EDSA-311
ISA Security Compliance Institute - Embedded Device Security Assurance -
Functional Security Asssessment (FSA)

Revision History

Version	Date	Changes
V1R3-03082010	2010.03.08	initial version published to http://www.ISASecure.org
1.4	2010.06.08	formatting, removed inapplicable comment text

Organization of FSA Specification

Reference ID and Name	*ISASecure*™ Level			
Access Control				
└── FSA-AC-1 Access Control Authorization	NA			
└── FSA-AC-1.1 Role Based Access	>1			
└── FSA-AC-1.2 Dual Approval Access	>1			
└── FSA-AC-1.3 Least Privilege Default Access	>1			
└── FSA-AC-1.4 Administrator User Role	>1			
└── FSA-AC-1.5 Administrator Support Functions	>2			
└── FSA-AC-2 User Authentication	NA			
└── FSA-AC-2.1 Authentication by User ID and Password	NA			
└── FSA-AC-2.1.1 User Management of Password	All			
└── FSA-AC-2.1.2 Monitor Unsuccessful Login Attempts	All			
└── FSA-AC-2.1.3 Record Successful Logins	All			
└── FSA-AC-2.1.4 Display Previous Login History	>2			
└── FSA-AC-2.1.5 Password Modification Reminder	>2			
└── FSA-AC-2.1.6 Password Strength Enforcement	>2			
└── FSA-AC-2.1.7 Action for High Number of Unsuccessful Login	All			
└── FSA-AC-2.1.8 Minimum Password Capability	All			
└── FSA-AC-2.1.9 Clear Text Passwords	All			
└── FSA-AC-2.1.10 Cryptographic Password Protection	>2			
└── FSA-AC-2.1.11 Access Control for All Exposed Services	All			
└── FSA-AC-2.2 Other Authentication Methods	Not required			
└── FSA-AC-2.3 Two Factor Authentication (local network)	>2			
└── FSA-AC-2.3 Two Factor Authentication (remote)	All			
└── FSA-AC-2.5 Authentication Feedback	All			
└── FSA-AC-3 System Use Notification	All			
└── FSA-AC-4 Local Session Locking Timeout	>1			
└── FSA-AC-5 Remote Session Termination Timeout	>1			
Use Control				
└── FSA-UC-1 Wireless Access	NA	*this appears to belong with Access Control but 99.01.03 has under Use Control*		
└── FSA-UC-1.1 Physical Disable Wireless Access	All			
└── FSA-UC-2 Device Authentication	NA			
└── FSA-UC-2.1 Failures in Cryptology Services	All			
└── FSA-UC-2.2 Basic Device Authentication	>1			
└── FSA-UC-2.3 Cryptographic Device Authentication	>2			
└── FSA-UC-3 Creation of Audit Trail	NA			
└── FSA-UC-3.1 Configuration of Audit Events	>2			
└── FSA-UC-3.2 Content of Audit Record	NA			
└── FSA-UC-3.2.1 Time Stamp for Audit	>1			
└── FSA-UC-3.2.2 Information for Non-repudiation	>2			
└── FSA-UC-3.2.3 Additional Content for Audit Record	>2			
└── FSA-UC-3.3 Protection of Audit Information	NA			
└── FSA-UC-3.3.1 Audit Fault Warning	>2			
└── FSA-UC-3.3.2 Basic Protection of Audit Information	>1			
└── FSA-UC-3.3.3 Crypto Protection of Audit Information	>2			
└── FSA-UC-3.4 System Wide Audit	>2			
└── FSA-UC-3.5 Audit Report Generation	>1			

Organization of FSA Specification

Reference ID and Name	*ISASecure*™ Level			
Data Integrity				
└── FSA-DI-1 Integrity of Data in Transit	NA			
└── FSA-DI-1.1 Insertion of Data Packets	>1			
└── FSA-DI-1.2 Deletion of Data Packets	>1			
└── FSA-DI-1.3 Excessive Delay of Data Packets	>1			
└── FSA-DI-1.4 Re-sequencing or Replay of Data Packets	>1			
└── FSA-DI-1.5 Basic Modification of Transmitted Data	>1			
└── FSA-DI-1.6 Crypto Modification of Transmitted Data	>2			
└── FSA-DI-1.7 Point to point Communications	NA			
└── FSA-DI-1.7.1 Session Creation	>1			
└── FSA-DI-1.7.2 Basic Session Protection	>1			
└── FSA-DI-1.7.3 Crypto Session Protection	>2			
└── FSA-DI-1.7.4 Session Closure	>2			
└── FSA-DI-1.7.5 Session Timeout	>2			
└── FSA-DI-1.8 Multicast / Broadcast Communications	NA			
└── FSA-DI-1.8.1 Multicast Restrictions	>2			
└── FSA-DI-1.8.2 Multicast Reception Protection	>2			
└── FSA-DI-1.8.3 Multicast Transmission Restrictions	>2			
└── FSA-DI-1.9 Verify Input Data Syntax	>1			
└── FSA-DI-1.10 Handling Error Conditions	>1			
└── FSA-DI-2 Integrity of Data at Rest Measures	>1			
└── FSA-DI-2.1 Protection of Static Data	NA			
└── FSA-DI-2.1.1 Disable Unused Ports	All			
└── FSA-DI-2.1.2 Write Protection	>2			
└── FSA-DI-2.2 Detection of Unauthorized Changes	NA			
└── FSA-DI-2.2.1 Executable Code Basic Mod Protection	>1			
└── FSA-DI-2.2.2 Executable Code Crypto Mod Protection	>2			
└── FSA-DI-2.2.3 App Configuration Basic Protection	>1			
└── FSA-DI-2.2.4 App Configuration Crypto Protection	>2			
└── FSA-DI-2.2.5 Verify Application Specific Syntax	>1			
└── FSA-DI-2.2.6 OS Basic Configuration Protection	>1			
└── FSA-DI-2.2.7 OS Crypto Configuration Protection	>2			
└── FSA-DI-2.2.8 Basic Executable Code Insert Protection	>1			
└── FSA-DI-2.2.9 Crypto Executable Code Insert Protection	>2			
└── FSA-DI-2.2.10 Non Execution of Data	>2			
└── FSA-DI-3 Auto Verify Security Functions	>2			
Data Confidentiality				
└── FSA-DC-1 Confidentiality of Data in Transit	NA			
└── FSA-DC-1.1 No Clear Text in Data Transit	All			
└── FSA-DC-1.1 Cryptographic Protection for Data Confidentiality	>1			
└── FSA-DC-1.2 Cryptographic Key Management	>2			
└── FSA-DC-2 Confidentiality of Data at Rest	NA			
└── FSA-DC-2.1 Basic Confidentiality of Data at Rest	>1			
└── FSA-DC-2.2 Crypto Confidentiality of Data at Rest	>2			
└── FSA-DC-3 Cryptographic Mechanisms	>1			

