provisioning asset owner roots of trust - inside zone	Network devices shall support the capability to provision without reliance on components that may be outside of the device's security zone.	Examine user and design documents for evidence to verify that the component process for provisioning asset owner roots of trust can be performed within the component's security zone. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 3.13(b)	2, 3, 4	See FSA-NDR 3.13A
	x			FSA-EDR 3.14	Integrity of the boot process	Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for component's boot and runtime processes prior to use.	Verify in design documentation, and by testing that the component provides measures to verify during the boot process that all firmware, software and configuration data needed for the boot or runtime process have not been modified between a prior point in time when they were assumed trustworthy, and each time of use for the boot or runtime process. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: EDR 3.14	1, 2, 3, 4	In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore the component must perform checks to validate the integrity of the component's firmware and/or software prior to use during the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.
	x			FSA-EDR 3.14 RE(1)	Authenticity of the boot process	Embedded devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.	Verify in design and user documentation, and by testing that the component uses supplier roots of trust to verify during the boot process that all firmware, software and configuration data needed for the boot process originate from the supplier. One possible method is validation of digital signatures and cryptographic hashes. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: EDR 3.14 RE(1)	2, 3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
		x		FSA-HDR 3.14	Integrity of the boot process	Host devices shall verify the integrity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.	Verify in design documentation, and by testing that the component provides measures to verify during the boot process that all firmware, software and configuration data needed for the boot process have not been modified between a prior point in time when they were assumed trustworthy, and each time of use for the boot process. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: HDR 3.14	1, 2, 3, 4	In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore the component must perform checks to validate the integrity and authenticity of the component's firmware and/or software prior to the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.
		x		FSA-HDR 3.14 RE(1)	Authenticity of the boot process	Host devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.	Verify in design and user documentation, and by testing that the component uses supplier roots of trust to verify during the boot process that all firmware, software and configuration data needed for the boot process originate from the supplier. One possible method is validation of digital signatures and cryptographic hashes. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: HDR 3.14 RE(1)	2, 3, 4	
			x	FSA-NDR 3.14	Integrity of the boot process	Network devices shall verify the integrity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.	Verify in design documentation, and by testing that the component provides measures to verify during the boot process that all firmware, software and configuration data needed for the boot process have not been modified between a prior point in time when they were assumed trustworthy and each time of use for the boot process. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: NDR 3.14	1, 2, 3, 4	In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore the component must perform checks to validate the integrity and authenticity of the component's firmware and/or software prior to the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.
			x	FSA-NDR 3.14 RE(1)	Authenticity of the boot process	Network devices shall use the component's product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.	Verify in design and user documentation, and by testing that the component uses supplier roots of trust to verify during the boot process that all firmware, software and configuration data needed for the boot process originate from the supplier. One possible method is validation of digital signatures and cryptographic hashes. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: NDR 3.14 RE(1)	2, 3, 4	

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 4.1A	Information confidentiality - at rest	Components shall provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported.	Identify all information at rest for which explicit read authorization is supported. Review design documentation and verify that all such information includes methods to protect the confidentiality such as encrypting the data or limiting user access to the location where the data is stored. If the user must configure or set up the component in a certain manner to meet this requirement, verify that this is clearly documented in a user manual. Attempt to access a sampling of confidential information to verify that it cannot be accessed by users without the proper authorization. Record one of: a. Met b. Not Met	Yes	IEC 62443-4-2: CR 4.1(a)	1, 2, 3, 4	The decision whether a given information should be protected or not depends on the context and cannot be made at product design. However, the fact that an organization limits access to information by configuring explicit read authorizations in the control system is an indicator that this information should be protected by the organization. Thus, all information for which the component supports the capability to assign explicit read authorizations should be considered potentially sensitive and thus the component should also provide the capability to protect its confidentiality. Confidentiality of information in transit requires system level capabilities which the component should be able to support. For confidentiality protection, 8.5 CR 4.3 – Use of cryptography provides further requirements.
