TEMPERED NETWORKS®

The Cybersecurity Framework – Manufacturing Profile

Reducing risk and facilitating NIST Compliance with an Identity-Defined Network (IDN) Architecture

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Table of Contents

Overview of NIST Cybersecurity Framework (CSF)

The CSF offers a dynamic set of cybersecurity practices, outcomes, and technical, operational, and managerial security controls that are designed to help organizations manage cybersecurity risk. These controls support the five risk management functions of the CSF: Identify, Protect, Detect, Respond, and Recover. While intended for adoption by the critical infrastructure sector, the foundational set of cybersecurity disciplines that make up the CSF have been supported by government and industry as a recommended baseline for use by any organization, regardless of its sector or size. A recent Gartner report estimated that the CSF is used by approximately 30% of U.S. organizations and projected to reach 50% by 2020.

The Manufacturing 'Target' Profile

The CSF "Manufacturing Profile" can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices.

The profile gives manufacturers:

- A method to identify opportunities for improving the current cybersecurity posture of the manufacturing system
- An evaluation of their ability to operate the control environment at their acceptable risk level
- A standardized approach to preparing the cybersecurity plan for ongoing assurance of the manufacturing system's security

By prioritizing security activities that meet specific business/mission goals, and identifying relevant and actionable security practices that can be implemented to support those key goals, you now can align cybersecurity activities with business requirements, risk tolerances, and resources.

The challenge of reducing cybersecurity risk for manufacturing companies

As organizations take steps towards digital transformation and the 'modern connected plant', they are faced with difficulties on how to ensure the confidentiality, availability, and integrity of today's sensitive information and mission-critical systems, as well as how to integrate industrial control systems (ICS) and information technology (IT). The largest barrier for most organizations is how to securely connect devices and "things" that cannot protect themselves to the network, and the wide array of new security risks and networking challenges that come with each additional addition.

Integrating these 'things' adds to the ecosystem of ever-increasing complexity for IT teams, and requires multiple tools and technologies to manage with a patchwork of VLANs, Access Control Lists, routing rules, and firewall policies that need to be configured for each device being added to the network. This approach is complex, prone to error, and difficult to scale for organizations with geographically distributed resources. A better solution is needed for manufacturing organizations.

Identity-Defined Networking enables conformance to the NIST CSF

Tempered Networks offers a unified networking and security architecture that simplifies today's complex and inherently vulnerable networks. IDN delivers a security model that assigns hardened machine (host) identities to any IP-networked device, so that each machine is defined by a cryptographic identity (CID) – instead of an unsecure IP address. With secure peer-to-peer networking for any device, anywhere in the world, across physical, virtual, and cloud domains, it's now easy to overcome impassable network barriers and borders like multi-NAT, CG-NAT, dynamic IP addressing, IP conflicts, and unwieldy inbound firewall rules for example.

An IDN architecture delivers:

- Orchestration for rapid provisioning, revocation, and instant verifiable quarantine
- Device cloaking and automatic AES-256 encryption between all IDN endpoints
- Device-level isolation and unbreakable micro, macro, and cross-boundary segmentation
- Connectivity for secure Layer 2 or Layer 3 networks across any link medium
- Network resiliency and instant failover

With IDN, you can now strengthen your cybersecurity posture by building an integrated, automated, simple, and secure network architecture to align with the business outcomes in the CSF. With built-in security and a level of segmented connectivity that simply hasn't been possible until now, Tempered Networks delivers strong cybersecurity risk management practices for each interconnected system to protect the confidentiality, integrity and availability of data.

Using Tempered Networks, it's easy to align with the CSF Core and achieve secure connectivity and segmentation at scale for any device, anywhere in the world, across any network environment.

Control Objectives	Tempered Networks
Identify	✓
Protect	✓
Detect	✗
Respond	✓
Recover	✓

Quick overview of the 5 core functions of CSF

Core Function: Identify

Tempered Networks does not provide in-depth asset management; however, no unauthorized devices can connect to the IDN fabric without being whitelisted first through their unique cryptographic identity. This means all connections are authorized, and then documented and reviewed using the Conductor's Visual Trust Map and user activity logs. With simple and secure remote access that can be micro-segmented down to the individual device based on user privilege, managing complex vendor eco-systems is now simple and fast, significantly reducing your supply chain risks.

