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 Foundation Requirements
GEN	**General** - General requirements
IAC	**ID & Auth Control** - detailed requirements for 1st Foundation Requirement
UC	**Use Control** - detailed requirements for 2nd Foundation Requirement
SI	**System Integrity** - detailed requirements for 3rd Foundation Requirement
DC	**Data Confidentiality** - detailed requirements for 4th Foundation Requirement
RDF	**Restricted Data Flow** - detailed requirements for 5th Foundation Requirement
TRE	**Timely Response to Event** - detailed requirements for 6th Foundation Requirement
RA	**Resource Availability** - detailed requirements for 7th Foundation Requirement

Common structure used for all requirement worksheets:

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes

Requirement ID - unique ID number assigned to each requirement for unobvious reference
Reference Name - unique name for each requirement that provides an indication of the scope / content
Requirement Description - text of the particular requirement
Validation Activity - defines activity that must be performed as part of the evaluation audit
Validation by Independent Test Required - is the auditor required to perform independent testing as part of the validation activity
Source of Requirement - documents source of the particular requirement
Security Level - specifies for what levels of ISASecure this requirement applies
Rationale, Supplemental Guidance, and Notes - Additional information on the requirement

Revision History

Version	Date	Changes
1.82	2014.02.10	Initial version published to http://www.ISASecure.org

Section	Reference ID and Name	Security Level
Identification & Authentication Control		
	FSA-S-IAC-1 Human user identification and authentication	1, 2, 3, 4
	FSA-S-IAC-1.1 Unique identification and authentication	2, 3, 4
	FSA-S-IAC-1.2 Multifactor authentication for untrusted networks	3, 4
	FSA-S-IAC-1.3 Multifactor authentication for all networks	4
	FSA-S-IAC-2 Software process and device identification and authentication	2, 3, 4
	FSA-S-IAC-2.1 Unique identification and authentication	3, 4
	FSA-S-IAC-3 Account management	1, 2, 3, 4
	FSA-S-IAC-3.1 Unified account management	3, 4
	FSA-S-IAC-4 Identifier management	1, 2, 3, 4
	FSA-S-IAC-5 Authenticator management	1, 2, 3, 4
	FSA-S-IAC-5.1 Initialize authenticator content	1, 2, 3, 4
	FSA-S-IAC-5.2 Change default authenticators	1, 2, 3, 4
	FSA-S-IAC-5.3 Change/ refresh all authenticators periodically	1, 2, 3, 4
	FSA-S-IAC-5.4 Protect authenticators	1, 2, 3, 4
	FSA-S-IAC-5.5 Hardware security for software process identity credentials	3, 4
	FSA-S-IAC-6 Wireless access management	1, 2, 3, 4
	FSA-S-IAC-6.1 Unique identification and authentication	2, 3, 4
	FSA-S-IAC-7 Strength of password-based authentication	1, 2, 3, 4
	FSA-S-IAC-7.1 Password generation and lifetime restrictions for human	3, 4
	FSA-S-IAC-7.2 Password lifetime restrictions for all users	4
	FSA-S-IAC-8 Public key infrastructure (PKI) certificates	2, 3, 4
	FSA-S-IAC-9 Strength of public key authentication	2, 3, 4
	FSA-S-IAC-9.1 Check validity of signature of a given certificate	2, 3, 4
	FSA-S-IAC-9.2 Construct a certification path to an accepted CA	2, 3, 4
	FSA-S-IAC-9.3 Check a given certificates revocation status	2, 3, 4
	FSA-S-IAC-9.4 Establish user control of private key	2, 3, 4
	FSA-S-IAC-9.5 Map authenticated identity to a user	2, 3, 4
	FSA-S-IAC-9.6 Hardware security for public key authentication	3, 4
	FSA-S-IAC-10 Authenticator feedback	1, 2, 3, 4
	FSA-S-IAC-11 Unsuccessful login attempts	1, 2, 3, 4
	FSA-S-IAC-12 System use notification	1, 2, 3, 4
	FSA-S-IAC-13 Access via untrusted networks	1, 2, 3, 4
	FSA-S-IAC-13.1 Explicit access request approval	2, 3, 4
Use Control		
	FSA-S-UC-1 Authorization enforcement	1, 2, 3, 4
	FSA-S-UC-1.1 Authorization enforcement for all users	2, 3, 4
	FSA-S-UC-1.2 Permission mapping to roles	2, 3, 4
	FSA-S-UC-1.3 Supervisor Override	3, 4
	FSA-S-UC-1.4 Dual Approval	4
	FSA-S-UC-2 Wireless use control	1, 2, 3, 4
	FSA-S-UC-2.1 Identify and report unauthorized wireless devices	3, 4
	FSA-S-UC-3 Use control for portable and mobile devices	1, 2, 3, 4
	FSA-S-UC-3.1 Preventing the use of portable and mobile devices	1, 2, 3, 4
	FSA-S-UC-3.2 Requiring context specific authorization	1, 2, 3, 4
	FSA-S-UC-3-3 Restricting code and data transfer to/from portable and mobile devices	1, 2, 3, 4
	FSA-S-UC-3.4 Enforcement of security status of portable and mobile devices	3, 4
	FSA-S-UC-4 Mobile code	1, 2, 3, 4
	FSA-S-UC-4.1 Preventing the execution of mobile code	1, 2, 3, 4
	FSA-S-UC-4.2 Requiring proper authentication and authorization for origin of the code	1, 2, 3, 4
	FSA-S-UC-4.3 Restricting mobile code transfer to/from the SUT	1, 2, 3, 4
	FSA-S-UC-4.4 Monitoring the use of mobile code	1, 2, 3, 4
	FSA-S-UC-4.5 Mobile code integrity check	3, 4
	FSA-S-UC-5 Session lock	1, 2, 3, 4
	FSA-S-UC-6 Remote session termination	2, 3, 4
	FSA-S-UC-7 Concurrent session control	3, 4
	FSA-S-UC-8 Auditable events	1, 2, 3, 4
	FSA-S-UC-8.1 Centrally managed, system-wide audit trail	3, 4
	FSA-S-UC-9 Audit storage capacity	1, 2, 3, 4
	FSA-S-UC-9.1 Warn when audit record storage capacity threshold reached	3, 4
	FSA-S-UC-10 Response to audit processing failures	1, 2, 3, 4
	FSA-S-UC-11 Timestamps	2, 3, 4
	FSA-S-UC-11.1 Internal time synchronization	3, 4
	FSA-S-UC-11.2 Protection of time source integrity	4
	FSA-S-UC-12 Non-repudiation	3, 4
	FSA-S-UC-12.1 Non-repudiation for all users	4
System Integrity		
	FSA-S-SI-1 Communication integrity	1, 2, 3, 4
	FSA-S-SI-1.1 Cryptographic Protection of Integrity	3, 4

