

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference document: Secure Controls Framework (SCF) version 2026.1
 https://securecontrolsframework.com/start-hereset-theory-relationship-mapping-strm/
 STRM Guidance:

Focal Document:
 Focal Document URL:
 Published STRM URL:

IEC 62443-4-2: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
 https://webstore.ansi.org/standards/iec/iec62443-4-2-2019
 https://content.securecontrolsframework.com/strm/scf-strm-general-iec-62443-4-2-2019.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Scope	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2	Normative references	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3	Terms and definitions	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4	Common component security constraints	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 1.1	Human user identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Identification & Authentication for Organizational Users	IA-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
CR 1.1	Human user identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IA-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
CR 1.1(1)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IA-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
CR 1.1(2)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Multi-Factor Authentication (MFA)	IA-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data.	5	
CR 1.2	Software process and device identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Identification & Authentication for Devices	IA-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
CR 1.2(1)	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Identification & Authentication for Devices	IA-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
CR 1.3	Account management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Subset Of	Identity & Access Management (IAM)	IA-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
CR 1.4	Identifier management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Identifier Management (User Names)	IA-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	
CR 1.4	Identifier management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	User Identity (ID) Management	IA-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	
CR 1.5	Authenticator management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Authenticator Management	IA-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
CR 1.5(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Default Authenticators	IA-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
CR 1.5(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Default Authenticators	IA-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
CR 1.5(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Password-Based Authentication	IA-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
CR 1.5(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Protection of Authenticators	IA-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
CR 1.5(1)	Hardware security for authenticators	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Hardware Security Modules (HSM)	IA-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
CR 1.6	Wireless access management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5	
CR 1.7	Strength of password-based authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Password-Based Authentication	IA-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
CR 1.7(1)	Password generation and lifetime restrictions for human users	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Password-Based Authentication	IA-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
CR 1.7(2)	Password lifetime restrictions for all users (human, software process, or device)	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Password-Based Authentication	IA-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
CR 1.8	Public key infrastructure certificates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) application or obtain PKI services from a reputable PKI service provider.	5	
CR 1.9	Strength of public key-based authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Subset Of	Authenticator Management	IA-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
CR 1.9(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	PKI-Based Authentication	IA-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	5	
CR 1.9(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	PKI-Based Authentication	IA-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	5	
CR 1.9(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	PKI-Based Authentication	IA-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	5	
CR 1.9(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
CR 1.9(e)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
CR 1.9(f)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
CR 1.9(1)	Hardware security for public key-based authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Hardware Security Modules (HSM)	IA-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
CR 1.10	Authenticator feedback	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Authenticator Feedback	IA-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	5	
CR 1.11	Unsuccessful login attempts	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Account Lockout	IA-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
CR 1.11(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Account Lockout	IA-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
CR 1.11(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Account Lockout	IA-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
CR 1.12	System use notification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	System Use Notification (Login Banner)	SEA-18	Mechanisms exist to utilize system use notification / login banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	5	
CR 1.12	System use notification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Standardized Microsoft Windows Banner	SEA-18.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system.	5	
CR 1.12	System use notification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Truncated Banner	SEA-18.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized directory services technology (e.g., Active Directory, Entra ID).	5	
CR 1.13	Access via untrusted networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 1.14	Strength of symmetric key-based authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	5	
CR 1.14(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	5	
CR 1.14(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	5	
CR 1.14(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	5	
CR 1.14(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443-4-2-2019	Functional	Intersects With	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CR 1.14(1)	Hardware security for symmetric key-based authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Hardware Security Modules (HSM)	IAE-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	5	
CR 2.1	Authorization enforcement	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Role-Based Access Control (RBAC)	IAE-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
CR 2.1(1)	Authorization enforcement for all users (humans, software processes and devices)	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Role-Based Access Control (RBAC)	IAE-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
CR 2.1(2)	Permission mapping to roles	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Role-Based Access Control (RBAC)	IAE-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8	