Organization of FSA Specification

Reference ID and Name	*ISASecure*™ Level			
Restrict Data Flow				
└── FSA-RDF-1 Information Flow Enforcement	All			
└── FSA-RDF-2 Application Partitioning	>1			
└── FSA-RDF-3 Security Function Isolation	>2			
└── FSA-RDF-4 Shared System Resources	>2			
Timely Response to Event				
└── FSA-TRE-1 Incident Response Support	>2			
Network Resource Availability				
└── FSA-NRA-1 Denial of Service Protection	All			
└── FSA-NRA-1.1 Data Flooding Protection	>2			
└── FSA-NRA-1.2 Protocol Fuzzing Protection	All			
└── FSA-NRA-1.3 Deterministic Loss of Comm	All			
└── FSA-NRA-1.4 Notification of Attack	>1			
└── FSA-NRA-1.5 Preservation of Essential Services	All			
└── FSA-NRA-2 IACS Backup	All			
└── FSA-NRA-3 IACS Recovery	All			

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-AC-1	Access Control Authorization	The IACS embedded device shall provide capability for user configured Access Control Functionality to facilitate automated enforcement of a site specific Access Control Policy based upon authenticated entities	FR 1.3 ACCESS ENFORCEMENT NIST 800-53 AC-3 FR 2.5 USER IDENTIFICATION AND AUTHENTICATION NIST 800-53 IA-2	NA	Access control should be a user configurable function based upon the identity of the person/system requesting access. The system should only allow properly authenticated entities have access unless other independent system components only allow properly authorized entities to make requests to this subsystem.
FSA-AC-1.1	Role Based Access	The IACS embedded device Access Control Functionally shall provide the capability to support role based access control policies.	FR 1.2 ACCOUNT MANAGEMENT NIST 800-53 AC-2 FR 1.3 ACCESS ENFORCEMENT (1) NIST 800-53 AC-3 (1) FR 1.4 SEPARATION OF DUTIES NIST 800-53 AC-5	>1	Role based access control allows an administrator to define generic user roles with specified levels of user access privileges and users may subsequently be assigned roles so upon successful authentication of the user they are authorized as having the privileges associated with the assigned role
FSA-AC-1.2	Dual Approval Access	The IACS embedded device Access Control Functionally shall provide the capability to support dual-approval mechanisms as an access control option for user modification or control of critical parameters or actions.	FR 1.3 ACCESS ENFORCEMENT (2) NIST 800-53 AC-3 (2)	>1	A security procedure requiring two people (or possibly processes or devices) to cooperate in gaining authorized access to a system resource (data, files, devices).
FSA-AC-1.3	Least Privilege Default Access	New Access Accounts for the Access Control shall be created by default based on least privileges requiring explicit action by the account administrator to raise privilege level.	FR 1.5 LEAST PRIVILEGE NIST 800-53 AC-6	>1	Support implementation of least privilege philosophy
FSA-AC-1.4	Administrator User Role	The IACS embedded device Access Control Functionally shall provide support for an administrator user role which has the ability to create user accounts and manage the privileges of other users	FR 1.2 ACCOUNT MANAGEMENT NIST 800-53 AC-2 FR 1.3 ACCESS ENFORCEMENT (1) NIST 800-53 AC-3 (1) FR 1.4 SEPARATION OF DUTIES NIST 800-53 AC-5	>1	Only Administrator Role authorization allows set up and management of accounts for other users
FSA-AC-1.5	Administrator Support Functions	The IACS embedded device shall provide the administrator the ability list of all current user accounts and login history such as time of last login	FR 1.2 ACCOUNT MANAGEMENT NIST 800-53 AC-2 FR 1.3 ACCESS ENFORCEMENT (1) NIST 800-53 AC-3 (1) FR 1.4 SEPARATION OF DUTIES NIST 800-53 AC-5	>2	This provides information to manage accounts and detect stale or unused accounts
FSA-AC-2	User Authentication	The IACS embedded device shall support acceptable authentication methods for user identification to support Access Management and Use Control Functionality for all services supported by the device.	FR 1.3 ACCESS ENFORCEMENT NIST 800-53 AC-3 FR 2.5 USER IDENTIFICATION AND AUTHENTICATION NIST 800-53 IA-2 NERC Security Guidelines	NA	
FSA-AC-2.1	Authentication by User ID and Password	The IACS embedded device shall support user authentication via entry of user ID and password.	FR 1.6 UNSUCCESSFUL LOGIN ATTEMPTS NIST 800-53 AC-7 ISA-99.01.03 - FR 1.8 PREVIOUS LOGON NOTIFICATION NIST 800-53 AC-9 NERC CIP	NA	