Core Function: Protect

Establishing and managing identification mechanisms for your network is easy, with access to individual devices within the IDN fabric that is based on machine authentication and authorization of unique cryptographic identities. Through built-in security with peer-to-peer AES 256 encryption and verifiable isolation that ensures data security, organizations can now significantly reduce the total available attack surface, while at the same time improving availability and resiliency of the network with simple and automated disaster recovery. Achieving the same level of secure connectivity and segmentation with other solutions is simply impractical, if not impossible.

Core Function: Detect

Tempered Networks does not provide any detection capabilities. However, using the RESTful API, you can integrate IDN with other third-party security and networking services like directory services, SIEMs, IPS/IDS, and other monitoring tools. Through simple integration with these detection systems, you can now build event-based logic for real-time isolation, mitigation, and disaster recovery across the adaptive IDN fabric.

Core Function: Respond

IDN helps you respond to security incidents in real-time. Either manually, or using the secure API, you can now remove and quarantine a compromised device out of hundreds of networks—instantly. And for further analysis, suspect traffic can be re-directed and quarantined to a purpose-built lab, without the attacker being aware that the network has changed.

Core Function: Recover

This section is focused on recovery processes, which Tempered Networks does not provide. However, with simple and automated disaster recovery, organizations can achieve a level of availability and resiliency that previously was impractical, if not impossible. This results in significantly reducing the risk of a cyber event, while minimizing interruption of revenue-generating activities.

Conclusion

As manufacturers are moving towards an integrated architecture, with connectivity across the plant floor, the corporate datacenter, and cloud providers, they are faced with how to address complexity and connectivity challenges that span the entire network.

Tempered Networks solves these challenges by delivering a secure networking architecture that spans the entire network and enables you to secure network segments and to transform vulnerable IP-enabled devices into hardened, invisible assets. This unified approach to security and networking will help manufacturers innovate and continue their digital transformation journey in the years ahead.

You can now easily enable conformance to the NIST CSF through a prioritized, flexible, repeatable, performance-based, and cost-effective approach to managing cybersecurity risk for the systems directly involved in the manufacturing process.

References

- https://www.nist.gov
- http://csrc.nist.gov/
- http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft2.pdf

To learn more about how Tempered Networks can help you comply with NIST CSF security controls, email: info@temperednetworks.com or visit www.temperednetworks.com

Function	Category	Subcategory	Manufacturing Profile	Tempered Networks Applicabiltity
IDENTIFY	Asset Management (ID.AM)	ID.AM-1	Low	
			Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	Tempered Networks does not provide in-depth asset management; however, no unauthorized devices can connect to the IDN fabric without being whitelisted first via their unique cryptographic idenitity. This means all connections are authorized, and then documented and reviewed using the Conductor's Visual Trust Map and user activity logs.
			Moderate	
			Identify individuals who are both responsible and accountable for administering manufacturing system components.	With role-based access control (RBAC), organizations can give control of specific network segments to specific individuals or business units, with verifiable levels of authorized access and control depending on role.
			High	
			Employ automated mechanisms where safe and feasible to detect the presence of unauthorized hardware and firmware components within the system.	No unauthorized device can participate within the IDN fabric without being whitelisted first using the unique crypto-ID assigned to the device(s).

IDENTIFY	Asset Management (ID.AM)	ID.AM-2	Low	
			Document an inventory of manufacturing system software components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, HMI and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	Tempered Networks does not provide this level of information. Known attributes of connected devices is IP and MAC addresses.
			Moderate	
			Update the inventory of manufacturing system software as an integral part of component installations, removals, and system updates. Identify individuals who are both responsible and accountable for administering manufacturing system software.	With role-based access control (RBAC), organizations can give control of specific network segments to specific individuals or business units, with verifiable levels of authorized access and control depending on role.
			High	
			Employ automated mechanisms where safe and feasible to detect the presence of unauthorized software within the system.	Not Applicable - Other Technology
		ID.AM-3	Low	
			Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.	While this requirement is designed for updated record keeping and not directly applicable to Tempered Network's enforcement function, the Visual Trust Map shows all authorized machines that are allowed and currently communicating with others within the individual network segment. In addition, the Conductor provides a real-time record of all systems that are online, active, and when they last connected to the overlay.

