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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - DoW Brilliant at the Basics: Top 10 OT Cybersecurity Best Practices for DIB Partners**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_OT-Tipsv2.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-ot.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	Legacy SCF #
1	Identity and Access Control	Manage who has access to your OT by enforcing strict identity and access control. Ensure your system verifies the identity of every user via stringent authentication methods before allowing access to your network. Enforce strong access controls and require multi-factor authentication (MFA) for sensitive systems. Under Zero Trust, users should only be granted the "least privilege" needed to do their specific job, nothing more. Adopt a "never trust, always verify" mindset to protect your business.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	8		IAC-01
1	Identity and Access Control	Manage who has access to your OT by enforcing strict identity and access control. Ensure your system verifies the identity of every user via stringent authentication methods before allowing access to your network. Enforce strong access controls and require multi-factor authentication (MFA) for sensitive systems. Under Zero Trust, users should only be granted the "least privilege" needed to do their specific job, nothing more. Adopt a "never trust, always verify" mindset to protect your business.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	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		IAC-08
1	Identity and Access Control	Manage who has access to your OT by enforcing strict identity and access control. Ensure your system verifies the identity of every user via stringent authentication methods before allowing access to your network. Enforce strong access controls and require multi-factor authentication (MFA) for sensitive systems. Under Zero Trust, users should only be granted the "least privilege" needed to do their specific job, nothing more. Adopt a "never trust, always verify" mindset to protect your business.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8		IAC-21
1	Identity and Access Control	Manage who has access to your OT by enforcing strict identity and access control. Ensure your system verifies the identity of every user via stringent authentication methods before allowing access to your network. Enforce strong access controls and require multi-factor authentication (MFA) for sensitive systems. Under Zero Trust, users should only be granted the "least privilege" needed to do their specific job, nothing more. Adopt a "never trust, always verify" mindset to protect your business.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	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 and/or regulated data.	5		IAC-06
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Asset Inventories	AST-04	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.	8		AST-02
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	3		AST-03
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities; (3) Maintain compliance; and (4) Maintain resilient capabilities.	8		
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-05	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive secure baseline configurations.	3		CFG-02.5
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Embedded Technology Inventory Management	EMB-04	Mechanisms exist to augment organizational IT Asset Management (ITAM) processes for Operational Technology (OT) and Internet of Things (IoT) devices with: (1) Passive network monitoring; and (2) Periodic physical inspections.	8		

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - DoW Brilliant at the Basics: Top 10 OT Cybersecurity Best Practices for DIB Partners**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_OT-Tipsv2.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-ot.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	Legacy SCF #
2	Validated Asset Inventory	The first step for any business is to create and maintain a rigorous, "as-operated" inventory of all physical and logical components within your OT environment. This includes tracking high-criticality assets such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs), Engineering Workstations, Distributed Control Systems (DCS), and Safety Instrumented Systems (SIS). To ensure a comprehensive baseline for risk management and threat detection, the inventory must catalog not only hardware but also firmware/software versions, active communication protocols, process logic/OT programs, transient assets, and external remote-access connection points. Ensure that all systems have clear ownership, accountability, and secure configuration baseline. Finally, validate this inventory through passive network monitoring and periodic physical walk-downs to eliminate shadow systems and map critical operational dependencies without disrupting live processes.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	5		EMB-03
3	Strict Network Segmentation	A key architectural step is to logically separate your business IT network from your critical operational systems. By creating strict partitions, or segments, you make it much harder for an intruder who gains access to one part of your network to move laterally and disrupt your core functions. This containment is a powerful defensive measure. A flat network is a vulnerable network.	Functional	Subset Of	Separate Operating Environments For Embedded Technologies	EMB-03	Mechanisms exist to logically or physically separate embedded technologies from organizational Information Technology (IT) networks.	10		