Section	Reference ID and Name	Security Level
	FSA-S-SI-2 Malicious code protection	1, 2, 3, 4
	FSA-S-SI-2.1 Protection of entry and exit points	2, 3, 4
	FSA-S-SI-2.2 Central Management and reporting	3, 4
	FSA-S-SI-3 Security functionality verification	1, 2, 3, 4
	FSA-S-SI-3.1 Automated security verification	3, 4
	FSA-S-SI-3.2 Security verification during normal operation	4
	FSA-S-SI-4 Software and information integrity	1, 2, 3, 4
	FSA-S-SI-4.1 Automated notification about integrity violations	3, 4
	FSA-S-SI-5 Input validation	1, 2, 3, 4
	FSA-S-SI-6 Deterministic output	1, 2, 3, 4
	FSA-S-SI-7 Error handling	2, 3, 4
	FSA-S-SI-8 Session integrity	2, 3, 4
	FSA-S-SI-8.1 Invalidation of session IDs after session termination	3, 4
	FSA-S-SI-8.2 Unique session ID generation and recognition	3, 4
	FSA-S-SI-8.3 Randomness of session IDs	4
	FSA-S-SI-9 Protection of audit information	2, 3, 4
	FSA-S-SI-9.1 Audit records on write-once media	4
Data Confidentiality		
	FSA-S-DC-1 Information confidentiality	1, 2, 3, 4
	FSA-S-DC-1.1 Protection of confidentiality at rest or in transit via untrusted networks	2, 3, 4
	FSA-S-DC-1.2 Protection of confidentiality across zone boundaries	4
	FSA-S-DC-2 Information persistence	2, 3, 4
	FSA-S-DC-2.1 Purging of shared memory resources	3, 4
	FSA-S-DC-3 Use of cryptography	1, 2, 3, 4
Restricted Data Flow		
	FSA-S-RDF-1 Network Segmentation	1, 2, 3, 4
	FSA-S-RDF-1.1 Physical network segmentation	2, 3, 4
	FSA-S-RDF-1.2 Independence from non-SUT networks	3, 4
	FSA-S-RDF-1.3 Logical and physical isolation of critical networks	3, 4
	FSA-S-RDF-2 Zone Boundary protection	1, 2, 3, 4
	FSA-S-RDF-2.1 Deny by default, allow by exception	2, 3, 4
	FSA-S-RDF-2.2 Island Mode	3, 4
	FSA-S-RDF-2.3 Fail Close	3, 4
	FSA-S-RDF-3 General purpose person-to-person communication restrictions	1, 2, 3, 4
	FSA-S-RDF-3.1 Prohibit all general purpose person-to-person communications	3, 4
	FSA-S-RDF-4 Application Partitioning	1, 2, 3, 4
Timely Response to Event		
	FSA-S-TRE-1 Audit log accessibility	1, 2, 3, 4
	FSA-S-TRE-1.1 Programmatic access to audit logs	3, 4
	FSA-S-TRE-2 Continuous monitoring	2, 3, 4
Resource Availability		
	FSA-S-RA-1 Denial of Service Protection	1, 2, 3, 4
	FSA-S-RA-1.1 Manage Communication Loads	2, 3, 4
	FSA-S-RA-1.2 Limit (D)DoS effects to other systems or networks	3, 4
	FSA-S-RA-2 Resource Management	1, 2, 3, 4
	FSA-S-RA-3 Control System Backup	1, 2, 3, 4
	FSA-S-RA-3.1 Backup verification	2, 3, 4
	FSA-S-RA-3.2 Backup automation	3, 4
	FSA-S-RA-4 SUT recovery and reconstitution	1, 2, 3, 4
	FSA-S-RA-5 Emergency power	1, 2, 3, 4
	FSA-S-RA-6 Network and security configuration settings	1, 2, 3, 4
	FSA-S-RA-6.1 Machine-readable reporting of current security settings	3, 4
	FSA-S-RA-7 Least functionality	1, 2, 3, 4
	FSA-S-RA-8 SUT component inventory	2, 3, 4

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-IAC-1	Human user identification and authentication	The SUT shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the SUT to support segregation of duties and least privilege in accordance with applicable security policies and procedures.	Verify that the SUT can uniquely identify and authenticate all users at all accessible interfaces and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.1	1, 2, 3, 4	All human users need to be identified and authenticated for all access to the SUT. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or, 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 SUT. In addition to identifying and authenticating all human users at the SUT level (for example, at system logon), identification and authentication mechanisms are often employed at the application level. Where human users function as a single group (such as control room operators), user identification and authentication may be role-based or group-based. For some SUTs, the capability for immediate operator interaction is critical. It is essential that local emergency actions as well as SUT essential functions not be hampered by identification or authentication requirements (see clause 4 for a more complete discussion). Access to these systems may be restricted by appropriate physical security mechanisms (see ISA 62443 2 1 (99.02.01)). An example of such a situation is a critical operations room where strict physical access control and monitoring is in place and where shift plans allocate responsibility to a group of users. These users may then be using the same user identity. In addition, the designated operator workstation clients should be authenticated (see 5.4, SR 1.2 – Software process and device identification and authentication) or the use of this shared account should be limited to the constrained environment of the control room. In order to support IAC policies, as defined according to ISA 62443 2 1 (99.02.01), the SUT verifies the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user are enforced (see 6.3, SR 2.1 – Authorization enforcement).
FSA-S-IAC-1.1	Unique identification and authentication	The SUT shall provide the capability to uniquely identify and authenticate all human users.	Verify that the SUT can uniquely identify and authenticate all users at all user accessible interfaces and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.1 (1)	2, 3, 4	
FSA-S-IAC-1.2	Multifactor authentication for untrusted networks	The SUT shall provide the capability to employ multifactor authentication for human user access to the SUT via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).	Verify that the SUT can provide the capability of multifactor authentication for remote access and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.1 (2)	3, 4	Note: Access via untrusted networks to SUT components should be enabled only when necessary and approved.
FSA-S-IAC-1.3	Multifactor authentication for all networks	The SUT shall provide the capability to employ multifactor authentication for all human user access to the SUT.	Verify that the SUT can require multifactor authentication for local access (e.g. access within the zone) and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.1 (3)	4	
FSA-S-IAC-2	Software process and device identification and authentication	The SUT shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the SUT to support least privilege in accordance with applicable security policies and procedures.	Vendor shall provide list of all software processes and devices that can connect to the SUT. Verify that evidence exists that identification and authentication is done for each listed process and device and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.2	2, 3, 4	The function of identification and authentication is to map an ID to an unknown software process or device (henceforth referred to an entity in this sub-clause) so as to make it known before allowing any data exchange. Allowing rogue entities to send and receive SUT specific data can result in detrimental behavior of the legitimate SUT. All entities need to be identified and authenticated for all access to the SUT. 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 SUT. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technical infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied. Identification and authentication mechanisms for all entities are needed to protect against attacks such as man-in-the-middle or message spoofing. In some cases, these mechanisms may involve multiple software processes running on the same physical server, each having their own identity. In other cases, the identity may be bound to the physical device, such as all processes running on a given PLC. 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 SUTs, 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 SUT 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 ISA 62443 2 1 (99.02.01), the SUT 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, SR 2.1 – Authorization enforcement).
FSA-S-IAC-2.1	Unique identification and authentication	The SUT shall provide the capability to uniquely identify and authenticate all software processes and devices.	Vendor shall provide list of all software processes and devices that can connect to the SUT. Verify that evidence exists that each process and device that can connect to the SUT has a unique identification and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.2 (1)	3, 4	
FSA-S-IAC-3	Account management	The SUT shall provide the capability to support the management of all accounts, including establishing, activating, modifying, disabling and removing accounts.	Verify SUT supports account management functions by an administrator type role to establish, activate, modify, disable and remove accounts and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.3	1, 2, 3, 4	Account management may include grouping of accounts (for example, individual, role-based, device-based and system), establishment of conditions for group membership and assignment of associated authorizations. In certain SUT instances, where individual accounts are determined to be unnecessary from a risk-analysis and/or regulatory aspect, shared accounts are acceptable as long as adequate compensating controls (such as limited physical access) are in place and documented. Non-human user accounts (sometimes termed service accounts) that are utilized for process-to-process communication (for example, a human-machine interface (HMI) connecting to a database) typically require different security policies and procedures from human user accounts.
FSA-S-IAC-3.1	Unified account management	The SUT shall provide the capability to support unified account management	Verify SUT supports unified account management functions to establish, activate, modify, disable and remove accounts. Verify that performing these functions on an account is applicable to all components of the system that support user accounts and record results as: a. Supported, or	Yes	ISA-62443-3-3: SR1.3 (1)	3, 4	
FSA-S-IAC-4	Identifier management	The SUT shall provide the capability to support the management of identifiers (e.g. user ID) by user, group, role and/or SUT interface	Verify user documents indicate that SUT allows managing identifiers by user, group, role and / or interface and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.4	1, 2, 3, 4	Identifiers are distinguished from the privileges which they permit an entity to perform within a specific SUT control domain or zone (see 6.3, SR 2.1 – Authorization enforcement). Where human users function as a single group (such as control room operators), user identification may be role-based, group-based or device-based. For some SUTs, the capability for immediate operator interaction is critical. Local emergency actions for the SUT should not be hampered by identification requirements. Access to these systems may be restricted by appropriate compensating countermeasures. Identifiers may be required on portions of the SUT but not necessarily the entire SUT. For example, wireless devices typically require identifiers, whereas wired devices may not. The management of identifiers will be determined by local policies and procedures established in compliance with ISA 62443 2 1 (99.02.01).