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-AC-2.1.1	Management of Password	The IACS embedded device shall provide the capability for [IACS Administrator] or the user to modify password within their control without impacting normal operation		All	Normal security management may require frequent changes to password access due to changes on personnel etc.
FSA-AC-2.1.2	Monitor Unsuccessful Login Attempts	The IACS embedded device shall monitor and record the number and time of unsuccessful login attempts per user id since the last successful login.	FR 1.6 UNSUCCESSFUL LOGIN ATTEMPTS NIST 800-53 AC-7 FR 1.8 PREVIOUS LOGON NOTIFICATION NIST 800-53 AC-9 NERC Security Guidelines	All	Suggested test sequence: create a user, define password, log in successfully, attempt login with bad password multiple times, record device logging of failed attempts.
FSA-AC-2.1.3	Record Successful Logins	The IACS embedded device shall monitor and record the date and time of the last successful login.	FR 1.8 PREVIOUS LOGON NOTIFICATION NIST 800-53 AC-9	All	
FSA-AC-2.1.4	Display Previous Login History	Following successful user authentication the IACS embedded device shall display the date and time of the last successful login plus the number of unsuccessful login attempts for this user ID since that time.	FR 1.8 PREVIOUS LOGON NOTIFICATION NIST 800-53 AC-9	>2	
FSA-AC-2.1.5	Password Modification Reminder	Following successful user authentication the IACS embedded device shall provide the capability for automated reminder of need to modify user password after [[IACS administrator defined time] has passed since the last password modification.		>2	
FSA-AC-2.1.6	Password Strength Enforcement	The IACS embedded device shall provide the capability to only accept user requested password updates for passwords that meet [[IACS administrator configured] criteria for strong passwords based on minimum length, use of upper / lower case and non-alpha characters.		>2	Administrator configured means administrator can enable or disable particular criteria and/or enter a integer numbers for a password attribute such as minimum or maximum length
FSA-AC-2.1.7	Action for High Number of Unsuccessful Login	The IACS embedded device shall provide option to take *[IACS administrator configured*] action if the number of unsuccessful login attempts exceeds a user configured value with in a [*user configured time period*].	FR 1.6 UNSUCCESSFUL LOGIN ATTEMPTS NIST 800-53 AC-7	>2	User configure action may be: user lockout, generation of security alert event, etc.
FSA-AC-2.1.8	Minimum Password Capability	User authentication through manual login with password shall support a minimum of 6 character passwords to be used		All	Password support which limit password length to lengths shorter than 6 characters are too weak to be counted as password protection
FSA-AC-2.1.9	Clear Text Passwords	The IACS embedded device shall not internally store or send password over shared networks in clear text format.		All	Passwords should not be viewable in clear text even for physically controlled network for higher levels of *ISASecure*
FSA-AC-2.1.10	Cryptographic Password Protection	The IACS embedded device passwords shall have cryptographic protection for transmission over networks		>2	Passwords should not be transmitted without cryptographic protection for higher levels of *ISASecure*

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-AC-2.1.11	Access Control for All Exposed Services	The IACS embedded device user authentication shall cover access to all services supported by the device during normal operation		All	All services should either be secured by access control or disabled for normal operation (service that must be disabled also need to be documented for the user)
FSA-AC-2.2	Other Authentication Methods	The IACS embedded device authentication may provide optional interfaces to support alternative user authentication methods.		Not required	Alternative authentication methods may include biometric scanners, ID card scanners, RFI tokens, etc.
FSA-AC-2.3	Two Factor Authentication (local network)	The IACS embedded device Access Control Functionally shall support two factor authentication mechanisms.	FR 1.3 ACCESS ENFORCEMENT (2) NIST 800-53 AC-3 (2) FR 2.5 USER IDENTIFICATION AND AUTHENTICATION (1) (2) NIST 800-53 IA-2 (1) (2)	>2	Two factor authentication of the user may be desired in some situations, especially for remote access *Required for local access SAL>2 according to S99*
FSA-AC-2.4	Two Factor Authentication (remote)	The IACS embedded device Access Control Functionally shall support two factor authentication mechanisms for remote access.	FR 1.3 ACCESS ENFORCEMENT (2) NIST 800-53 AC-3 (2) FR 2.5 USER IDENTIFICATION AND AUTHENTICATION (1) (2) NIST 800-53 IA-2 (1) (2)	All	Two factor authentication of the user may be desired in some situations, especially for remote access
FSA-AC-2.5	Authentication Feedback	The IACS embedded device shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	FR 2.9 AUTHENTICATOR FEEDBACK NIST 800-53 IA-6	All	The feedback from the IACS does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information
FSA-AC-3	System Use Notification	The IACS embedded device authentication shall provide option for presenting an [IACS administrator] provided "system use notification message" before granting system access informing potential users they are entering a redistricted area.	FR 1.7 SYSTEM USE NOTIFICATION NIST 800-53 AC-8 NERC CIP	All	May be regulatory requirement in some markets May be documented as not appropriate or required for some embedded devices where this requirement would not apply due to lack of terminal type login
FSA-AC-4	Local Session Locking Timeout	The IACS embedded device authentication shall provide option for session locking after a [IACS administrator] specified period of time of inactivity for the session.	FR 1.10 SESSION LOCK NIST 800-53 AC-11	>1	Session locking should preserve state of the session for resumption upon re-login
FSA-AC-5	Remote Session Termination Timeout	The IACS embedded device authentication shall provide option for automated session termination for remote sessions after a user specified period of time of inactivity for the session.	FR 1.11 REMOTE SESSION TERMINATION NIST 800-53 AC-12 FR 5.6 NETWORK DISCONNECT NIST 800-53 SC-10	>1	Primarily recommended for remote access but embedded device is unlikely to have knowledge of local versus remote access