IDENTIFY	Asset Management (ID.AM)	ID.AM-3	Moderate and High	
			Map the flow of information within the manufacturing system and to external systems.	No unauthorized (or external) systems or device can participate within the IDN fabric without being whitelisted first using the unique crypto-ID assigned to the device(s). The flow of information is easily verifiable through the Visual Trust Map.
		ID.AM-4	Low	
			Identify and document all external connections for the manufacturing system. Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services. Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services.	No unauthorized (or external) systems or device can participate within the IDN fabric without being whitelisted first using the unique crypto-ID assigned to the device(s). Verifiable and easy documentation is provided through the Conductor.
			Moderate and High	
			Require external providers to identify the functions, ports, protocols, and other services required for the use with the manufacturing system.	Not Applicable - Process Requirement
		ID.AM-5	Low, Moderate and High	
			Identify and prioritize manufacturing system components and functions based on their classification, criticality, and business value. Identify the types of information in possession, custody, or control for which security safeguards are needed (e.g. sensitive or protected information). Address the security of protected information in its third-party relationships.	Not Applicable - Process Requirement

IDENTIFY	Asset Management (ID.AM)	ID.AM-6	Low, Moderate and High	
			Establish and maintain personnel cybersecurity roles and responsibilities for the manufacturing system. Include cybersecurity roles and responsibilities for third-party providers. Third-party providers are required to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components. Third-party providers include, for example, service providers, contractors, and other organizations providing manufacturing system development, technology services, outsourced applications, or network and security management.	The Conductor provides reporting of authorized users and level of control of individual network segments. Instantly revoking a machine from the IDN fabric means completely shutting off the ability to communicate, significantly simplifying third-party access.
	Business Environment (ID.BE)	ID.BE-1	Low and Moderate	
			Define and communicate the organization's role in the supply chain. Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system.	While this requirement is designed for updated record keeping and not directly applicable to Tempered Network's enforcement function, managing third-party access is easy with IDN by building individual network segments for both upstream and downstream supply channels based on their role.
			High	
			Protect against supply chain threats to the manufacturing system, system components, or system services by employing security safeguards as part of a comprehensive, defense-in-depth security strategy.	Tempered Networks is uniquely positioned to significantly reduce the complexity of third-party ecosystems with hardened and verifiable segmentation of individual systems and devices. Access from anywhere in the world can be granted and revoked in seconds, with segmentation down to the individual system or device deep inside the network.

IDENTIFY	Business Environment (ID.BE)	ID.BE-2	Low, Moderate and High	
			Define and communicate the manufacturer's place in critical infrastructure and its industry sector. Define and communicate critical infrastructure and key resources relevant to the manufacturing system. Develop, document, and maintain a critical infrastructure and key resources protection plan. Define and communicate critical infrastructure and key resources relevant to the manufacturing system. Develop, document, and maintain a critical infrastructure and key resources protection plan.	Not Applicable - Process Requirement
		ID.BE-3	Low, Moderate and High	
			Establish and communicate priorities for manufacturing missions, objectives, and activities with consideration for security and the resulting risk to manufacturing operations, components, and individuals. Identify critical manufacturing system components and functions by performing a criticality analysis. Identify critical manufacturing system components and functions by performing a criticality analysis.	Not Applicable - Process Requirement
		ID.BE-4	Low	
			Identify and prioritize supporting services for critical manufacturing system processes and components. Provide an uninterruptable power supply for identified critical manufacturing system components to facilitate the transition of the manufacturing system to long-term alternate power in the event of a primary power source loss.	While this requirement is not directly applicable to Tempered Networks, the IDN fabric can protect the power controls of manufacturing system processes and components, as well as provide automated disaster recovery and failover.
			Moderate and High	
			Identify alternate and redundant supporting services for critical manufacturing system processes and components.	Not Applicable - Process Requirement

IDENTIFY	Business Environment (ID.BE)	ID.BE-5	Low	
			Establish resilience requirements for the manufacturing system to support delivery of critical services.	Not Applicable - Process Requirement
			Moderate	
			Define recovery time objective and recovery point objective for the resumption of essential manufacturing system processes. Identify critical manufacturing system assets that support essential manufacturing system processes.	Not Applicable - Process Requirement
			High	
			Conduct capacity planning for manufacturing system processing, telecommunications, and environmental support as required during contingency operations. Conduct contingency planning for the continuance of essential manufacturing functions and services with little or no loss of operational continuity, and sustain that continuity until full system restoration.	Not Applicable - Process Requirement