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-IAC-5	Authenticator management	The SUT shall provide the capability to: a) initialize authenticator content; b) change all default authenticators upon SUT installation; c) change/refresh all authenticators; and d) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.	See child requirements	No	ISA-62443-3-3: SR1.5	1, 2, 3, 4	In addition to an identifier (see 5.6, SR 1.4 – Identifier management) an authenticator is required to prove identity. SUT 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. Human users should 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.
FSA-S-IAC-5.1	Initialize authenticator content	The SUT shall provide the capability to define initial authenticator content;	Verify user documents indicate ability to define initial authentication content and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.5 (a)	1, 2, 3, 4	
FSA-S-IAC-5.2	Change default authenticators	The SUT shall provide the capability to change default authenticators upon SUT installation;	Verify user documents indicate ability to change default authenticators and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.5 (b)	1, 2, 3, 4	
FSA-S-IAC-5.3	Change/ refresh all authenticators periodically	The SUT shall provide the capability to change/refresh authenticators periodically; and	Verify user documents indicate ability to change/refresh authenticators and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.5 (c)	1, 2, 3, 4	
FSA-S-IAC-5.4	Protect authenticators	The SUT shall provide the capability to protect authenticators from unauthorized disclosure and modification when stored and transmitted.	Verify user documents indicate ability to protect authenticators from unauthorized disclosure and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.5 (d)	1, 2, 3, 4	
FSA-S-IAC-5.5	Hardware security for software process identity credentials	For software process and device users, the SUT shall provide the capability to protect the relevant authenticators via hardware mechanisms.	Verify user documents indicate ability to protect relevant authenticators with hardware mechanisms and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.5 (1)	3, 4	
FSA-S-IAC-6	Wireless access management	The SUT shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Review user documentation and determine if wireless communication is supported on the SUT. If not record the result as: a. Not Applicable If wireless is communication is supported vendor shall provide list of all software processes and devices that can connect to the SUT via the wireless connection. Verify that evidence exists that identification and authentication is done for each listed process and device and for human users and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.6	1, 2, 3, 4	Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus 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. For this and possibly other reasons (for example regulatory differences), a risk analysis might legitimately result in a higher SL-T(IAC,SUT) for wireless communications versus a wired protocol being used in an identical use case. Wireless technologies include, but are not limited to, microwave, satellite, packet radio, Institute of Electrical and Electronics Engineers (IEEE) 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – Wireless HART®, ISA 100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.
FSA-S-IAC-6.1	Unique identification and authentication	The SUT shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.	Review user documentation and determine if wireless communication is supported on the SUT. If not record the result as: a. Not Applicable If wireless is communication is supported vendor shall provide list of all software processes and devices that can connect to the SUT via the wireless connection. Verify that evidence exists that each process and device that can connect to the SUT has a unique identification and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.6 (1)	2, 3, 4	
FSA-S-IAC-7	Strength of password-based authentication	For SUT utilizing password-based authentication, the SUT shall provide the capability to enforce password strength restrictions	See child requirements	No	ISA-62443-3-3: SR1.7	1, 2, 3, 4	User authentication based on a username and a secret password is a very commonly used mechanism. Many attacks on such mechanisms focus on guessing the password (for example, dictionary attacks or targeted social engineering) or breaking the cryptographic protection of the stored password representation (for example, using rainbow tables or brute-forcing a hash collision). Increasing the size of the set of valid passwords by increasing the number of allowed characters makes such attacks more complex, but only if the increased set size is actually used (generally users would tend to not include special characters in a password as they are perceived harder to remember). Limiting the lifetime of a password decreases the window of opportunity for an attacker to breach a given password's secrecy. In order to prevent users from circumventing this control by once changing their password to a new one and then immediately changing back to their original password, a minimum lifetime for a password is commonly enforced as well. A notification to change the password prior the expiration allows the user to change the password at a convenient time according to process operations conditions.
FSA-S-IAC-7.1	Password generation and lifetime restrictions for human users	The SUT shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the SUT shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices.	Verify user documents indicate that password re-use can be limited for a specified number of generations and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.7 (1)	3, 4	This protection can be further enhanced by limiting the reuse of passwords (preventing small sets of alternating passwords), which further decreases the usefulness of a once-breached password. Extended protection beyond password based mechanisms can be achieved using multifactor authentication (see 4.3, SR 1.1 – Human user, process and device identification and authentication).
FSA-S-IAC-7.2	Password lifetime restrictions for all users	For SUT utilizing password-based authentication, the SUT shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users	Verify user documents indicate that the SUT provides the capability to enforce password minimum and maximum lifetime restrictions for all users and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.7 (2)	4	
FSA-S-IAC-8	Public key infrastructure (PKI) certificates	Where PKI is utilized, the SUT shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.	Verify user documents indicate that the required public key authentication are supported if public key functionality is offered and record results as: a. Supported, or b. Not Supported, or c. NA - if public key is not supported	No	ISA-62443-3-3: SR1.8	2, 3, 4	Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. Any latency induced from the use of public key certificates should not degrade the operational performance of the SUT. 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 SUT versus on the Internet, and the list of trusted CAs should be considered in the policy and depends on the network architecture (see also ISA 62443 2 1 (99.02.01)).

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-IAC-9	Strength of public key authentication	For SUTs utilizing public key authentication, the SUT shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; b) validate certificates by constructing a certification path to an accepted certification authority (CA)CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; and e) map the authenticated identity to a user (human, software process or device).	See child requirements	No	ISA-62443-3-3: SR1.9	2, 3, 4	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 SUT 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 SUT environment.
FSA-S-IAC-9.1	Check validity of signature of a given certificate	validate certificates by checking the validity of the signature of a given certificate	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, provide a certificate with an invalid signature to a test system. Verity that the system detects this problem and reports this problem to the user. Verify that the connection is denied unless the user chooses to allow the connection anyway and record results as: a. Supported b. Not Supported	Yes	ISA-62443-3-3: SR1.9 (a)	2, 3, 4	
FSA-S-IAC-9.2	Construct a certification path to an accepted CA	validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued;	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, review design documentation and determine if the system validates certificates by construction a certification path to an accepted CA or in the case of self-signed certificates, by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued and record results as: b. Supported c. Not Supported	No	ISA-62443-3-3: SR1.9 (b)	2, 3, 4	
FSA-S-IAC-9.3	Check a given certificates revocation status	validate certificates by checking a given certificate's revocation status;	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, provide a certificate with a revoked status. verify that the system detects this problem and reports this problem to the user. Verify that the connection is denied unless the user chooses to allow the connection anyway and record results as: a. Supported b. Not Supported	Yes	ISA-62443-3-3: SR1.9 (c)	2, 3, 4	
FSA-S-IAC-9.4	Establish user control of private key	establish user (human, software process or device) control of the corresponding private key	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, provide a certificate with an valid signature and non-revoked status to a test system. verify that the system allows this connection and accepts the data from this server and record results as: a. Supported b. Not Supported	Yes	ISA-62443-3-3: SR1.9 (d)	2, 3, 4	
FSA-S-IAC-9.5	Map authenticated identity to a user	map the authenticated identity to a user (human, software process or device)	Test for FSA-S-IAC-9.4 covers this item as well	Yes	ISA-62443-3-3: SR1.9 (e)	2, 3, 4	
FSA-S-IAC-9.6	Hardware security for public key authentication	The SUT shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations	Review user documentation and determine if public key authentication is used. If not record results as: a. Not applicable If public key authentication is used, review design documentation if hardware mechanisms according to commonly accepted security industry practices and recommendations are used to protect the relevant private keys and record results as: b. Supported c. Not Supported	No	ISA-62443-3-3: SR1.9 (1)	3, 4	
FSA-S-IAC-10	Authenticator feedback	The SUT shall provide the capability to obscure feedback of authentication information during the authentication process	Verify SUT is capable of obscuring feedback of authentication information and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.10	1, 2, 3, 4	Obscuring the 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 password obscures feedback of authentication information. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as "unknown user name".
FSA-S-IAC-11	Unsuccessful login attempts	The SUT shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The SUT shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the SUT shall provide the capability to disallow interactive logons.	Verify SUT is capable of monitoring of unsuccessful login attempts with configurable ability to deny access permanently or for a configurable time period based on repeated unsuccessful attempts and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.11	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 SUT 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, process or device) to gain access if they have the correct login identifier. Automatic denial of access for SUT 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 total system failure or injury to personnel.