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-UC-1	Wireless Access	The IACS embedded device wireless access must be protected via sufficient authentication and encryption protection.	FR 2.1 WIRELESS ACCESS RESTRICTIONS	NA	Wireless access is not bound by physical access restrictions and physical network boundary devices so that technical protection measures applied to this access must be sufficiently strong independent of the other protection measures that do not apply
FSA-UC-1.1	Physical Disable Wireless Access	***IACS embedded products*** that provide wireless access must provide the option to be physically disabled by the end user of the product by a method unable to be overridden by SW or user soft configuration	ISCI CURRENTLY DOES NOT RECOGNIZE OR CERTIFY WIRELESS STANDARDS	All	**NOTE ISCI CURRENTLY DOES NOT RECOGNIZE OR CERTIFY WIRELESS STANDARDS** Physical disabling of wireless access points that can not be overridden via soft configuration downloads is the only truly secure mechanism for the highest level of integrity Use of wireless connections if present is not currently covered by ISASecure Certification
FSA-UC-2	Device Authentication	The IACS embedded device shall provide authentication methods for device identification prior to establishing a connection to support Access Management and Use Control Functionality.	FR 2.6 DEVICE IDENTIFICATION AND AUTHENTICATION NIST 800-53 IA-3	NA	ISA 99 - "When practical, devices need to be chosen with capability to support authentication mechanisms" Automatic equipment identification may be considered as a means to authenticate connections.
FSA-UC-2.1	Failures in Cryptography Services	IACS embedded device shall not be dependent on outside cryptography services that could result in denial of service for the embedded device if the service were no longer available	FR 2.10 CRYPTOGRAPHIC MODULE AUTHENTICATION NIST 800-53 IA-7	All	Access for critical functions from local process area primary access points should not be dependent on external verification services that may experience failures independent of user site's control. For remote access to critical functions loss of availability may be an acceptable tradeoff for significantly stronger access control *do not expect this type of service to be utilized by an embedded product* *may not even apply at all for IACS other than e-commerce*
FSA-UC-2.2	Basic Device Authentication	The IACS embedded device shall provide at least basic measures for authentication of device identification	FR 2.6 DEVICE IDENTIFICATION AND AUTHENTICATION NIST 800-53 IA-3	>1	ISA 99 - "When practical, devices need to be chosen with capability to support authentication mechanisms" Automatic equipment identification may be considered as a means to authenticate connections.
FSA-UC-2.3	Cryptographic Device Authentication	The IACS embedded device shall provide cryptographic measures for authentication of device identification	FR 2.6 DEVICE IDENTIFICATION AND AUTHENTICATION NIST 800-53 IA-3	>2	ISA 99 - "When practical, devices need to be chosen with capability to support authentication mechanisms" Automatic equipment identification may be considered as a means to authenticate connections.

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-UC-3	Creation of Audit Trail	The IACS embedded device shall provide option for generation and storage of audit information for post security incident and process improvement activities.	FR 2.12 AUDITABLE EVENTS NIST 800-53 AU-2	NA	Auditing activity can affect IACS performance. Therefore, the organization decides, based upon a risk assessment, which events are adequate to support after-the-fact investigations of security incidents. Checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events.
FSA-UC-3.1	Configuration of Audit Events	The IACS embedded device shall provide for [IACS administrator] configuration of what events are included in list of auditable events.	FR 2.12 AUDITABLE EVENTS (1) NIST 800-53 AU-2 (1)	>2	
FSA-UC-3.2	Content of Audit Record	The IACS embedded device shall provide for [IACS administrator] configuration of required information for each auditable event.	FR 2.13 CONTENT OF AUDIT RECORDS NIST 800-53 AU-3 FR 2.18 TIME STAMPS NIST 800-53 AU-8	NA	User should be able to determine what events occurred, when the events occurred, the sources of the events, and the outcomes of the events Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the IACS (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.
FSA-UC-3.2.1	Time Stamp for Audit	The IACS embedded device shall provide time stamps for use in audit record generation based on "system time".	FR 2.18 TIME STAMPS NIST 800-53 AU-8	>1	System Time - refers to a synchronized time reference across the control system so the time of events from various sources can be accurately compared within a stated accuracy.
FSA-UC-3.2.2	Information for Non-repudiation	The IACS embedded device or the responsible higher level component shall provide the capability to include in the audit trail which device or individual initiated or performed a particular action.	FR 2.20 NON-REPUDIATION NIST 800-53 AU-10	*>2*	Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. *In FR2.20 applied only to SAL 4 but knowing who initiated an action seems to be a basic requirement*