x	x	x	x	FSA-CR 4.1B	Information confidentiality - in transit	Components shall support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 [11] SR 4.1.	Identify all information in transit over external boundaries of the component for which explicit read authorization is supported. Review design documentation and verify that all such information includes methods to protect the confidentiality such as encrypting the data or limiting user access to the physical medium data used for transmission. If the user must configure or set up the component in a certain manner to meet this requirement, verify that this is clearly documented in a user manual. If a user can access a physical medium used for transmission, verify by test that no confidential information can be seen on the transmission medium by using an eavesdropping tool such as Wireshark to view a sampling of communications while the system is performing its normal operations. Record one of: a. Met b. Not Met	Yes	IEC 62443-4-2: CR 4.1(b)	1, 2, 3, 4	See FSA-CR 4.1A
x	x	x	x	FSA-CR 4.2	Information persistence	Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.	Review component documentation and verify that the component has the ability to purge all information for which explicit read authorization is supported. Verify that the data is purged from the component such that it can not be recreated. Record one of: a. Met b. Not Met	No	IEC 62443-4-2: CR 4.2	2, 3, 4	Removal of a control system component from active service should not provide the opportunity for unintentional release of information for which explicit read authorization is supported. An example of such information can include authentication information and network configuration information stored in non-volatile storage or other cryptographic information that would facilitate unauthorized or malicious activity. Information produced by the actions of a user or role (or the actions of a software process acting on behalf of a user or role) should not be disclosed to a different user or role in an uncontrolled fashion. Control of control system information or data persistence prevents information stored on a shared resource from being unintentionally disclosed after that resource has been released back to the control system.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 4.2 RE(1)	Erase of shared memory resources	Components shall provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.	Determine from component documention if the component may have more than one user, and if confidential information may be placed in volatile memory. If both of these statements are true, then review component design documentation and verify that confidential information is purged from RAM before that memory is released back to the component for use by a different user. Review component design documentation and verify that confidential information is not stored in memory that can be accessed by unauthorized users of any type (human, device, software application). Record one of: a. Met b. Not Met c. Not relevant, if the component has only one user or if no confidential information is placed in volatile memory Confidential information is information such that the security of the component depends upon confidentiality protection of this data from some or all users, or for which explicit read authorization may be configured/customized by the user.	No	IEC 62443-4-2: CR 4.2 RE(1)	3, 4	
x	x	x	x	FSA-CR 4.2 RE(2)	Erase verification	Components shall provide the capability to verify that the erasure of information occurred.	Review the component documentation and verify that the component has the cabability to verify that information has been purged from the component as defined in the CR-4.2 base requirement. Carry out a test to follow the recommended practice to purge information from the component and perform the documented verification method to verify that the information has been purged from the component. Carry out an additional test to perform the documented verification method on a system that has not had its information purged to ensure that the method will detect a failure of the purge. Record one of: a. Met b. Not Met	Yes	IEC 62443-4-2: CR 4.2 RE(2)	3, 4	
x	x	x	x	FSA-CR 4.3	Use of cryptography	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.	Verify through design documentation that if the component uses cryptography then algorithms, key sizes and mechanisms for key establishment are done according to commonly accepted industry best practices and recommendations as defined in ICSA-500, or in NIST SP 800-57 or similar publication. a. Met by the component b. Not Met	No	IEC 62443-4-2: CR 4.3	1, 2, 3, 4	The selection of cryptographic protection should be based on a threat and risk analysis which covers the value of the information being protected, the consequences of the confidentiality and integrity of the information being breached, the time period during which the information is confidential and control system operating constraints. This can involve either information at rest, in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality and integrity assessment process. The control system product supplier should document the practices and procedures relating to cryptographic key establishment and management. The control system should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes based on an assigned standard. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution and encryption key backup in accordance with defined standards. Generally accepted practices and recommendations can be found in documents such as NIST SP 800-57, *Recommendation for Key Management, Part 1: General* [25]. Implementation requirements can be found for example in FIPS 140-2, *Security Requirements for Cryptographic Modules* [24] or ISO/IEC 19790, *Information technology – Security techniques – Security requirements for cryptographic modules* [17]. This CR, along with 5.10, CR 1.8 – Public key infrastructure certificates may be applicable when meeting many other requirements defined within this document.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 5.1	Network segmentation	Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.	Verify that the device supports a networking technology that is capable of being segmented. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 5.1	1, 2, 3, 4	Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection. Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements. Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture used by an asset owner in their facility and even system integrators within their control systems. Logically segmenting networks based on their functionality provides some measure of protection, but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case, but will lead to a more complex and costly network design. These trade-offs will need to be evaluated during the network design process (see IEC 62443 2-1). In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local CAs. It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.