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-IAC-12	System use notification	The SUT shall provide the capability to display a configurable system use notification message before authenticating.	Verify SUT is capable of displaying user configurable system use notifications and records results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.12	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 does not improve IACS security. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the SUT. A warning banner implemented as a posted physical notice in the SUT 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 specific SUT; 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.
FSA-S-IAC-13	Access via untrusted networks	The SUT shall provide the capability to monitor and control all methods of access to the SUT via untrusted networks.	Verify user documents include the capability to monitor and control all forms of remote access via untrusted networks is supported and records results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.13	1, 2, 3, 4	Examples of access to the SUT 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-SUT) network. The SUT should restrict access achieved through dial-up connections (for example, limiting dial-up access based upon the source of the request) or protect against unauthorized connections or subversion of authorized connections (for example, using virtual private network technology). Security policies and procedures may require multifactor authentication for remote user access to the SUT
FSA-S-IAC-13.1	Explicit access request approval	The SUT shall provide the capability to deny ~~remote~~ access requests by default (e.g. access via untrusted networks) unless explicitly approved by an assigned role.	Verify user documents include the capability to deny remote access by default and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR1.13 (1)	2, 3, 4	Access via untrusted networks to geographically remote SUT component locations (for example, control centers and field locations) should only be enabled when necessary and authenticated.

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-UC-1	Authorization enforcement	On all interfaces, the SUT shall provide the capability to enforce authorizations assigned to all human users for controlling use of the SUT to support segregation of duties and least privilege.	Verify SUT enforces authorizations for human users to control use of the SUT as configured by account management and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.1	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 objects (for example, devices, files, records, software processes, programs and domains). After the SUT has verified the identity of a user (human, software process or device) and SUT objects (see 4.3, SR 1.1 – Human user, 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 SUT would check which roles are assigned to a verified user or object 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 SUT.
FSA-S-UC-1.1	Authorization enforcement for all users	On all interfaces, the SUT shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the SUT to support segregation of duties and least privilege.	Verify SUT enforces authorizations for processes and devices to control use of the SUT as configured by account management and record results as: a. Supported, or b. Not Supported c. Not applicable if software processes and devices are not supported as users.	No	ISA-62443-3-3: SR2.1 (1)	2, 3, 4	
FSA-S-UC-1.2	Permission mapping to roles	The SUT shall provide the capability for an authorized user or role to modify the mapping of permissions to roles for human users	Verify SUT provides the capability to map permisions to roles if authorized by a supervisory level account and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.1 (2)	2, 3, 4	Roles should not be limited to fixed nested hierarchies in which a higher level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges. This RE should be applicable to software processes and devices as well.
FSA-S-UC-1.3	Supervisor Override	The SUT shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence	Verify that the SUT can support a configurable time limit or event sequence limit for supervisor manual override, if provided, and record results as: a. Supported, or b. Not Supported, or c. Not Applicable (if supervisor manual override is not supported)	No	ISA-62443-3-3: SR2.1 (3)	3, 4	NOTE Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events is often needed. This allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege user.
FSA-S-UC-1.4	Dual Approval	The SUT shall support dual approval where an action can result in serious impact on the industrial process	Verify that the SUT can provide the capability of dual approval if required and record reulsts as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.1 (4)	4	NOTE Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard health, safety or environmental (HSE) consequences, for example, emergency shutdown of a process.
FSA-S-UC-2	Wireless use control	The SUT shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the SUT according to commonly accepted security industry practices.	Verify that the SUT can provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the SUT per commonly accepted security practices and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.2	1, 2, 3, 4	Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same IACS security requirements as any other communication type utilized by the IACS. However, a risk analysis may result in a requirement for wireless IACS components to support higher use control capabilities than are typically required of wired systems for the same use case and SL-T. Regulatory differences may also result in different required capabilities between wired and wireless communications. As noted in 5.8, SR 1.6 – Wireless access management, wireless technologies include, but are not limited to, microwave, satellite, packet radio, IEEE 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – WirelessHART®, ISA 100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.
FSA-S-UC-2.1	Identify and report unauthorized wireless devices	The SUT shall provide the capability to identify and report unauthorized wireless devices transmitting within the SUT physical environment.	Place an unauthorized wireless device within the SUT physical environment. Verify that the SUT identifies and reports that the unauthorized device has been detected and record results as: a. Supported b. Not Supported c. Not applicable if the system does not support wireless communications.	Yes		3, 4	
FSA-S-UC-3	Use control for portable and mobile devices	The SUT shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.	See Child Requirements	No	ISA-62443-3-3: SR2.3	1, 2, 3, 4	Portable and mobile devices (such as USB drives, portable harddrives, laptops, etc.) may introduce undesired network traffic, malware and/or information exposure, so there should be specific control associated with their usage in the typical SUT environment. Security policies and procedures may not allow certain functions or activities via portable and/or mobile devices. Note: Protecting information residing on portable and mobile devices (for example, employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered elsewhere (see Clause 7, FR 4 – Data confidentiality).
FSA-S-UC-3.1	Preventing the use of portable and mobile devices	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices;	Review user documentation and verify that the SUT provides a means to prevent the use of portable and mobile devices and record the results as: a. Supported b. Not Supported	No	ISA-62443-3-3: SR2.3 (a)	1, 2, 3, 4	
FSA-S-UC-3.2	Requiring context specific authorization	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: b) requiring context specific authorization	Review user documentation and verify that the SUT provides a means to authorize the use of portable and mobile devices in context specific situations and record the results as: a. Supported b. Not Supported	No	ISA-62443-3-3: SR2.3 (b)	1, 2, 3, 4	

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-UC-3.3	Restricting code and data transfer to/from portable and mobile devices	The control system shall provide the capability to automatically enforce configurable usage restrictions that include: c) restricting code and data transfer to/from portable and mobile devices.	Configure the system such that portable and mobile devices are not permitted in a certain context. Connect such a device to the system within the prohibited context and attempt to transfer data between the device and the system. Verify that no data can be sent to or from this device and record results as: a. Supported b. Not Supported	Yes	ISA-62443-3-3: SR2.3 (c)	1, 2, 3, 4	
FSA-S-UC-3, 4	Enforcement of security status of portable and mobile devices	The SUT shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.	Identify the security requirements of the SUT (which can be considered a zone). This information should be documented in the security requirements specification for the system. Review system documentation to verify that the system can verify that each of these security requirements are met by any portable or mobile devices attemting to connect to the SUT. If it is not possible or easy to verify that a requirement is met from the system documentation, then a test of the system may be conducted to verify that such a requirement has been met. Record results as: a. Supported b. Not supported c. Not applicable if portable or mobile devices cannot connect to the system.	No	ISA-62443-3-3: SR2.3 (1)	3, 4	
FSA-S-UC-4	Mobile code	The SUT shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the SUT that include: a) preventing the execution of mobile code; b) requiring proper authentication and authorization for origin of the code; c) restricting mobile code transfer to/from the SUT; and d) monitoring the use of mobile code.	See Child Requirements	No	ISA-62443-3-3: SR2.4	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 SUT. For example, mobile code exchanges may be disallowed directly with the SUT, but may be allowed in a controlled adjacent environment maintained by SUT personnel.
FSA-S-UC-4.1	Preventing the execution of mobile code	The SUT shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the SUT that include: a) preventing the execution of mobile code;	Review system documentation and verify that the execution of mobile code is always prevented or that there is a configurable option to prevent such code from being transferred into the SUT and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.4 (a)	1, 2, 3, 4	
FSA-S-UC-4.2	Requiring proper authentication and authorization for origin of the code	The SUT shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the SUT that include: b) requiring proper authentication and authorization for origin of the code;	Review system documentation and verify that if the execution of mobile code is allowed, then the mobile code must be authenticated before it is allowed to run. In addition, verify that there is authorization as to which interfaces the mobile code can be transferred onto the SUT to execute. Record the results as: A. Supported, or B. Not Supported	No	ISA-62443-3-3: SR2.4 (b)	1, 2, 3, 4	
FSA-S-UC-4.3	Restricting mobile code transfer to/from the SUT	The SUT shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the SUT that include: c) restricting mobile code transfer to/from the SUT; and	Connect a device to the SUT that contains mobile code not authorized to transfer to the SUT. Verify that the transfer is prevented and the user is notified of this occurrence. Record the results as: A. Supported B. Not Supported C. Not applicable if the device does not allow any mobile code to execute.	Yes	ISA-62443-3-3: SR2.4 (c)	1, 2, 3, 4	
FSA-S-UC-4.4	Monitoring the use of mobile code	The SUT shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the SUT that include: d) monitoring the use of mobile code.	Connect a device to the SUT that contains mobile code authorized to transfer to the SUT. Verify that the transfer is successful and the user is notified of this occurrence. Record the results as: A. Supported B. Not Supported C. Not applicable if the device does not allow any mobile code to execute.	Yes	ISA-62443-3-3: SR2.4 (d)	1, 2, 3, 4	
FSA-S-UC-4.5	Mobile code integrity check	The SUT shall provide the capability to verify integrity of the mobile code before allowing code execution.	Review system documentation and verify that there is an integrity check that must be run before allowing mobile code exectuion and record the results as: A. Supported, or B. Not supported, or C. Not applicable if the device does not allow any mobile code to execute.	No	ISA-62443-3-3: SR2.4 (1)	3, 4	