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-UC-3.2.3	Additional Content for Audit Record	The IACS embedded device shall provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	FR 2.13 CONTENT OF AUDIT RECORDS (1) NIST 800-53 AU-3 (1)	>2	
FSA-UC-3.3	Protection of Audit Information	The IACS embedded device shall protect audit information and audit tools from unauthorized access, modification, and deletion.	FR 2.19 PROTECTION OF AUDIT INFORMATION NIST 800-53 AU-9	NA	It is important to protect the audit information as it is important for error correction, security breach recovery, investigations, and related efforts.
FSA-UC-3.3.1	Audit Fault Warning	The IACS embedded device or a higher level component shall alert appropriate organizational officials in the event of an audit processing failure and support additional configurable actions (e.g., overwrite oldest audit records, stop generating audit records).	FR 2.15 RESPONSE TO AUDIT PROCESSING FAILURES NIST 800-53 AU-5	>2	Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.
FSA-UC-3.3.2	Basic Protection of Audit Information	The IACS embedded device shall provide basic non-cryptographic measures for protection of audit information	FR 2.19 PROTECTION OF AUDIT INFORMATION NIST 800-53 AU-9	>1	The audit information is important for error correction, security breach recovery, investigations, and related efforts. Non-repudiation of this service may be obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).
FSA-UC-3.3.3	Cryptographic Protection of Audit Information	The IACS embedded device shall provide cryptographic measures for protection of audit information	FR 2.19 PROTECTION OF AUDIT INFORMATION NIST 800-53 AU-9	>2	The audit information is important for error correction, security breach recovery, investigations, and related efforts. Non-repudiation of this service may be obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).
FSA-UC-3.4	System Wide Audit	The IACS embedded device shall provide capability to pass [IACS administrator configurable] auditable events to another device for creation of a higher level consolidated audit log.	FR 2.12 AUDITABLE EVENTS NIST 800-53 AU-2	>2	It is likely that most embedded devices will have limited capacity for storage of audit information. Audit information is best viewed within a system context with tools capable of filtering data based upon multiple criteria.

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-UC-3.5	Audit Report Generation	The IACS embedded device or the responsible higher level component shall provide an audit reduction and report generation capability for audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.	FR 2.17 AUDIT REDUCTION AND REPORT GENERATION NIST 800-53 AU-7	>1	In general, audit reduction and report generation will typically be performed on a separate information system.

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DI-1	Integrity of Data in Transit	The IACS embedded device shall protect the integrity of transmitted information	FR 3.2 COMMUNICATION INTEGRITY NIST 800-53 SC-8	NA	
FSA-DI-1.1	Insertion of Data Packets	The IACS embedded device shall protect the integrity of transmitted information against insertion of data packets not intended to be part of the transmitted data	Basic Communications standards outside scope of FSA review	>1	Application level sequence numbers is a commonly used method
FSA-DI-1.2	Deletion of Data Packets	The IACS embedded device shall protect the integrity of transmitted information against deletion of data packets	Basic Communications standards outside scope of FSA review	>1	Application level sequence numbers is a commonly used method
FSA-DI-1.3	Excessive Delay of Data Packets	The IACS embedded device shall protect the integrity of transmitted information against delay of data packets by more than tolerable by the intended application	Basic Communications standards outside scope of FSA review	>1	Protocol acknowledgement or time window expectations or application level timeouts are typical measures
FSA-DI-1.4	Re-sequencing or Replay of Data Packets	The IACS embedded device shall protect the integrity of transmitted information against re-sequencing or replay of data packets	Basic Communications standards outside scope of FSA review	>1	Sequence numbers, time stamps are common methods

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DI-1.5	Basic Modification of Transmitted Data	The IACS embedded device shall employ basic mechanisms to recognize changes to information during communication independent of the basic communication protocol stack	FR 3.2 COMMUNICATION INTEGRITY (1) NIST 800-53 SC-8 (1)	>1	Standard communication protocol protection against corruption during transmission are only intended for random corruption and are easily defeated by individuals with malicious intent If not present end user must provide protection by restricted access by both physical and cyber boundary blocking measures to keep transmission within a physically protected area. Note: certified safety systems will already have equivalent of application level CRC
FSA-DI-1.6	Modification of Transmitted Data	The IACS embedded device shall employ cryptographic mechanisms to recognize changes to information during communication	FR 3.2 COMMUNICATION INTEGRITY (1) NIST 800-53 SC-8 (1)	>2	Standard communication protocol protection against corruption during transmission are only intended for random corruption and are easily defeated by individuals with malicious intent
FSA-DI-1.7	Point to point Communications	All point to point communication connections to the IACS embedded device shall provide sufficient security measures to insure communications only take place with properly authorized parties	ISA-99.01.03 - FR 1.3 ACCESS ENFORCEMENT NIST 800-53 AC-3 FR 3.14 SESSION AUTHENTICITY NIST 800-53 SI-14	NA	
FSA-DI-1.7.1	Session Creation	All point to point communication connections to the IACS embedded device shall provide measures to properly identify and authenticate the other party prior to approving the connection	ISA-99.01.03 - FR 1.3 ACCESS ENFORCEMENT NIST 800-53 AC-3	>1	Access Control for all connections
FSA-DI-1.7.2	Basic Session Protection	All point to point communication connections to the IACS embedded device shall provide measures to protect the integrity of authorized sessions and prevent others from participating in or stealing the authorized session	FR 3.14 SESSION AUTHENTICITY NIST 800-53 SI-14	>1	This requirement focuses on communications protection at the session, versus packet, level. The intent of this requirement is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). Encryption can prevent observation of protocol to steal credentials needed to participate in or steal session