			x	FSA-NDR 5.2	Zone boundary protection	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	Unless the supplier has documented that a network device is not intended to be used at a zone boundary, verify that the network device has the capability to inspect network traffic passing through the device, that determines whether the network device takes action to control the traffic. Examples of control actions supported may include rerouting the traffic or dropping it. For example, a firewall or router would satisfy this aspect of the requirement. Also verify that the occurrence of control actions taken on network traffic is recorded in a log. Record one of: a. Met b. Not met If the supplier has documented that a network device is not intended to be used at a zone boundary, record: c. Not relevant	No	IEC 62443-4-2: NDR 5.2	1, 2, 3, 4	Any connections to outside each security zone should occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site.
			x	FSA-NDR 5.2 RE(1)	Deny all, permit by exception	The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).	Verify that user documents indicate the capability to deny all network traffic through the network device by default and allow network traffic by exception. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 5.2 RE(1)	2, 3, 4	
			x	FSA-NDR 5.2 RE(2)	Island mode	The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).	Verify in user documentation and by testing that the network device has the capability to be placed in a mode to block all traffic passing through the device. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: NDR 5.2 RE(2)	3, 4	NOTE Examples of when this capability may be used include where a security violation and/or breach has been detected within the control system, or an attack is occurring at the enterprise level.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
			x	FSA-NDR 5.2 RE(3)	Fail close	The network component shall provide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).	Verify in user documentation and by testing that the network device has the capability to block all traffic passing through the device, when there is any operational failure of boundary protection mechanisms. Examples of operational failures for which this capability may be provided are power failure, software failures, and hardware failures. a. Met b. Not met	Yes	IEC 62443-4-2: NDR 5.2 RE(3)	3, 4	NOTE Examples of when this capability may be used include scenarios where a hardware failure or power failure causes boundary protection devices to function in a degraded mode or fail entirely.
			x	FSA-NDR 5.3	General purpose, person-to-person communication restrictions	A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.	Verify in user documentation that the network device has the capability to block all types of general purpose, person-to-person messages. Record one of: a. Met b. Not met	No	IEC 62443-4-2: NDR 5.3	1, 2, 3, 4	General purpose, person-to-person communications systems include but are not limited to: email systems, forms of social media (Twitter, Facebook, picture galleries, etc.) or any message systems that permit the transmission of any type of executable file. These systems are usually utilized for private purposes that are not related to control system operations, and therefore the risks imposed by these systems normally outweigh any perceived benefit. These types of general purpose communications systems are commonly used as attack vectors to introduce malware to the control system, pass information for which read authorization exists to locations external to the control system and introduce excessive network loading that can be used to create security problems or launch attacks on the control system. Network devices could realize such restrictions, for example, by blocking specific communications based on port numbers and source and/or target address as well as more in depth checks by application layer firewalls.