CR 2.1(3)	Supervisor override	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Manual Override	IAE-16.5	Mechanisms exist to enable a manual override of the current account privileges to enable the timely response to unusual conditions without terminating the current session and establishing a new session as a higher-privileged user.	5	
CR 2.1(4)	Dual approval	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Dual Approval For High-Impact Environments	CHG-08	Mechanisms exist to require dual approval for any changes that might result in a serious, but adverse impact to: (1) Business processes; and/or (2) Technology Assets, Applications, Services and/or Data (TAASD).	5	
CR 2.2	Wireless use control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CR 2.2	Wireless use control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
CR 2.3	Use control for portable and mobile devices	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 2.4	Mobile code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 2.5	Session lock	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session Lock	IAE-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
CR 2.5(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session Lock	IAE-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
CR 2.5(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session Lock	IAE-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
CR 2.6	Remote session termination	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	5	
CR 2.7	Concurrent session control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Concurrent Session Control	IAE-23	Mechanisms exist to limit the number of concurrent sessions for each system account.	5	
CR 2.8	Auditable events	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
CR 2.8	Auditable events	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
CR 2.9	Audit storage capacity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 2.9(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
CR 2.9(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
CR 2.9(1)	Warn when audit record storage capacity threshold reached	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.	5	
CR 2.10	Response to audit processing failures	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 2.10(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CR 2.10(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5	
CR 2.11	Timestamps	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	5	
CR 2.11(1)	Time synchronization	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
CR 2.11(2)	Protection of time source integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	5	
CR 2.12	Non-repudiation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	5	
CR 2.12(1)	Non-repudiation for all users	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	5	
CR 2.13	Use of physical diagnostic and test interfaces	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 3.1	Communication integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
CR 3.1(1)	Communication authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
CR 3.2	Protection from malicious code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 3.3	Security functionality verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
CR 3.3(1)	Security functionality verification during normal operation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5	
CR 3.4	Software and information integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
CR 3.4(1)	Authenticity of software and information	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
CR 3.4(2)	Automated notification of integrity violations	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
CR 3.5	Input validation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	5	
CR 3.6	Deterministic output	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Fail Safe	SEA-07.3	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	5	
CR 3.7	Error handling	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and (3) Revealing error messages only to authorized personnel.	5	
CR 3.8	Session integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
CR 3.8(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
CR 3.8(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
CR 3.8(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
CR 3.9	Protection of audit information	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CR 3.9(1)	Audit records on write-once media	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Equal	Write Once Read Many (WORM) Event Log Generation	MON-19	Mechanisms exist to produce event logs on hardware-enforced, write-once media (e.g., Write Once Read Many (WORM) technologies).	10	
CR 3.10	Support for updates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
CR 3.11	Physical tamper resistance and detection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
CR 3.12	Provisioning product supplier roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	5	
CR 3.13	Provisioning asset owner roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for system component and service refreshes are obtained from trusted sources.	5	
CR 3.14	Integrity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	5	
CR 4.1	Information confidentiality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 4.1(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
CR 4.1(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
CR 4.2	Information persistence	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
CR 4.2	Information persistence	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.	5	
CR 4.2(1)	Erase of shared memory resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
CR 4.2(2)	Erase verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
CR 4.3	Use of cryptography	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
CR 5.1	Network segmentation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
CR 5.2	Zone boundary protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
CR 5.3	General-purpose person-to-person communication restrictions	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
CR 5.4	Application partitioning	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 6.1	Audit log accessibility	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
CR 6.1	Audit log accessibility	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	5	
CR 6.1(1)	Programmatic access to audit logs	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
CR 6.2	Continuous monitoring	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
CR 7.1	Denial of service protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Fallover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5	
CR 7.1	Denial of service protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
CR 7.1(1)	Manage communication load from component	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5	
CR 7.2	Resource management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
CR 7.3	Control system backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CR 7.3(1)	Backup integrity verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
CR 7.4	Control system recovery and reconstitution	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CR 7.5	Emergency power	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CR 7.6	Network and security configuration settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
CR 7.6(1)	Machine-readable reporting of current security settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CR 7.7	Least functionality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
CR 7.8	Control system component inventory	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