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DI-1.7.3	Crypto Session Protection	All point to point communication connections to the IACS embedded device shall provide cryptographic measures to protect the integrity of authorized sessions and prevent others from participating in or stealing the authorized session	FR 3.14 SESSION AUTHENTICITY NIST 800-53 SI-14	>2	This requirement focuses on communications protection at the session, versus packet, level. The intent of this requirement is to implement session-level protection where needed Encryption can prevent observation of protocol to steal credentials needed to participate in or steal session
FSA-DI-1.7.4	Session Closure	All point to point communication connections to the IACS embedded device shall have a method to close the session when the purpose of the session has be completed or session is no longer required	FR 5.6 NETWORK DISCONNECT NIST 800-53 SC-10	>2	Closing of unneeded sessions is good practice to reduce the attack surface of the device S99 has required for SAL >1
FSA-DI-1.7.5	Session Timeout	All point to point communication connections to the IACS embedded device shall have a method to close the session when it has been open or inactive for longer than a [IACS administrator] configured time	FR 5.6 NETWORK DISCONNECT NIST 800-53 SC-10	>2	Importance of session timeout depends on other protection measures such as limited physical access but is typically required for remote access where use of independent measures is not ensured
FSA-DI-1.8	Multicast / Broadcast Communications	All multicast / broadcast communication connections to the IACS embedded device shall provide product measures for [IACS administrator] to manage security of broadcast communications or sufficient information disclosure and security measures to allow proper management of its capabilities		NA	
FSA-DI-1.8.1	Multicast Restrictions	The IACS embedded device shall only use critical information from multicast transmissions for which it can properly validate the source and integrity of the transmission		>2	The word "multicast" is typically used to refer to IP multicast which is often employed for streaming media and Internet television applications. Multicast addressing is a network technology for the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the multiple destinations split. Encryption with private key insures transmission is originating from a source that knows the encryption algorithm and the key.

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DI-1.8.2	Multicast Reception Protection	The IACS embedded device using critical data from a multicast source shall verify multicast transmissions continue to originate from a properly validated source and verify integrity of the transmission	FR 3.14 SESSION AUTHENTICITY NIST 800-53 SI-14	>2	Encryption with private key insures transmission is originating from a source that knows the encryption algorithm and the key
FSA-DI-1.8.3	Multicast Transmission Restrictions	The IACS embedded device multicast transmissions shall include measures to only allow properly authorized devices to subscribe to its multicast transmission or alternatively clearly document means for users to restrict the propagation of the multicast signal within a controlled region of the network		>2	Encryption to prevent connection by parties that do not have the required encryption algorithm and key
FSA-DI-1.9	Verify Input Data Syntax	The IACS embedded device shall check information for reasonability of values, completeness, validity, and authenticity	FR 3.11 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY NIST 800-53 SI-10	>1	Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.
FSA-DI-1.10	Handling Error Conditions	The IACS embedded device shall identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries	FR 3.12 ERROR HANDLING NIST 800-53 SI-11	>1	
FSA-DI-2	Integrity of Data at Rest Measures	The IACS embedded device shall protect the integrity of data stored within the device by measures independent of access control		NA	Within a protected area physical controls may be sufficient
FSA-DI-2.1	Protection of Static Data	The IACS embedded device shall protect against unauthorized changes to software and information	FR 3.8 SOFTWARE AND INFORMATION INTEGRITY (1) (2) NIST 800-53 SI-7 (1) (2)	NA	
FSA-DI-2.1.1	Disable Unused Ports	The IACS embedded device shall provide the user the capability to disable communication services and ports that are not required for normal online use for their particular application or not covered by Access Control measures	FR 7.26 LEAST FUNCTIONALITY NIST 800-53 CM-7	All	This should include disabling of any dedicated port only used for firmware updates not sufficiently covered by access control measures.
FSA-DI-2.1.2	Write Protection	The IACS embedded device shall have independent hardware and/or software measures to prevent writing to static data		>2	This could be in the form of preventing writes to FLASH by blocking program voltage or write only access enforced by MMU
FSA-DI-2.2	Detection of Unauthorized Changes	The IACS embedded device shall employ mechanisms to automatically recognize changes to static data stored in memory able to be modified but not automatically modified during normal operation	FR 3.8 SOFTWARE AND INFORMATION INTEGRITY (1) (2) NIST 800-53 SI-7 (1) (2)	NA	