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-UC-5	Session lock	The SUT shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or manual initiation. The session lock shall remain in effect until the human user or authorized supervisory personnel re-establishes access using appropriate identification and authentication procedures.	Verify user documents include evidence that Session Locking Timeout is supported and records results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.5	1, 2, 3, 4	The entity responsible for an SUT should employ session lock to prevent access to specified workstations or nodes. The SUT should activate session lock mechanisms automatically after a configurable time period for designated workstations or nodes. In some cases, session lock for SUT operator workstations or nodes is not advised (for example, sessions which are required for immediate operator responses in emergency situations). Session locks are not a substitute for logging out of the SUT. In situations where the SUT cannot support session lock, the responsible entity should employ appropriate compensating controls (for example, providing increased physical security, personnel security and auditing measures).
FSA-S-UC-6	Remote session termination	The SUT shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.	Verify the SUT is able to be configured to automatically terminate a remote session after a configurable time and records results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR2.6	2, 3, 4	A remote session is initiated whenever an SUT 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 SUT monitoring and maintenance activities (not critical operations) based on the risk assessment of the SUT and security policies and procedures. Some SUT or components may not allow sessions to be terminated
FSA-S-UC-7	Concurrent session control	The SUT shall provide the capability to limit the number of concurrent remote sessions per interface for any given user (human, software process or device) to a configurable number of sessions.	Verify the SUT is able to be configured to limit the number of concurrent remote sessions and record results as: a. Supported, or b. Not Supported	No	ISA-624423-3-3: SR2.7	3, 4	A resource starvation denial of service (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 SUT resources. Product supplier and/or systems integrator guidance is likely required to provide sufficient information as to how the number of sessions value should be assigned.
FSA-S-UC-8	Auditable events	The SUT shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, SUT events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.	Verify via user documtation SUT supports capability to generate audit records for the following categories: access control, request errors, system events, configuration changes, potential reconnaissance activity and audit log events and record results as: a. Supported, or b. Partially Supported -if not all specified criteria, or c. Not Supported	No	ISA-624423-3-3: SR2.8	1, 2, 3, 4	The purpose of this requirement is to record the occurrence of important events which need to be audited as significant and relevant to the security of the SUT. Auditing activity can affect SUT performance. The security audit function is usually coordinated with the network health and status monitoring function which may be in a different zone. Commonly recognized and accepted checklists and configuration guides should be considered when compiling a list of auditable events. The security policies and procedures should define auditable events that are adequate to support after-the-fact investigations of security incidents. In addition, audit records should be sufficient to monitor the effectiveness and proper operation of the security mechanisms utilized to meet the requirements in this standard. It should be noted that the requirement for event recording is applicable within the given system functionality, specifically given system security requirements on a given level. For example, the requirement for recording of authentication events (in the access control category) on a SL 1 system is only applicable to the level of authentication functionality required for SL 1 according to the requirements in clause 5. Events may occur in any SUT component (for example login events) or may be observed by dedicated monitors. For example, port scanning might be detected by an intrusion detection system (IDS) or intrusion prevention system (IPS).
FSA-S-UC-8.1	Centrally managed, system-wide audit trail	The SUT shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the SUT into a system-wide (logical or physical), time-correlated audit trail. The SUT shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).	Verify via user documtation SUT supports capability to compile audit records from multiple components throughout the system and record results as: a. Supported, or b. Not Supported	No	ISA-624423-3-3: SR2.8 (1)	3, 4	
FSA-S-UC-9	Audit storage capacity	The SUT shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The SUT shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.	Review audit record storage cpactiy and determine how many records can be stored. Estimate rate of audit record generation based on existing systems. Verify that there is sufficient storage for at least 30 days of audit information based on record generation on existing systems. Review system documentation and verify that the SUT provides mechanisms to reduce the likelihood of this capacity being exceeded (such as warnings when approach the limit or periodic archiving of audit records).	No	ISA-624423-3-3: SR2.9	1, 2, 3, 4	The SUT should provide sufficient audit storage capacity, taking into account retention policy, the auditing to be performed and the online audit processing requirements. Guidelines to be considered could include the NIST Special Publication (SP) 800 92 [29]. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.
FSA-S-UC-9.1	Warn when audit record storage capacity threshold reached	The control system shall provide the capability to issue a warning when allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.	Review user documentation and confirm that the control system will provide a warning when allocated audit record storage volume reaches a configurable percentage of the maximum audit record storage capacity. Record results as: A. Supported B. Not Supported	No	ISA-624423-3-3: SR2.9 (1)	3, 4	
FSA-S-UC-10	Response to audit processing failures	The SUT shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The SUT 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 audit function support the following for lack of storage space to record new events: overwrite oldest audit records and stop generating audit records and records results as: a. Supported, or b. Not Supported	No	ISA-624423-3-3: SR2.10	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 SP800 92. 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.
FSA-S-UC-11	Timestamps	The SUT shall provide system generated timestamps for use in audit record generation.	Verify that system-wide audit records include timestamps by looking at system audit logs and recorded results as: a. Supported, or b. Not Supported	No	ISA-624423-3-3: SR2.11	2, 3, 4	Timestamps (including date and time) of audit records should be generated using internal system clocks. If system-wide time synchronization is not present (which is typical in many installations), known offsets would be needed to support analysis of a sequence of events. In addition, synchronization of internally generated audit records with external events might require synchronization with a generally recognized external time source (such as the Global Positioning System (GPS), Global Navigation Satellite System (GLONASS) and Galileo). The time source should be protected from unauthorized alteration.
FSA-S-UC-11.1	Internal time synchronization	The SUT shall provide the capability to synchronize internal system clocks at a configurable frequency.	Verify user documents include evidence that time synchronization for Time Stamp is provided and record results as: a. Supported, or b. Not Supported	No	ISA-624423-3-3: SR2.11 (1)	3, 4	

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-UC-11.2	Protection of time source integrity	The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration.	Verify user documents include evidence that time synchronization for Time Stamp is protected from unauthorized alteration and record results as: a. Supported, or b. Not Supported	No	ISA-624423-3-3: SR2.11 (2)	4	
FSA-S-UC-12	Non-repudiation	The SUT shall provide the capability to determine whether a given human user took a particular action	Verify user documents include evidence that documentation that the human user responsible for initiation of an event may be included in the audit records and records results as: a. **Supported**, or b. **Not Supported**	No	ISA-624423-3-3: SR2.12	*3, 4*	Examples of particular actions taken by a user include performing operator actions, changing SUT 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, digital signatures, digital message receipts and timestamps).
FSA-S-UC-12.1	Non-repudiation for all users	The SUT shall provide the capability to determine whether a given user (human, software process or device) took a particular action.	Verify user documents include evidence that documentation that the device or process responsible for initiation of an event (including process or device users) may be included in the audit records and records results as: a. **Supported**, or b. **Not Supported**	No	ISA-624423-3-3: SR2.12 (1)	4	