3	Strict Network Segmentation	A key architectural step is to logically separate your business IT network from your critical operational systems. By creating strict partitions, or segments, you make it much harder for an intruder who gains access to one part of your network to move laterally and disrupt your core functions. This containment is a powerful defensive measure. A flat network is a vulnerable network.	Functional	Intersects With	Separate Subnets To Isolate Functions	NET-08	Mechanisms exist to implement physically or logically separate subnetworks to isolate organization-defined Technology Assets, Applications, Services and/or Data (TAASD).	5		NET-06.9
3	Strict Network Segmentation	A key architectural step is to logically separate your business IT network from your critical operational systems. By creating strict partitions, or segments, you make it much harder for an intruder who gains access to one part of your network to move laterally and disrupt your core functions. This containment is a powerful defensive measure. A flat network is a vulnerable network.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		SEA-01.5
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	5		
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Data Backups	BCD-24	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		BCD-11
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Redundant Copies of Business-Critical Data	BCD-25	Mechanisms exist to maintain redundant copies of all business-critical data within one(1), or more, logically vaulted or offline environments.	5		
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8		IRO-02
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - DoW Brilliant at the Basics: Top 10 OT Cybersecurity Best Practices for DIB Partners**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_OT-Tipsv2.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-ot.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	Legacy SCF #
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Embedded Technology Incidents	IRO-25	Mechanisms exist to handle failures and/or incidents with embedded technologies.	8		
4	OT-Specific Incident Response and Recovery Plan	A well-rehearsed, OT-specific Incident Response Plan (IRP) is critical for safeguarding mission assurance and maintaining operational resilience against cyber-physical disruptions. Unlike enterprise IT, OT incident response prioritizes life safety, environmental protection, and physical availability, meaning abrupt system shutdowns are rarely a viable containment strategy. A robust plan requires maintaining offline backups, segregating Safety Instrumented Systems (SIS), and coordinating closely with external vendors to validate embedded firmware. During an event, response teams must quickly correlate network anomalies with physical process deviations and safely transition to manual control. Finally, recovery demands scrubbing malicious logic, executing localized and phased physical restarts with joint sign-off from both cybersecurity and process engineering leads, and integrating lessons learned into regular cross-functional tabletop exercises.	Functional	Intersects With	Post-Incident Technology Assets, Applications and Services (TAAS) Validation	IRO-26	Mechanisms exist to utilize post-incident assurance activities to validate Technology Assets, Applications and Services (TAAS) are (1) Secure; (2) Compliant; and (3) Capable of supporting the resumption of normal business operations.	8		
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-14	Automated mechanisms exist to prevent the execution of unauthorized software programs.	3		CFG-03.2
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	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		NET-03
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	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		NET-04
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Microsegmentation	NET-11	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5		NET-06.6
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or (4) Accepting the risk.	5		RSK-06.3
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
5	Manage Known Exploitable Vulnerabilities	To protect critical infrastructure, prioritize compensating controls when you cannot immediately patch operational equipment. Because taking machinery offline for patching is often impossible due to mission-critical availability requirements, compensating controls act as essential, temporary safeguards. These measures-including strict firewall rules, network isolation/micro-segmentation, and application allowlisting-effectively isolate vulnerable devices from exploitation until they can be safely updated during a scheduled maintenance window.	Functional	Intersects With	Known Exploited Vulnerabilities (KEV) Mitigations	VPM-06.3	Mechanisms exist to prioritize remediation and mitigation of Known Exploited Vulnerabilities (KEV) by: (1) Reducing or removing public exposure to exploitation; and (2) Expediting patch deployment actions.	8		VPM-02.1

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - DoW Brilliant at the Basics: Top 10 OT Cybersecurity Best Practices for DIB Partners
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_OT-Tipsv2.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-ot.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	Legacy SCF #