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DI-2.2.1	Executable Code Basic Mod Protection	The IACS embedded device shall implement basic means to detect modifications to executable code if susceptible to this type of threat within vendor published time interval	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>1	This provides basic online protection for known vulnerabilities
FSA-DI-2.2.2	Executable Code Crypto Mod Protection	The IACS embedded device shall implement cryptographic means to detect modifications to executable code if susceptible to this type of threat within vendor published time interval	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>2	This provides strong online protection for known vulnerabilities
FSA-DI-2.2.3	App Configuration Basic Protection	The IACS embedded device shall implement basic means to detect unauthorized modification, deletion or insertion of user application configuration data within vendor published time interval		>1	
FSA-DI-2.2.4	App Configuration Crypto Protection	The IACS embedded device shall implement cryptographic means to detect unauthorized modification, deletion or insertion of user application configuration data within vendor published time interval		>2	
FSA-DI-2.2.5	Verify Application Specific Syntax	The IACS embedded device shall check application input and program configuration information for reasonability of values, completeness, validity, and correctness of syntax or include crypto protection of application against code modification (FSA-DI-2.2.4)	FR 3.11 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY NIST 800-53 SI-10	>1	Required for SAL>1 Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.
FSA-DI-2.2.6	OS Basic Configuration Protection	The IACS embedded device shall implement basic means to detect modification, deletion or insertion of data that is capable of modifying the behavior or operation of the product's operating system such as exception vectors or scheduling, if an OS is used by the product.	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>1	
FSA-DI-2.2.7	OS Crypto Configuration Protection	The IACS embedded device shall implement cryptographic means to detect modification, deletion or insertion of data that is capable of modifying the behavior or operation of the product's operating system such as exception vectors or scheduling, if an OS is used by the product.	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>2	
FSA-DI-2.2.8	Basic Executable Code Insert Protection	The IACS embedded device shall implement means to prevent or detect insertion of malicious code within vendor published time interval	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>1	

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DI-2.2.9	Crypto Executable Code Insert Protection	The IACS embedded device shall implement means to prevent or cryptographic means to detect insertion of malicious code within vendor published time interval	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>2	
FSA-DI-2.2.10	Non Execution of Data	The IACS embedded device shall have separate memory spaces for data versus executable code and have measures to prevent execution of code located in data space	FR 3.4 MALICIOUS CODE PROTECTION NIST 800-53 SI-3	>2	Typically uses OS support of hardware MMU or dedicated separate memory in hardware design with support from CPU (such as supported by 68000 based chip sets)
FSA-DI-3	Auto Verify Security Functions	The IACS embedded device shall periodically verify the correct operation of security protection functions and notify system administrator when anomalies are discovered.	FR 3.7 SECURITY FUNCTIONALITY VERIFICATION NIST 800-53 SI-6	>2	For those security functions not able to execute automated self-tests, organization implements compensating security requirements or explicitly accepts risk of not performing as required.

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DC-1	Confidentiality of Data in Transit	The IACS embedded device shall protect the confidentiality of transmitted information	FR 4.10 COMMUNICATION CONFIDENTIALITY NIST 800-53 SC-9	NA	Within a protected area physical controls may be sufficient
FSA-DC-1.1	No Clear Text in Data Transit	The IACS embedded device shall not send any data in clear text format for basic prevention of unauthorized disclosure of information during communication	FR 4.10 COMMUNICATION CONFIDENTIALITY (1) NIST 800-53 SC-9 (1)	All	If required by application and not directly supported can only be allocated if confidentiality is only needed outside the zone of the embedded controller and the communications can be limited to the zone or encrypted by a boundary device prior to leaving the zone.
FSA-DC-1.2	Cryptographic Protection for Data Confidentiality	The IACS embedded device shall employ cryptographic mechanisms to prevent unauthorized disclosure of information during communication	FR 4.10 COMMUNICATION CONFIDENTIALITY (1) NIST 800-53 SC-9 (1)	>1	If required by application and not directly supported can only be allocated if confidentiality is only needed outside the zone of the embedded controller and the communications can be limited to the zone or encrypted by a boundary device prior to leaving the zone.
FSA-DC-1.3	Cryptographic Key Management	The IACS embedded device shall provide automated support for automation of cryptographic key management	FR 4.11 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT NIST 800-53 SC-12	>2	Key generation needs to be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards
FSA-DC-2	Confidentiality of Data at Rest	The IACS embedded device shall provide measures to protect confidentiality of stored information		N/A	Can provide additional layer of security for high value data. May not apply frequently to embedded products but can protect critical information stored within an otherwise non-secured environment

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-DC-2.1	Basic Confidentiality of Data at Rest	The IACS embedded device shall use storage in non clear text formats to provide measures for sensitive data storage to protect confidentiality of stored information		>1	Can provide additional layer of security for high value data. May not apply frequently to embedded products but can protect critical information stored within an otherwise non-secured environment
FSA-DC-2.2	Crypto Confidentiality of Data at Rest	The IACS embedded device shall provide cryptographic measures for sensitive data storage to protect confidentiality of stored information		>2	Can provide additional layer of security for high value data. May not apply frequently to embedded products but can protect critical information stored within an otherwise non-secured environment
FSA-DC-3	Cryptographic Mechanisms	The IACS embedded device shall document the cryptographic mechanisms used and any independent validation of the measures so that users can verify if the mechanisms used comply with applicable laws, directives, policies, regulations, standards, and guidance for their target market	FR 4.12 USE OF CRYPTOGRAPHY NIST 800-53 SC-13 FR 2.10 CRYPTOGRAPHIC MODULE AUTHENTICATION NIST 800-53 IA-7	>1	The most effective safeguard is to use a cryptographic module validated by the Cryptographic Module Validation Program. Additional information on the use of validated cryptography can be found at http://csrc.nist.gov/cryptval.