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-SI-1	Communication integrity	The SUT shall provide the capability to protect the integrity of transmitted information.	No validation activity needed as covered by validation of the child requirements	NA	ISA-62443-3-3: SR3.1	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 SUT 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, SR 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.
FSA-S-SI-1.1	Cryptographic Protection of Integrity	The SUT shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.	Examine design and user documents and determine if integrity of mission critical data transmitted over communication channels is protected via cryptographic measures and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.1 (1)	3, 4	NOTE The use of cryptographic mechanisms to provide message authentication and integrity should be determined after careful consideration of the security needs and the potential ramifications on system performance and capability to recover from system failure. Alternative physical protection measures include, but are not limited to, protected distribution systems.
FSA-S-SI-2	Malicious Code Protection	The SUT shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The SUT shall provide the capability to update the protection mechanisms.	No validation activity needed as covered by validation of the child requirements	NA	ISA-62443-3-3: SR3.2	1, 2, 3, 4	The SUT should use protection mechanisms to prevent, detect, mitigate and report instances of detected malicious code (for example, viruses, worms, Trojan horses and spyware) transported by electronic mail, electronic mail attachments, Internet access, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops or other common means. 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. Mitigation techniques may include, but are not limited to, file cleaning, quarantining, file deletion, host communication restriction and IPSs. Prevention techniques may include, but are not limited to, application blacklisting and whitelisting techniques, 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, SR 6.2 – Continuous monitoring for an associated requirement involving SUT monitoring tools and techniques. Prevention and mitigation mechanisms may include those designed for host elements (such as computers and servers) and network-based mechanisms (such as IDSs and IPSs) and those mechanisms focused on SUT specific components (such as PLCs and HMIs).
FSA-S-SI-2.1	Protection of entry and exit points	The SUT shall provide the capability to employ malicious code protection mechanisms at all entry and exit points	Verify SUT provides the capability to employ malicious code protection at zone boundaries and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.2 (1)	2, 3, 4	Note: Mechanisms at this level may include removable media, firewalls, unidirectional gateways, web servers, proxy servers and remote-access servers.
FSA-S-SI-2.2	Central Management and reporting	The SUT shall provide the capability to manage malicious code protection mechanisms.	Verify through design document review that the SUT provides the capability to centrally manage malicious code protection mechanisms and record results as: a. Supported, or b. Note Supported	No	ISA-62443-3-3: SR3.2 (2)	3, 4	NOTE Such mechanisms may be provided by endpoint infrastructure centralized management and SIEM solutions

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-SI-3	Security functionality verification	The SUT shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.	No validation activity needed as covered by validation of the child requirements	NA	ISA-62443-3-3: SR3.3	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 measures by European Institute for Computer Antivirus Research (EICAR) testing of the SUT file system. Antivirus software should detect this and appropriate incident handling procedures should be triggered. • Verification of the identification, authentication and use control measures by attempting access with an unauthorized account (for some functionality this could be automated). • Verification of 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
FSA-S-SI-3.1	Automated security verification	The SUT shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance	Verify SUT or SUT documentation provides methods to verify security functions during FAT, SAT or scheduled maintenance and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.3 (1)	3, 4	
FSA-S-SI-3.2	Security verification during normal operation	The SUT shall provide the capability to support verification of the intended operation of security functions during normal operations	Verify SUT provides methods to test security functions during normal operation and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.3 (2)	4	NOTE This RE needs to be carefully implemented to avoid detrimental effects. May not be suitable for safety systems.
FSA-S-SI-4	Software and information integrity	The SUT shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest	Verify SUT or SUT documentation provides manual or automated integrity mechanisms (such as cryptographic hashes) to verify the integrity of critical SUT software and configuration information and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.4	2, 3, 4	Unauthorized changes are changes for which the entity attempting the change does not have the required privileges. This SR complements related SRs from FRs 1 and 2. FRs 1 and 2 involve enforcing the roles, privileges and use patterns as designed. 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. The SUT 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).
FSA-S-SI-4.1	Automated notification about integrity violations	The SUT shall provide automated tools that detect, record, and provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.	Verify SUT provides automated methods to verify software and configuration integrity with automated notification and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.4 (1)	3, 4	
FSA-S-SI-5	Input validation	The SUT shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the SUT.	Verify SUT or SUT documentation provides manual or automated methods to verify integrity of information from external sources and records results as: a. Supported, or b. Not Supported, or c. NA - SUT does not accept process control inputs from external sources	No	ISA-62443-3-3: SR3.5	1, 2, 3, 4	Rules for checking the valid syntax of SUT inputs 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 SR, 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 could include the Open Web Application Security Project (OWASP) [33] Code Review Guide.
FSA-S-SI-6	Deterministic output	The SUT shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.	Review system documentation and verify that the system will set outputs to a predetermined state if normal operation can not be maintained as a result of an attack. Record results as: a. Supported, or b. Not Supported.	No	ISA-62443-3-3: SR3.6	1, 2, 3, 4	The deterministic behavior of SUT outputs as a result of threat actions against the SUT is an important characteristic to ensure the integrity of normal operations. Ideally, the SUT continues to operate normally while under attack, but if the SUT cannot maintain normal operation, then the SUT outputs need to fail to a predetermined state. The appropriate predetermined state of SUT outputs is application 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 • Fixed – the outputs fail to a fixed value that is determined by the asset owner or an application

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-SI-7	Error handling	The SUT shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.	Verify that SUT error messages provide sufficient and necessary information to assist plant personnel to identify and diagnose system problems without revealing sensitive information that could be used by attackers to exploit the system and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR3.7	2, 3, 4	The structure and content of error messages should be carefully considered by the product supplier and/or systems integrator. Error messages generated by the SUT should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Since it may be unclear whether a particular error condition is due to a security event, all error messages may need to be easily accessible during incident response. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include the OWASP Code Review Guide.
FSA-S-SI-8	Session integrity	The SUT shall provide the capability to protect the integrity of sessions. The SUT shall reject any usage of invalid session IDs.	No validation activity needed as covered by validation of the child requirements	NA	ISA-62443-3-3: SR3.8	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 or insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use must be considered in light of requirements for real-time communications.
FSA-S-SI-8.1	Invalidation of session IDs after session termination	The SUT shall provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).	Verify that user session identifiers are invalidated upon user logout and record results as: a. Supported, or b. Not Supported, or c. NA - if does not support sessions or session IDs	No	ISA-62443-3-3: SR3.8 (1)	3, 4	
FSA-S-SI-8.2	Unique session ID generation and recognition	The SUT shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid	Verify that user session identifiers are unique and that session IDs not generated by the system are rejected and record results as: a. Supported, or b. Not Supported, or c. NA - if does not support sessions or session Ids	No	ISA-62443-3-3: SR3.8 (2)	3, 4	
FSA-S-SI-8.3	Randomness of session IDs	The SUT shall provide the capability to generate unique session IDs with commonly accepted sources of randomness	Verify that user session identifiers are generated by the system with an accepted level of randomness and record results as: a. Supported, or b. Not Supported, or c. NA - if does not support sessions or session Ids	No	ISA-62443-3-3: SR3.8 (3)	4	NOTE 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 which were not properly invalidated after session termination. Therefore the validity of a session authenticator must 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
FSA-S-SI-9	Protection of audit information	The SUT shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.	Review system documentation and verify that audit information and audit tools (if present) require authorization in order to access, modify or delete. Attempt to delete an audit log as an unauthorized user and verify that access is denied. Record results as: a. Supported, or b. Not Supported	Yes	ISA-62443-3-3: SR3.9	2, 3, 4	Audit information includes all information (for example, audit records, audit settings and audit reports) needed to successfully audit SUT 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.
FSA-S-SI-9.1	Audit records on write-once media	The SUT shall provide the capability to produce audit records on hardware-enforced write-once media.	Review system documentation and verify that the system has the capability to produce audit records on hardware enforced write once media. Record results as: a. Supported, or b. Not supported	No	ISA-62443-3-3: SR3.9 (1)	4	