IDENTIFY	Governance (ID.GV)	ID.GV-1	Low, Moderate and High	
			Develop and disseminate a security policy that provides an overview of the security requirements for the manufacturing system. The policy includes for example the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the manufacturing system. Review and update the security policy as determined necessary. Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by manufacturing operations.	Not Applicable - Process Requirement. However, Tempered Networks can aid in this process by providing logs for user activities and role-based access-control for individual network segments.
		ID.GV-2	Low, Moderate and High	
			Develop and disseminate a security program for the manufacturing system that includes, for example, the identification of personnel security roles and assignment of responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements, roles and responsibilities for third-party providers. Review and update the security program as determined necessary.	Not Applicable - Process Requirement

IDENTIFY	Governance (ID.GV)	ID.GV-3	Low, Moderate and High	
			Ensure that legal and regulatory requirements affecting the manufacturing operations regarding cybersecurity are understood and managed.	Not Applicable - Process Requirement
		ID.GV-4	Low, Moderate and High	
			Develop a comprehensive strategy to manage risk to manufacturing operations. Include cybersecurity considerations in the risk management strategy. Review and update the risk management strategy as determined necessary. Determine and allocate required resources to protect the manufacturing system.	Not Applicable - Process Requirement
	Risk Assessment (ID.RA)	ID.RA-1	Low and Moderate	
			Develop a plan to identify, document, and report vulnerabilities that exist on the manufacturing system. Include the use of vulnerability scanning where safe and feasible on the manufacturing system, its components, or a representative system. Develop a plan for continuous monitoring of the security posture of the manufacturing system to facilitate ongoing awareness of vulnerabilities. Conduct risk assessments on the manufacturing system that take into account vulnerabilities and potential impact to manufacturing operations and assets.	Not Applicable - Process Requirement. However, IDN enables organizations to cloak critical infrastructure (e.g networks, control systems, endpoints, etc.) from threat action reconnaissance. Cloaked endpoints and networks have no visible TCP/IP footprint and are invisible to the underlying network and any untrusted devices or systems, which protects against DDOS, MiTM attacks, IP spoofing and other types of network and transport layer attacks.

IDENTIFY	Risk Assessment (ID.RA)	ID.RA-1	High Conduct performance/load testing and penetration testing on the manufacturing system with care to ensure that manufacturing operations are not adversely impacted by the testing process. Identify where manufacturing system vulnerabilities may be exposed to adversaries. Production systems may need to be taken off-line before testing can be conducted. If the manufacturing system is taken off-line for testing, tests are scheduled to occur during planned manufacturing outages whenever possible. If penetration testing is performed on non-manufacturing networks, extra care is taken to ensure that tests do not propagate into the manufacturing network.	Not Applicable - Process Requirement. However, the ability to create networks in seconds with simple segmentation makes it easy to build and configure network segments that are separate from production environments for penetration testing.

IDENTIFY	Risk Assessment (ID.RA)	ID.RA-2	Low and Moderate	
			Establish and maintain ongoing contact with security groups and associations, and receive security alerts and advisories. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Implement a threat awareness program that includes a cross- organization information-sharing capability. Organizations should consider having both an unclassified and classified information sharing capability. Collaborate and share information about potential vulnerabilities and incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.	Not Applicable - Process Requirement
			High	
			Employ automated mechanisms where technically feasible to make security alert and advisory information available throughout the organization.	Not Applicable - Process Requirement. However, the Conductor provides automated alerting capabilities for email, as an example.
		ID.RA-3	Low, Moderate and High	
			Conduct and document periodic assessment of risk to the manufacturing system that takes into account threats and likelihood of impact to manufacturing operations and assets. The risk assessment includes threats from insiders and external parties.	Not Applicable - Process Requirement. However, organizations can permanently revoke a machine(s) from the IDN fabric. Even if the user credentials are active, without being whitelisted to the IDN fabric no access will be granted.