				FSA-CR 5.4	Application partitioning	There is no component level requirement associated with IEC 62443-3-3 SR 5.4.	No validation activity		IEC 62443-4-2: CR 5.4		

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 6.1	Audit log accessibility	Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Verify that the component provides a means for authorized humans and/or authorized external tools to access audit logs on a read-only basis. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 6.1	1, 2, 3, 4	The applications and devices may generate audit records about events occurring in that application or device (see 6.10). Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as, screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as security information and event management (SIEM). See relevant SRs in Clauses 5, 6 and 9 regarding the creation of, protection of and access to audit logs.
x	x	x	x	FSA-CR 6.1 RE(1)	Programmatic access to audit logs	Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system	Verify in user or design documentation that the component provides programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 6.1 RE(1)	3, 4	
x	x	x	x	FSA-CR 6.2	Continuous monitoring	Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.	Verify that the supplier chose an industry resource that provides recommendations for events to be monitored to identify security breaches for the component. Verify that the component is capable of being monitored for those events. For example failed authorization and access control attempts, failed input validation, and high value transactions are identified in the OWASP Top 10 resource. Verify that monitoring can be done in a continuous manner, and that the component is capable of reporting of events in a time frame to permit mitigation of a possible associated security breach associated with the event. Verify that events are reported with content and format usable by a centralized analysis solution. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 6.2	2, 3, 4	Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, intrusion prevention system (IPS), protection from malicious code mechanisms and network monitoring mechanisms). As attacks become more sophisticated, these monitoring tools and techniques will need to become more sophisticated as well, including for example behavior-based IDS/IPS. Monitoring devices should be strategically deployed within the control system (for example, at selected perimeter locations and near server farms supporting critical applications) to collect essential information. Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions. Monitoring should include appropriate reporting mechanisms to allow for a timely response to events. To keep the reporting focused and the amount of reported information to a level that can be processed by the recipients, mechanisms such as SIEM are commonly applied to correlate individual events into aggregate reports that establish a larger context in which the raw events occurred.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 7.1	Denial of service protection	Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.	If the component has essential functions, verify that the threat model for the component identifies DoS threats and their mitigations using a systematic analysis method. Verify that the supplier has test cases to show that the component maintains essential functions when subjected to DoS attack. Verify that those tests have passed. Record one of: a. Met b. Not met c. Not relevant, if component has no essential functions	No	IEC 62443-4-2: CR 7.1	1, 2, 3, 4	Components may be subjected to different forms of DoS situations. When these occur the component should be designed in such a manner that it maintains essential functions necessary for continued safe operations while in a degraded mode.
x	x	x	x	FSA-CR 7.1 RE(1)	Manage communication load from component	Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.	Verify that the threat model for the component identifies information and/or message flooding types of DoS events. Verify that the threat model indicates the capability to mitigate the effects of these threats. Verify that the supplier has test cases that have passed for these mitigations as required by IEC 62443-4-1 requirement SVV-2. (This examination of test cases can be done as part of validation activity in the SDA-C element of certification, for requirement SDLA-SVV-2-1 in SDLA-312.) Verify that the requirement SDLA-SVV-3A4 from SDLA-312 in the SDA-C element of the certification has passed. This requirement includes audit of testing under network traffic load events. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 7.1 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 7.2	Resource management	Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.	Verify using design documentation that usage of security functions provided by the component to meet the IEC 62443-4-2 standard are limited in such a way that high usage of these functions does not interfere with other component functions. Examples include but are not limited to: high rates of user authentication attempts (possibly failed attempts), high audit logging rates, high rates of incoming data requiring authenticity checking or outgoing data requiring integrity protections, series of physical attacks triggering a series of automated notifications. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 7.2	1, 2, 3, 4	Resource management (for example, network segmentation or priority schemes) prevents a lower-priority software process from delaying or interfering with the control system servicing any higher-priority software process. For example, initiating network scans, patching and/or antivirus checks on an operating system can cause severe disruption to normal operations. Traffic rate limiting schemes should be considered as a mitigation technique.