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-RDF-1	Information Flow Enforcement	The IACS embedded device shall provide means to enforce assigned authorizations for controlling the flow of information outside the embedded controller zone and between interconnected systems in accordance with user specific policy	FR 5.1 INFORMATION FLOW ENFORCEMENT NIST 800-53 AC-4 FR 5.5 BOUNDARY PROTECTION NIST 800-53 SC-7	All	Information flow control regulates where information is allowed to travel within an IACS and between IACS (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Documentation of the communications protocols and guidance on how to block selective data flows via a properly configured independent boundary protection device (i.e.: firewall) can be considered sufficient if unprotected path is protected via physical protection
FSA-RDF-2	Application Partitioning	The IACS embedded device shall separate data acquisition services, from management functionality	FR 5.2 APPLICATION PARTITIONING NIST 800-53 SC-2	>1	Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate
FSA-RDF-3	Security Function Isolation	The IACS embedded device shall isolate security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions	FR 5.3 SECURITY FUNCTION ISOLATION NIST 800-53 SC-3	>2	The IACS maintains a separate execution domain (e.g., address space) for each executing process. Some legacy IACS may not implement this capability. In situations where it is not implemented, the organization details its risk acceptance and mitigation in the IACS security plan
FSA-RDF-4	Shared System Resources	The IACS embedded device shall prevent unauthorized and unintended information transfer via shared system resources where it supports connection sessions from users with different levels of access	FR 5.4 INFORMATION REMNANCE NIST 800-53 SC-4	>2 In most cases probably does not apply to single embedded products	Control of IACS remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role from being available to any current user/role that obtains access after that resource has been released back to the IACS For embedded devices could be exposure of passwords or access rights after administrator has been logged in and accessed the privileged information

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-TRE-1	Incident Response Support	The IACS embedded device may provide features to support configurable automated incident notification services to those not currently connected to the IACS	FR6 Timely Response to an Event	>2	This could take the form of e-mail, text message, pager, etc. notification

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-NRA-1	Denial of Service Protection	The IACS embedded device shall protect against or limit the effects of denial of service attacks	FR 7.1 DENIAL OF SERVICE PROTECTION NIST 800-53 SC-5	All	Some aspects covered by communications robustness testing boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks for allocation
FSA-NRA-1.1	Data Flooding Protection	The IACS embedded device shall be capable of taking mitigating actions to attempt to maintain primary function communications while under standard DOS style attacks	FR 7.1 DENIAL OF SERVICE PROTECTION NIST 800-53 SC-5	>2	
FSA-NRA-1.2	Protocol Fuzzing Protection	The IACS embedded device communications shall be tolerant to standard protocol fuzzing attacks for protocols supported by the device	FR 7.1 DENIAL OF SERVICE PROTECTION NIST 800-53 SC-5	All	Target of evaluation may include vendor specified boundary device with specific configuration specified to be included but needs to be tested with boundary device so not Allocatable unless included in documentation and tested
FSA-NRA-1.3	Deterministic Loss of Comm	The IACS embedded device communications shall provide documented or configurable default states for IO and other transmitted variable to be applied upon loss of communications	FR 7.1 DENIAL OF SERVICE PROTECTION NIST 800-53 SC-5	All	Target of evaluation should exhibit deterministic behavior when primary function can no longer be maintained. Need to inform user or allow user to configure this behavior
FSA-NRA-1.4	Notification of Attack	The IACS embedded device communications shall be able to notify the higher level system if experiencing heavy communication demands as would experience under DOS attack	FR 7.1 DENIAL OF SERVICE PROTECTION NIST 800-53 SC-5	>1	Configurable default state on loss of communications is sufficient for level 1 "Notification" can include higher system detection of loss of expected periodic message or network statistics Should consider however need for an attack on a lower level network to be reported to the higher level device on another network that can not directly see the low level attack
FSA-NRA-1.5	Preservation of Essential Services	The IACS embedded device communications shall be able to maintain essential services under flooding attack, as defined in robustness testing specification	FR 7.1 DENIAL OF SERVICE PROTECTION NIST 800-53 SC-5	All	
FSA-NRA-2	IACS Backup	The IACS embedded device or its support utilities shall provide user functionality to facilitate creation of backups of user-level and system-level information (including system security state information) contained in the IACS	FR 7.11 IACS BACKUP NIST 800-53 CP-9	All	Functionality or methods sufficiently described in user manuals

Requirement ID	Reference Name	Requirement Description	Source of Requirement	*ISASecure*™ Level	Comments / Clarifications
FSA-NRA-3	IACS Recovery	The IACS embedded device shall provide user functionality to allow the IACS to be recovered and reconstituted to previously saved IACS Backup after a disruption or failure	FR 7.12 IACS RECOVERY AND RECONSTITUTION NIST 800-53 CP-10	All	