SAR 2.4	Mobile code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SAR 2.4(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SAR 2.4(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SAR 2.4(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SAR 2.4(1)	Mobile code authenticity check	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
SAR 3.2	Protection from malicious code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	
EDR 2.4	Mobile code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
EDR 2.4(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
EDR 2.4(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
EDR 2.4(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
EDR 2.4(1)	Mobile code authenticity check	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
EDR 2.13	Use of physical diagnostic and test interfaces	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Physical Diagnostic & Test Interfaces	TDA-05.1	Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
EDR 2.13(1)	Active monitoring	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Diagnostic & Test Interface Monitoring	TDA-05.2	Mechanisms exist to enable endpoint devices to log events and generate alerts for attempts to access diagnostic and test interfaces.	5	
EDR 3.2	Protection from malicious code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Prevent Alterations	EMB-06	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	5	
EDR 3.10	Support for updates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
EDR 3.10(1)	Update authenticity and integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Certificate-Based Authentication	EMB-16	Mechanisms exist to enforce certificate-based authentication for embedded technologies (e.g., IoT, OT, etc.) and their supporting services.	5	
EDR 3.11	Physical tamper resistance and detection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for indicators of Compromise (IoC).	5	
EDR 3.11(1)	Notification of a tampering attempt	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access devices are detected.	5	
EDR 3.12	Provisioning product supplier roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
EDR 3.13	Provisioning asset owner roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
EDR 3.13(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
EDR 3.13(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
EDR 3.14	Integrity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	5	
EDR 3.14(1)	Authenticity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	5	
HDR 2.4	Mobile code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
HDR 2.4(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
HDR 2.4(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
HDR 2.4(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
HDR 2.4(1)	Mobile code authenticity check	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Certificate-Based Authentication	EMB-16	Mechanisms exist to enforce certificate-based authentication for embedded technologies (e.g., IoT, OT, etc.) and their supporting services.	5	
HDR 2.13	Use of physical diagnostic and test interfaces	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Physical Diagnostic & Test Interfaces	TDA-05.1	Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse.	5	
HDR 2.13(1)	Active monitoring	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Diagnostic & Test Interface Monitoring	TDA-05.2	Mechanisms exist to enable endpoint devices to log events and generate alerts for attempts to access diagnostic and test interfaces.	5	
HDR 3.2	Protection from malicious code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	
HDR 3.2(1)	Report version of code protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage anti-malware technologies.	5	
HDR 3.10	Support for updates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
HDR 3.10	Support for updates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
HDR 3.10(1)	Update authenticity and integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
HDR 3.11	Physical tamper resistance and detection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for indicators of Compromise (IoC).	5	
HDR 3.11(1)	Notification of a tampering attempt	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
HDR 3.12	Provisioning product supplier roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
HDR 3.13	Provisioning asset owner roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
HDR 3.13(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
HDR 3.13(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Zero-Touch Provisioning (ZTP)	CFG-07	Mechanisms exist to implement Zero-Touch Provisioning (ZTP), or similar technology, to automatically and securely configure devices upon being added to a network.	5	
HDR 3.14	Integrity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	5	
HDR 3.14(1)	Authenticity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	5	
NDR 1.6	Wireless access management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
NDR 1.6(1)	Unique Identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	5	
NDR 1.13	Access via untrusted networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
NDR 1.13(1)	Explicit access request approval	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
NDR 1.13(1)	Explicit access request approval	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
NDR 2.4	Mobile code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
NDR 2.4(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
NDR 2.4(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
NDR 2.4(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
NDR 2.4(1)	Mobile code authenticity check	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
NDR 2.13	Use of physical diagnostic and test interfaces	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Physical Diagnostic & Test Interfaces	TDA-05.1	Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse.	5	
NDR 2.13(1)	Active monitoring	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Diagnostic & Test Interface Monitoring	TDA-05.2	Mechanisms exist to enable endpoint devices to log events and generate alerts for attempts to access diagnostic and test interfaces.	5	
NDR 3.2	Protection from malicious code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed019	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
NDR 3.10	Support for updates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
NDR 3.10(1)	Update authenticity and integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
NDR 3.11	Physical tamper resistance and detection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IOC).	5	
NDR 3.11(1)	Notification of a tampering attempt	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
NDR 3.12	Provisioning product supplier roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
NDR 3.13	Provisioning asset owner roots of trust	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
NDR 3.13(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
NDR 3.13(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
NDR 3.14	Integrity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of systems.	5	
NDR 3.14(1)	Authenticity of the boot process	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in systems.	5	
NDR 5.2	Zone boundary protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
NDR 5.2(1)	Deny all, permit by exception	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
NDR 5.2(2)	Island mode	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
NDR 5.2(3)	Fail close	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.	5	
NDR 5.3	General purpose, person-to-person communication restrictions	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.ansi.org/standards/iec/iec62443ed2019	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	