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-DC-1	Information confidentiality	The SUT shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.	Review system documentation and verify if the system has the ability to protect the confidentiality of information for which explicit read authorization is supported (either all of the time or as a configurable option). If the user must configure or setup the system in a certain manner to meet this requirement, verify that this is clearly documented in a user manual. Record the results as: a. Supported, or b. Not Supported.	No	ISA-62443-3-3: SR4.1	1, 2, 3, 4	Protection of information, at rest or in transit, can be maintained through physical means, compartmentalization or encryption, among other techniques. It is crucial that the technique chosen considers the potential ramifications on SUT performance and the capability to recover from system failure or attack. The decision whether the confidentiality of a given piece of 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 SUT is an indicator that this information is considered confidential by the organization. Thus, all information for which the SUT supports the capability to assign explicit read authorizations should be considered potentially confidential and thus the SUT should also provide the capability to protect it. Different organizations and industries may require different levels of encryption strength for different categories of information, based on the sensitivity of the information as well as industry standards and regulatory requirements (see 8.5, SR 4.3 – Use of cryptography). In some situations network configuration information stored and processed in switches and routers may be considered as confidential.
FSA-S-DC-1.1	Protection of confidentiality at rest or in transit via untrusted networks	The SUT shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.	Review system documentation and verify if the system has the ability to protect the confidentiality of information traversing an untrusted network. If the user must configure or setup the system in a certain manner to meet this requirement, verify that this is clearly documented in a user manual. Record the results as: a. Supported, or b. Not Supported.	No	ISA-62443-3-3: SR4.1 (1)	2, 3, 4	NOTE Cryptography is a common mechanism for ensuring information confidentiality.
FSA-S-DC-1.2	Protection of confidentiality across zone boundaries	The SUT shall provide the capability to protect the confidentiality of information traversing any zone boundary.	Review system documentation and verify if the system has the ability to protect the confidentiality of information traversing any zone boundary. If the user must configure or setup the system in a certain manner to meet this requirement, verify that this is clearly documented in a user manual. Record the results as: a. Supported, or b. Not Supported.	No	ISA-62443-3-3: SR4.1 (2)	4	
FSA-S-DC-2	Information persistence	The SUT shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.	Review system documentation and verify that the system has the ability to purge all information for which explicit read authorization is supported. Verify that the data is purged from the system such that it can not be recreated. Record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR4.2	2, 3, 4	Removal of a SUT 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 would include ‘join keys’ (in the case of some wireless field devices) 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 SUT information or data persistence prevents information stored on a shared resource from being unintentionally disclosed after that resource has been released back to the SUT.

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-DC-2.1	Purging of shared memory resources	The SUT shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.	Review system documentation and verify that confidential information is purged from RAM before that memory is released back to the SUT for use by a different user. Review system documentation and verify that confidential information is not stored in memory that can be accessed by unauthorized programs or users. Record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR4.2 (1)	3, 4	NOTE Volatile memory resources are those which generally do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) which might extract key material or other confidential data before it is actually over-written. Therefore, when volatile shared memory is released back to the SUT for use by a different user, all unique data and connections to unique data need to be purged from the resource so it is not visible or accessible to the new user.
FSA-S-DC-3	Use of cryptography	If cryptography is required, the SUT shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted industry practices and recommendations	Verify through design documentation that if the SUT uses cryptography then algorithms, key sizes and mechanisms for key establishment are done according to commonly accepted industry best practices and recommendations and record results as: a. Supported, b. Not Supported, or c. NA (cryptography is not used)	No	ISA-62443-3-3: SR4.3	1, 2, 3, 4	The selection of cryptographic protection should match the value of the information being protected, the consequences of the confidentiality of the information being breached, the time period during which the information is confidential and the SUT operating constraints. This can involve either information at rest or in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality assessment process. The SUT product supplier should document the practices and procedures relating to cryptographic key establishment and management. The SUT should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithms (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 standards such as NIST SP800 57 [23]. This SR, along with 7.6, SR 4.4 – Public key infrastructure certificates, may be applicable when meeting many other requirements defined within this standard (for example, Clauses 4 and 6).

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-RDF-1	Network Segmentation	The SUT shall provide the capability to segment SUT networks from non-SUT networks and to segment critical SUT networks from other SUT networks	No validation activity needed as covered by validation of the child requirements	NA	ISA-62443-3-3: SR5.1	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 SUT and reduce the spread, or egress, of network traffic from a SUT. 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 SUT, including critical SUTs and safety-related systems, to be segmented from other systems for an additional level of protection. Access from the SUT to the World Wide Web should be clearly justified based on SUT 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 SUTs. 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 ISA 99.02.01). 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 SUT 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 SUTs and safety-related systems be designed from the beginning to be completely isolated from other networks.
FSA-S-RDF-1.1	Physical network segmentation	The SUT shall provide the capability to physically segment SUT networks from non-SUT networks and to physically segment critical SUT networks from non-critical SUT networks	Verify through user documentation that the SUT provides the capability to segment SUT networks from non-SUT networks and to physically segment critical SUT networks from other SUT networks and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR5.1 (1)	2, 3, 4	
FSA-S-RDF-1.2	Independence from non-SUT networks	The SUT shall have the capability to provide network services to SUT networks, critical or otherwise, without a connection to non-SUT networks	Verify through user documentation that the SUT provides the capability to provide network services to SUT networks without a connection to non-SUT networks and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR5.1 (2)	3, 4	
FSA-S-RDF-1.3	Logical and physical isolation of critical networks	The SUT shall provide the capability to logically and physically isolate critical SUT networks from non-critical SUT networks	Verify through user documentation that the SUT provides the capability to logically and physically segment critical SUT networks from other critical SUT networks and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR5.1 (3)	4	
FSA-S-RDF-2	Zone Boundary protection	The SUT 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.	Verify that the SUT manages its external interfaces at any zone boundary through an appropriate boundary device and record results as: a. Supported b. Not Supported	No	ISA-62443-3-3: SR5.2	1, 2, 3, 4	Any connections to external networks or other SUTs 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 on a DMZ). SUT boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site. As part of a defense-in-depth protection strategy, higher impact SUTs should be partitioned into separate zones utilizing conduits to restrict or prohibit network access in accordance with security policies and procedures and an assessment of risk. SL T(system) categorization guides the selection of appropriate candidates for zone partitioning (see ISA 99.03.02 [8]).
FSA-S-RDF-2.1	Deny by default, allow by exception	The SUT shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).	Verify SUT boundary device settings are able to be configured based on permit by exception and record results as: a. Supported , or b. Not Supported	No	ISA-62443-3-3: SR5.2 (1)	2, 3, 4	
FSA-S-RDF-2.2	Island Mode	The SUT shall provide the capability to prevent any communication through the SUT boundary (also termed island mode).	Verify through user documentation that SUT boundary device has the capability to prevent any communication through the SUT boundary and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR5.2 (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 SUT, or an attack is occurring at the enterprise level, This island mode needs to support essential functions (see also clause 4.2, Support of essential functions).
FSA-S-RDF-2.3	Fail Close	The SUT shall provide the capability to prevent any communication through the SUT boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This ‘fail close’ functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions	Verify through user documentation that SUT boundary device can be configured to prevent all access upon failure and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR5.2 (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. This fail close needs to support essential functions (see also clause 4.2, Support of essential functions).