x	x	x	x	FSA-CR 7.3	Control system backup	Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.	Verify that the supplier has test cases to show that the component provides the capability to provide component user and component state information as part of a system level backup operation, with no effect on the normal component operations. Verify this capability in user documentation. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 7.3	1, 2, 3, 4	The availability of up-to-date backups is essential for recovery from a control system failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead. When designing to support a backup capability, consideration should be given to information that will be stored in backups. Some of this information may contain cryptographic keys and other information that is protected through security controls while part of the system. Once the information is placed into a backup it most likely will not have the same controls in place to protect it. Thus the component backup ability needs to include the mechanisms to support the necessary protection of the information that is contained in the backup. This may include encryption of the backup, encryption of the sensitive data as part of the backup procedure or not including the sensitive information as part of the backup. If the backup is encrypted it is important not to include the cryptographic keys as part of the backup but to backup the cryptographic keys as part of a separate more secure backup procedure.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 7.3 RE(1)	Backup integrity verification	Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.	Verify in user documentation that the component provides the capability to validate the integrity of backed up information prior to the initiation of a restore of that information. Verify via testing by both deleting and modifying the data in the backed up information associated with some event. Attempt to restore and verify that a problem is reported to the user before the restore to the component is initiated. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 7.3 RE(1)	2, 3, 4	
x	x	x	x	FSA-CR 7.4	Control system recovery and reconstitution	Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.	Verify in user documentation that a process is described for restoring a failed or suspected defective component to a known secure state. Verify that the expected state is described in the user documentation. Perform the process and verify that it achieves the documented state. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 7.4	1, 2, 3, 4	Component recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, components are reinstalled and configured with established settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.
				FSA-CR 7.5	Emergency power	There is no component level requirement associated with IEC 62443-3-3 SR 7.5.	No validation activity		IEC 62443-4-2: CR 7.5		
x	x	x	x	FSA-CR 7.6	Network and security configuration settings	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.	The SDA-C certification element under requirements SDLA-SG-3A and SDLA-SG-3D in document SDLA-312, requires guidelines for security hardening and security configuration, respectively. If the evaluation for SDLA-SG-3A has passed, verify by test that the user may view currently deployed network configuration settings through a component interface. Verify that the component may be configured through a component interface to modify these settings, and in particular to meet any network configuration guidance found in the guidelines that have met SDLA-SG-3A. If the evaluation for SDLA-SG-3D has passed, verify by test that the user may view the settings described in the guidelines that have met that requirement, through a component interface. Modify any settings that do not conform to the recommended settings. View and verify any changes in the resulting configuration through the interface provided. Record one of: a. Met b. Not met If evaluations for either of the requirements SDLA-SG-3A and SDLA-SG-3D in the SDA-C element of certification have not passed, Record: b. Not met	Yes	IEC 62443-4-2: CR 7.6	1, 2, 3, 4	These configuration settings are the adjustable parameters of the control system components. By default the component should be configured to the recommended settings. In order for a component to detect and correct any deviations from the approved and/or recommended configuration settings, the component needs to support monitoring and control of changes to the configuration settings in accordance with security policies and procedures.
x	x	x	x	FSA-CR 7.6 RE(1)	Machine-readable reporting of current security settings	Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.	Verify that a report can be generated listing the currently deployed security settings in a machine-readable format, by generating and reading this report. Record one of: a. Met b. Not met	Yes	IEC 62443-4-2: CR 7.6 RE(1)	3, 4	
x	x	x	x	FSA-CR 7.7	Least functionality	Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.	Verify the user documentation specifies required ports and protocols, and provides guidance for how to prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or other services. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 7.7	1, 2, 3, 4	Components are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support IACS functionality. Therefore, by default, functions beyond a baseline configuration should be disabled. Additionally, it is sometimes convenient to provide multiple services from a single component of a control system, but doing so increases the risk compared to limiting the services provided by any one component.

Software Application	Embedded Device	Host Device	Network Device	Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Capability Security Level	Rationale and Supplemental Guidance
x	x	x	x	FSA-CR 7.8	Control system component inventory	Components shall provide the capability to support a control system component inventory according to IEC 62443-3-3 [11] SR 7.8.	Verify that the component provides the capability to identify its presence and its associated properties for a control system component inventory. Record one of: a. Met b. Not met	No	IEC 62443-4-2: CR 7.8	2, 3, 4	Components may bring their own set of components into the overall control system. When this is the case then those components need to provide a mechanism to augment the overall component inventory which is compatible with IEC 62443-2-4 [8] SP.06.02.