6	Remote Access Pathways	Grant remote access to your OT only when needed, for the shortest time possible, and with strong authentication. Eliminate "always-on" connections to reduce your exposure to external threats, particularly cellular gateways and other direct internet-exposed assets. Many businesses rely on vendors or remote employees for support, but every remote connection is a potential door to your network.	Functional	Intersects With	Separate Operating Environments For Embedded Technologies	EMB-03	Mechanisms exist to logically or physically separate embedded technologies from organizational Information Technology (IT) networks.	8		
6	Remote Access Pathways	Grant remote access to your OT only when needed, for the shortest time possible, and with strong authentication. Eliminate "always-on" connections to reduce your exposure to external threats, particularly cellular gateways and other direct internet-exposed assets. Many businesses rely on vendors or remote employees for support, but every remote connection is a potential door to your network.	Functional	Intersects With	Remote Management of Embedded Technologies	EMB-15	Mechanisms exist to restrict remote management of embedded technologies by: (1) Allowing access only when needed; (2) Eliminating "always on" connections; and (3) Requiring strong authentication.	8		
6	Remote Access Pathways	Grant remote access to your OT only when needed, for the shortest time possible, and with strong authentication. Eliminate "always-on" connections to reduce your exposure to external threats, particularly cellular gateways and other direct internet-exposed assets. Many businesses rely on vendors or remote employees for support, but every remote connection is a potential door to your network.	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8		NET-14
6	Remote Access Pathways	Grant remote access to your OT only when needed, for the shortest time possible, and with strong authentication. Eliminate "always-on" connections to reduce your exposure to external threats, particularly cellular gateways and other direct internet-exposed assets. Many businesses rely on vendors or remote employees for support, but every remote connection is a potential door to your network.	Functional	Intersects With	Remote Access Pathways	NET-26.1	Mechanisms exist to route all remote access pathways through managed network access control points (e.g., VPN concentrator).	5		NET-14.3
6	Remote Access Pathways	Grant remote access to your OT only when needed, for the shortest time possible, and with strong authentication. Eliminate "always-on" connections to reduce your exposure to external threats, particularly cellular gateways and other direct internet-exposed assets. Many businesses rely on vendors or remote employees for support, but every remote connection is a potential door to your network.	Functional	Intersects With	Third-Party Remote Access Governance	NET-30	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5		NET-14.6
7	Continuous Monitoring	Extend basic monitoring to the production floor to detect unusual traffic or unauthorized access to machinery. Many firewall and antivirus solutions include logging features that can provide visibility. Regularly reviewing these logs helps you spot and respond to threats before they cause damage. Remember, you can't stop what you can't see!	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-08	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	5		EMB-05
7	Continuous Monitoring	Extend basic monitoring to the production floor to detect unusual traffic or unauthorized access to machinery. Many firewall and antivirus solutions include logging features that can provide visibility. Regularly reviewing these logs helps you spot and respond to threats before they cause damage. Remember, you can't stop what you can't see!	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
7	Continuous Monitoring	Extend basic monitoring to the production floor to detect unusual traffic or unauthorized access to machinery. Many firewall and antivirus solutions include logging features that can provide visibility. Regularly reviewing these logs helps you spot and respond to threats before they cause damage. Remember, you can't stop what you can't see!	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
7	Continuous Monitoring	Extend basic monitoring to the production floor to detect unusual traffic or unauthorized access to machinery. Many firewall and antivirus solutions include logging features that can provide visibility. Regularly reviewing these logs helps you spot and respond to threats before they cause damage. Remember, you can't stop what you can't see!	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	3		NET-08
8	System Resiliency	Build your systems to be resilient from the start by mandating secure, composable architecture. Design your industrial networks to fail safely. When upgrading control systems, prioritize resilience by grouping assets by physical location and sensitivity. A secure, modular approach ensures that critical machinery incorporates fault tolerance, physical redundancy, and localized manual overrides, meaning a cyber disruption to one component won't stop your entire production line.	Functional	Intersects With	Predictable Failure Analysis	AST-40	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	3		SEA-07
8	System Resiliency	Build your systems to be resilient from the start by mandating secure, composable architecture. Design your industrial networks to fail safely. When upgrading control systems, prioritize resilience by grouping assets by physical location and sensitivity. A secure, modular approach ensures that critical machinery incorporates fault tolerance, physical redundancy, and localized manual overrides, meaning a cyber disruption to one component won't stop your entire production line.	Functional	Intersects With	Redundant Secondary System	BCD-21	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	3		BCD-11.7