IDENTIFY	Risk Management Strategy (ID.RM)	ID.RA-4	Low, Moderate and High	
			Conduct criticality reviews of the manufacturing system that define the potential adverse impacts to manufacturing operations, assets, and individuals if compromised or disabled.	Not Applicable - Process Requirement
		ID.RA-5	Low, Moderate and High	
			Conduct risk assessments of the manufacturing system incorporating threats, vulnerabilities, likelihood, and impact to manufacturing operations, assets, and individuals. Disseminate risk assessment results to relevant stakeholders.	Tempered Networks can assist in the threat and risk assessment by providing verifiable reporting of network segmentation, user activity and level of control and access based on role.
		ID.RA-6	Low, Moderate and High	
			Develop and implement a comprehensive strategy to manage risk to the manufacturing system that includes the identification and prioritization of risk responses.	Not Applicable - Process Requirement
		ID.RM-1	Low, Moderate and High	
			Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally.	Not Applicable - Process Requirement
		ID.RM-2	Low, Moderate and High	
			Define the risk tolerance for the manufacturing system.	Not Applicable - Process Requirement
		ID.RM-3	Low, Moderate and High	
			Ensure the risk tolerance for the manufacturing system is informed by the organization's role in critical infrastructure and sector-specific risk analysis.	Not Applicable - Process Requirement
PROTECT	Access Control (PR.AC)	PR.AC-1	Low	
			Establish and manage identification mechanisms and credentials for users and devices of the manufacturing system.	No unauthorized device(s) can participate within the IDN fabric without being whitelisted first using the unique crypto-ID assigned to the device(s). Even if the user credentials are active, without being whitelisted to the IDN fabric using the unique crypto-ID, no access is granted.

PROTECT	Access Control (PR.AC)	PR.AC-1	Moderate	
			Employ automated mechanisms where feasible to support the management and auditing of information system credentials.	Not Applicable - Process Requirement
			High	
			Deactivate system credentials after a specified time period of inactivity, unless this would result in a compromise to safe operation of the process. Monitor the manufacturing system for atypical use of system credentials. Credentials associated with significant risk are disabled.	Tempered Networks provides logs for user activities, hightlighting failed login events, along with timestamps. In addition, passwords can be configured as a requirement by the Admin. Without whitelisted authorization, no device(s) can participate within the IDN fabric.
		PR.AC-2	Low	
			Protect physical access to the manufacturing facility. Determine access requirements during emergency situations. Physical access controls may include, for example, lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access. Maintain and review visitor access records to the facility where the manufacturing system resides.	Not Applicable - Process Requirement
			Moderate	
			Protect power equipment, power cabling, network cabling, and network access interfaces for the manufacturing system from accidental damage, disruption, and physical tampering. Ensure availability and integrity of wireless systems, especially safety related systems. Employ redundant and physically separated power systems for critical manufacturing operations.	While this requirement is not directly applicable to Tempered Networks, the IDN fabric can protect the power controls of manufacturing system processes and components, as well as provide automated disaster recovery and failover. This means higher availability and integrity of systems.
			High	
			Control physical access to the manufacturing system in addition to the physical access for the facility.	Not Applicable - Process Requirement

PROTECT	Access Control (PR.AC)	PR.AC-3	Low	
			Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the manufacturing system. Remote access methods include, for example, wireless, dial-up, broadband, VPN connections, mobile device connections, and communications through external networks. Provide an explicit indication of active remote access connections to users physically present at the devices.	Remote access to any system or device is incredibly easy with Tempered Networks. IDN delivers secure network connectivity for any device, anywhere in the world, across any network environment that can be granted or revoked in seconds - allowing organizations to elimiate complicated VPN technologies.
			Moderate and High	
			Allow remote access only through approved and managed access points. Monitor remote access to the manufacturing system, and employ cryptographic mechanisms where determined necessary. Allow only authorized use of privileged functions from remote access. Establish agreements and verify security for connections with external systems.	IDN delivers simple and secure remote access from anywhere in the world, for any device, with built-in peer-to-peer AES 256 encryption. Unless a machine is explicitly allowed to communicate within the IDN fabric, it simply cannot connect.
		PR.AC-4	Low	
			Define and manage access permissions for users of the manufacturing system. Identify and document user actions that can be performed on the manufacturing system without identification or authentication (e.g. during emergencies).	The Conductor provides reporting of authorized users and level of control of individual network segments. No communication is allowed unless explicity whitelisted.