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-RDF-3	General purpose person-to-person communication restrictions	The SUT shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the SUT.	Review user documentation and verify that there is a method to prevent general purpose person-to-person messages from being received from users or systems external to the SUT. If necessary to confirm that this requirement has been met, follow the described method and then attempt to receive a person-to-person message. Record results as: a. Supported, or b. Not supported.	No	ISA-62443-3-3: SR5.3	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 which are not related to SUT operations, and therefore the risks imposed by these systems normally outweigh any perceived benefit. These types of general purpose communications systems are commonly used attack vectors to introduce malware to the SUT, pass information for which read authorization exists to locations external to the SUT, and introduce excessive network loading that can be used to create security problems or launch attacks on the SUT. Application of a broad range of other system requirements covering, for example, usage restrictions and limiting data flow as described elsewhere in this document to general purpose person-to-person communication systems can provide adequate compensating countermeasures to meet this requirement. The SUT may provide the capability to utilize these types of two-way communication systems, but only between servers and/or workstations within the SUT. Note that this SR needs to support the requirements associated with 8.3, SR 4.1 – Information confidentiality. The SUT may also restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages. These internal-to-external communications may be limited to the purpose of sending system alerts or other computer generated information messages to users or systems external to the SUT. To prevent the passing of information for which explicit read authorization is supported, pre-configured messages (perhaps with the ability to include some limited text) should be used to transmit the alerts or status information. Users may not be given the ability to attach files or other information to these outbound-only messages at the time the messages are created by the system.
FSA-S-RDF-3.1	Prohibit all general purpose person-to-person communications	The SUT shall provide the capability to prevent both transmission and receipt of general purpose person-to-person messages.	Review user documentation and verify that there is a method to prevent general purpose person-to-person messages from being sent to users or systems external to the SUT. If necessary to confirm that this requirement has been met, follow the described method and then attempt to send a person-to-person message. Record results as: a. Supported, or b. Not supported.	No	ISA-62443-3-3: SR5.3 (1)	3, 4	
FSA-S-RDF-4	Application Partitioning	The SUT shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model	Verify SUT user documents include evidence that Application Partitioning capability is included to support zoning models and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR5.4	1, 2, 3, 4	Partitioning may be accomplished via physical or logical means through the use of different computers, different central processing units, different instances of the operating system, different network addresses and combinations of these methods or other methods as appropriate. Examples of applications and services that could be considered for different partitions include, but are not limited to, emergency and/or safety systems, closed-loop control applications, operator workstations and engineering workstations.

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-TRE-1	Audit log accessibility	The SUT shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	Verify SUT provides a means to access audit logs and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR6.1	1, 2, 3, 4	The SUT generates audit records about events occurring in the system (see 6.10, SR 2.8 – Auditable events). 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. This access should not alter the original audit records. 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 SIEM. See relevant SRs in clauses 5, 6 and 9 regarding the creation of, protection of and access to audit logs.
FSA-S-TRE-1.1	Programmatic access to audit logs	The SUT shall provide programmatic access to audit records using an application programming interface (API)	Verify via SUT documents the system supports API access to audit logs and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR6.1 (1)	3, 4	NOTE This capability is necessary to ensure complete and timely response to security incidents
FSA-S-TRE-2	Continuous monitoring	The SUT shall provide the capability to continuously monitor all security mechanism performance to detect, characterize, mitigate, and report security breaches in a timely manner.	Verify SUT provides the capability to continuously monitor security mechanisms to detect attacks and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR6.2	2, 3, 4	SUT monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, IPS, malicious code protection 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 SUT (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 SUT 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 which establish a larger context in which the raw events occurred. Additionally, these mechanisms can be used to track the effect of security changes to the SUT (see 6.10, SR 2.8 – Auditable events). Having forensic tools pre-installed can facilitate incident analysis.

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-RA-1	Denial of Service Protection	The SUT shall provide the capability to operate in a degraded mode during a DoS event.	No validation activity needed as covered by validation of the child requirements	NA	ISA-62443-3-3: SR7.1	1, 2, 3, 4	A variety of technologies exist to limit, or in some cases, eliminate the effects of DoS situations. For example, boundary protection devices can filter certain types of packets to protect devices on an internal, trusted network from being directly affected by DoS events or restricting the information flow to be unidirectional outbound. Specifically, as noted in clause 4, a DoS event on the control system should not adversely impact any safety-related systems.
FSA-S-RA-1.1	Manage Communication Loads	The SUT shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events	Perform CRT testing based on storms directed at devices and verify upstream services return to normal by end of test, and downstream services are not adversely effected during the test. See EDSA 310 for details of this testing. Record the results as: a. Supported, or b. Not Supported Note: Devices that have ISASecure certification are exempt from testing	Yes	ISA-62443-3-3: SR7.1 (1)	2, 3, 4	
FSA-S-RA-1.2	Limit DoS effects to other systems or networks	The SUT shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks	Verify through user or design documentation that the SUT provides the capability to restrict the ability of users to cause DoS events and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.1 (2)	3,4	
FSA-S-RA-2	Resource Management	The SUT shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion	Verify through user or design documentation that the SUT provides the capability of limiting the user of resources for security functions such as virus scanning and patch management and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.2	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 SUT 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.
FSA-S-RA-3	Control System Backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the SUT without affecting normal plant operations.	Verify the SUT provides the ability to conduct backups of user-level and system-level information (including system state information) without affecting normal plant operations and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.3	1, 2, 3, 4	The availability of up-to-date backups is essential for recovery from an SUT failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead. Although not usually required for SUT recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup (see 9.4, SR 6.2 – SUT monitoring tools and techniques). If the resulting backups contain confidential information, encryption should be considered (see 7.5, SR 4.3 – Use of cryptography).
FSA-S-RA-3.1	Backup verification	The SUT shall provide the capability to verify the reliability of backup mechanisms	Verify the SUT provides the capability to verify the reliability of backup mechanisms and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.3 (1)	2, 3, 4	
FSA-S-RA-3.2	Backup automation	The SUT shall provide the capability to automate the backup function based on a configurable frequency.	Review system documentation and verify that the system has the ability to automate the backup function based on a configurable frequency. Record results as: a. Supported, or b. Not Supported.	No	ISA-62443-3-3: SR7.3 (2)	3,4	
FSA-S-RA-4	SUT recovery and reconstitution	The SUT shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure	Verify user data restore functionality and record results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.4	1, 2, 3, 4	SUT 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, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

Requirement ID	Reference Name	Requirement Description	Validation Activity	Validation by Independent Test Required (Yes/No)	Source of Requirement	Security Level	Rationale, Supplemental Guidance, and Notes
FSA-S-RA-5	Emergency power	The SUT shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.	Verify the SUT's ability to switch to and from an emergency power supply without affecting the existing security state and record the results as: a. Supported, or b. Not Supported	Yes	ISA-62443-3-3: SR7.5	1, 2, 3, 4	There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.
FSA-S-RA-6	Network and security configuration settings	The SUT shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the SUT supplier. The SUT shall provide an interface to the currently deployed network and security configuration settings.	Review vendor documentation and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.6	1, 2, 3, 4	These configuration settings are the adjustable parameters of the SUT components. In order to be able to detect and correct any deviations from the approved and/or recommended configuration settings, the SUT needs to support monitoring and control of changes to the configuration settings in accordance with security policies and procedures.
FSA-S-RA-6.1	Machine-readable reporting of current security settings	The SUT 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 and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.6 (1)	3,4	
FSA-S-RA-7	Least functionality	The SUT shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services	Verify the SUT documentation provides guidance for how to prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or other services and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.7	1, 2, 3, 4	SUT are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support essential operations (for example, key missions and functions). 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 an SUT, but doing so increases risk over limiting the services provided by any one component. Many functions and services commonly provided by commercial-off-the-shelf (COTS) equipment may be candidates for elimination, for example, email, voice over internet protocol (VoIP), instant messaging (IM), file transfer protocol (FTP), hypertext transfer protocol (HTTP) and file sharing.
FSA-S-RA-8	SUT component inventory	The SUT shall provide the capability to report the current list of installed components and their associated properties	Verify the SUT provides the capability to report the current list of installed components and their associated properties and record the results as: a. Supported, or b. Not Supported	No	ISA-62443-3-3: SR7.8	2, 3, 4	A control system component inventory may include but is not limited to component ID, capability and revision level. The component inventory should be consistent with the SuC. A formal process of configuration management should be deployed to keep control of the changes in the component inventory baseline (see ISA 62443 2 1 (99.02.01)).