8	System Resiliency	Build your systems to be resilient from the start by mandating secure, composable architecture. Design your industrial networks to fail safely. When upgrading control systems, prioritize resilience by grouping assets by physical location and sensitivity. A secure, modular approach ensures that critical machinery incorporates fault tolerance, physical redundancy, and localized manual overrides, meaning a cyber disruption to one component won't stop your entire production line.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		SEA-01.5
8	System Resiliency	Build your systems to be resilient from the start by mandating secure, composable architecture. Design your industrial networks to fail safely. When upgrading control systems, prioritize resilience by grouping assets by physical location and sensitivity. A secure, modular approach ensures that critical machinery incorporates fault tolerance, physical redundancy, and localized manual overrides, meaning a cyber disruption to one component won't stop your entire production line.	Functional	Intersects With	Fail Safe	SEA-16	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	5		SEA-07.3
9	Supply Chain Security	Knowing your suppliers is critical to mitigating vulnerabilities. This is accomplished through things like proactive procurement, lifecycle management, and supply chain illumination. Your company's security is connected to the security of your suppliers. It is crucial to understand the entirety of your organization's supply chain and to hold external suppliers to the same security standards as that of the organization to maintain the overall level of security. Requiring vendors to engineer systems and system components to DoW standards ensures built-in security features before purchase. For legacy OT, programs need to set a hard schedule to replace undefendable hardware.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17
9	Supply Chain Security	Knowing your suppliers is critical to mitigating vulnerabilities. This is accomplished through things like proactive procurement, lifecycle management, and supply chain illumination. Your company's security is connected to the security of your suppliers. It is crucial to understand the entirety of your organization's supply chain and to hold external suppliers to the same security standards as that of the organization to maintain the overall level of security. Requiring vendors to engineer systems and system components to DoW standards ensures built-in security features before purchase. For legacy OT, programs need to set a hard schedule to replace undefendable hardware.	Functional	Subset Of	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10		TPM-03
9	Supply Chain Security	Knowing your suppliers is critical to mitigating vulnerabilities. This is accomplished through things like proactive procurement, lifecycle management, and supply chain illumination. Your company's security is connected to the security of your suppliers. It is crucial to understand the entirety of your organization's supply chain and to hold external suppliers to the same security standards as that of the organization to maintain the overall level of security. Requiring vendors to engineer systems and system components to DoW standards ensures built-in security features before purchase. For legacy OT, programs need to set a hard schedule to replace undefendable hardware.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8		TPM-05
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	5		CHG-01
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Safety Assessment	EMB-19	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	3		EMB-15

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - DoW Brilliant at the Basics: Top 10 OT Cybersecurity Best Practices for DIB Partners**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_OT-Tipsv2.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-ot.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	Legacy SCF #
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	3		IAO-01
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Assessment Boundaries	IAO-03	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the Technology Assets, Applications, Services and/or Data (TAASD) under review.	3		IAO-01.1
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3		IAO-02
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	3		IAO-03
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-10	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	3		IAO-04
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Technical Verification	IAO-11	Mechanisms exist to perform Control Validation Testing (CVT) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	3		IAO-06
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Security Assessment Report (SAR)	IAO-13	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	3		IAO-02.4
10	Review Processes	For businesses with physical operations, safety and security go hand-in-hand. Before making any significant changes to your systems, including security updates, it's crucial to have a formal review process. This engineers safety and mission assurance into all changes in order to ensure that a security change doesn't accidentally create an unsafe condition for your employees or your operations.	Functional	Intersects With	Security Authorization	IAO-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	3		IAO-07