PROTECT	Access Control (PR.AC)	PR.AC-4	Moderate	
			Employ automated mechanisms where feasible to support the management of manufacturing system user accounts, including the disabling, auditing, notification, and removal of user accounts. Implement separation of duties for manufacturing system users. Limit, document, and explicitly authorize privileged user access to the manufacturing system. Audit the execution of privileged functions on the manufacturing system. Separation of duties includes, for example: dividing operational functions and system support functions among different roles; conducting system support functions with different individuals; and ensuring security personnel administering access control functions do not also administer audit functions.	Tempered Networks can create separation of duties by restriciting network and device access according to the defined job role. Even if the user credentials are active, without being whitelisted to the IDN fabric based on the unique crypto-ID, no access is granted.
			High	
			Enforce account usage restrictions for specific time periods and locality. Monitor manufacturing system usage for atypical use. Disable accounts of users posing a significant risk. Specific restrictions can include, for example, restricting usage to certain days of the week, time of day, or specific durations of time. Privileged user access through non-local connections to the manufacturing system is restricted and managed.	Using the RESTful API, organizations can programmatically configure time-based access. Instant revocation of unauthorized machines make it simple to manage restricted user access.
		PR.AC-5	Low	
			Protect network integrity of the manufacturing system, incorporating network segregation where appropriate. Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries within the manufacturing system. Employ boundary protection devices. Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.	IDN moves the security boundary from the perimeter down to the individual device, thereby reducing the need for boundary protection devices. With verifiable isolation and segmentation of network segments, organizations can control all authorized connections and trusted communications.

PROTECT	Access Control (PR.AC)	PR.AC-5	Moderate	
			Limit external connections to the manufacturing system. Monitor and use managed interfaces to conduct external system connections. Deny by default connections to the managed interface. Disable split tunneling and covert channel options in conjunction with remote devices. Ensure the manufacturing system fails securely in the event of the operational failure of a boundary protection device.	Tempered Networks security model is deny-by-default, where no unauthorized (or external) systems or devices can participate within the IDN fabric without being whitelisted first using the unique crypto-ID assigned to the devices. IDN also provides automated disaster recovery and failover in the event of a operational failure.
			High	
			Employ, where feasible, authenticated proxy servers for defined communications traffic between the manufacturing system and external networks. Isolate manufacturing system components performing different missions.	Any authorized and whitelisted device(s) have secure connectivity to other trusted device(s), no matter where in the world they are connecting from (external networks). With hardened segmentation of network segments, it's now easy to isolate manufacturing systems.
	Awareness and Training (PR.AT)	PR.AT-1	Low	
			Provide security awareness training for all manufacturing system users and managers. Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, responding to suspected cybersecurity incidents, and awareness of operational security.	Not Applicable - Process Requirement
			Moderate and High	
			Incorporate insider threat recognition and reporting into security awareness training.	Not Applicable - Process Requirement
		PR.AT-2	Low, Moderate and High	
			Ensure that users with privileged access to the manufacturing system understand the requirements and responsibilities of their assignments. Establish standards for measuring, building, and validating individual qualifications for privileged users.	Not Applicable - Process Requirement

PROTECT	Awareness and Training (PR.AT)	PR.AT-3	Low	
			Establish and enforce security requirements for third-party providers and users. Ensure that third- party providers understand their responsibilities regarding the security of the manufacturing system and the responsibilities of their assignments. Require notifications be given for any personnel transfers, termination, or transition involving personnel with physical or logical access to the manufacturing system components. Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.	While this requirement is designed for updated record keeping and not directly applicable to Tempered Network's enforcement function, managing third-party access is easy with IDN by building individual network segments for each third-party provider and user.
			Moderate and High	
			Require external service providers to identify the functions, ports, protocols, and services necessary for the connection services.	Not Applicable - Process Requirement
		PR.AT-4	Low, Moderate and High	
			Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them.	Not Applicable - Process Requirement
		PR.AT-5	Low, Moderate and High	
			Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility are trained for, and understand their responsibilities. Establish standards for measuring, building, and validating individual qualifications for physical security personnel.	Not Applicable - Process Requirement

PROTECT	Data Security (PR.DS)	PR.DS-1	Low	
			None	Not Available
			Moderate and High	
			Protect while at rest manufacturing system information determined to be critical.	Tempered Networks transforms vulnerable IP-enabled devices into hardened, invisible assets. Cloaked endpoints and networks have no visible TCP/IP footprint and are invisible to the underlying network and any untrusted devices or systems, which protects against DDOS, MiTM attacks, IP spoofing and other types of network and transport layer attacks.
		PR.DS-2	Low	
			None	Not Available
			Moderate and High	
			Protect manufacturing system information when in transit. Implement cryptographic mechanisms where determined necessary to prevent unauthorized access, distortion, or modification of system data and audit records.	Tempered Networks delivers built-in security with peer-to-peer AES 256 encryption between whitelisted devices based on their unique crypto-IDs.
		PR.DS-3	Low	
			Enforce accountability for all manufacturing system components throughout the system lifecycle, including removal, transfers, and disposition. Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items.	Not Applicable - Process Requirement

PROTECT	Data Security (PR.DS)	PR.DS-3	Moderate	
			Update the inventory of manufacturing system components as an integral part of component installations, removals, and system updates.	Not Applicable - Process Requirement
			High	
			Employ automated mechanisms where safe and feasible to maintain an up-to-date, complete, accurate, and readily available inventory of manufacturing system components. Ensure that disposal actions are approved, tracked, documented, and verified.	Not Applicable - Process Requirement
		PR.DS-4	Low, Moderate and High	
			Ensure that adequate resources are maintained for manufacturing system information processing, networking, telecommunications, and data storage. Protect the manufacturing system against, or limit the effects of, denial of service attacks. Off-load audit records from the manufacturing system for processing to an alternate system.	IDN is resistant against DDOS, MiTM attacks, IP spoofing and other types of network and transport layer attacks. Audit records can be exported in either CSV or JSON for simple integration and processing through alternate systems.
		PR.DS-5	Low	
			Protect the manufacturing system against data leaks. Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use. Heighten system monitoring activity whenever there is an indication of increased risk to manufacturing operations and assets. Develop and document access agreements for all users of the manufacturing system.	IDN delivers the highest level of security on the market today, with micro-segmentation down to the individual device(s). By moving the security boundary from the perimeter down to individual devices, and whitelisting authorized access based on crypto-IDs, no unauthorized access can occur.
			Moderate and High	
			Regulate the information flow within the manufacturing system and to outside systems. Enforce controls restricting connections to only authorized interfaces. Protect the system from information leakage due to electromagnetic signals emanations.	No unauthorized (or external) systems or device can participate within the IDN fabric without being whitelisted first using the unique crypto-ID assigned to the device(s).

PROTECT	Data Security (PR.DS)	PR.DS-6	Low	
			None	Not Available
			Moderate	
			Employ software, firmware, and information integrity checks to detect unauthorized changes to manufacturing system components during storage, transport, startup and when determined necessary. Incorporate the detection of unauthorized changes to the manufacturing system into the system's incident response capability.	While this requirement is not directly applicable to Tempered Networks, unauthorized machines cannot access the IDN fabric and therefore cannot make any changes to manufacturing systems.
			High	
			Employ automated tools where feasible to provide notification upon discovering discrepancies during integrity verification. Employ automatic response capability with pre-defined security safeguards when integrity violations are discovered.	Tempered Networks does not provide automated monitoring. However, integrating IDN with other third-party monitoring tools using the RESTful API allows organizations to build event-based logic for real-time network automation and changes.
		PR.DS-7	Low, Moderate and High	
			Utilize an off-line development and testing system for implementing and testing changes to the manufacturing system.	IDN allows organizations to create separate development/ test environments with simple network creation in seconds.
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1	Low	
			Develop, document, and maintain a baseline configuration for the manufacturing system. Baseline configurations include for example, information about manufacturing system components (e.g. software license information, software version numbers, HMI and other ICS component applications, software, operating systems), current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Configure the manufacturing system to provide only essential capabilities. Review the baseline configuration and disable unnecessary capabilities.	Tempered Networks does not provide in-depth asset management. However, IDN can provide a verifiable topology map of trusted connections between manufacturing systems through the Visual Trust Map.

PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-1	Moderate	
			Review and update the baseline configuration of the manufacturing system as an integral part of system component installations and upgrades. Retain previous versions of the baseline configuration to support rollback. Employ software program usage restrictions. Develop a configuration management plan for the manufacturing system. The plan includes, for example, configuration processes, roles, lifecycle definition, configuration items, and control methods. Define configuration parameters, capabilities, and fail-to-known-state procedures such that, upon a system failure (or failure conditions), assets revert to a state that achieves a predetermined mode of operation. Employ a deny-all, permit-by-exception policy to allow the execution of only authorized software programs.	Tempered Networks security model is by default deny-all, only allowing whitelisted devices to communicate.
			High	
			Employ automated mechanisms where feasible to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the manufacturing system. Automated system support includes for example, documentation, notification, and management of the change control process on the manufacturing system. Review system changes to determine whether unauthorized changes have occurred.	Not Applicable - Process Requirement. However, no unauthorized changes can occur as you need whitelisted access to the network segment in order to make changes.
		PR.IP-2	Low	
			Manage the manufacturing system using a system development life cycle that includes security considerations. Include security requirements into the acquisition process of the manufacturing system and its components.	Not Applicable - Process Requirement

PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-2	Moderate and High	
			Require the developer of the manufacturing system and system components to provide a description of the functional properties of security controls, and design and implementation information for security-relevant system interfaces. Apply security engineering principles into the specification, design, development, implementation, and modification of the manufacturing system. Employ configuration management and change control during the development of the manufacturing system and its components, and include flaw tracking and resolution, and security testing.	Not Applicable - Process Requirement
		PR.IP-3	Low	
			Employ configuration change control for the manufacturing system and its components. Conduct security impact analyses in connection with change control reviews.	Not Applicable - Process Requirement
			Moderate	
			Test, validate, and document changes to the manufacturing system before implementing the changes on the operational system. Review and authorize proposed configuration-controlled changes prior to implementing them on the manufacturing system.	Not Applicable - Process Requirement
			High	
			Employ automated mechanisms where feasible to support the change control process. Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to the manufacturing system.	Not Applicable - Process Requirement. However, IDN enables organizations to build separate test environments that are segregated from production environments.

PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-4	Low	
			Conduct and maintain backups for manufacturing system data. Manufacturing system data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, operational control limits, control bands and set points for pre-incident operation for all ICS programmable equipment	Not Applicable - Process Requirement
			Moderate	
			Verify the reliability and integrity of backups. Coordinate backup testing with organizational elements responsible for related plans. Establish a separate alternate storage site for system backups and ensure the same security safeguards are employed.	Not Applicable - Process Requirement. However, Tempered Networks enables organizations to easily create separate network segments for test and production environments that can be used for backup testing. In addition, high availability pairing is also available for the Conductor.
			High	
			Include into contingency plan testing the conducting of restorations from backup data. Store critical manufacturing system backup information separately.	Not Applicable - Process Requirement. However, Tempered Networks enables organizations to increase security for the backup systems by easily segmenting those systems from the rest of the network.
		PR.IP-5	Low and Moderate	
			Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls for the manufacturing system. Fire suppression mechanisms should take the manufacturing environment into account (e.g., water sprinkler systems could be hazardous in specific environments).	Not Applicable - Process Requirement. However, IDN enables organizations to securely connect and segment emergency and safety systems, fire protection systems, and environment controls across the network.
			High	
			Employ fire detection devices that activate and notify key personnel automatically in the event of a fire.	Not Available
		PR.IP-6	Low and Moderate	
			Ensure that manufacturing system data is destroyed according to policy.	Not Applicable - Process Requirement

PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-6	High	
			Ensure that media sanitization actions are approved, tracked, documented, and verified. Test sanitation equipment and procedures. Apply nondestructive sanitization techniques to portable storage devices connecting to the manufacturing system.	Not Applicable - Process Requirement
		PR.IP-7	Low	
			Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions. Ensure that the security plan for the manufacturing system facilitates the review, testing, and continual improvement of the security protection processes.	Not Applicable - Process Requirement
			Moderate and High	
			Employ independent teams to assess the protection process. Independent teams, for example, may include internal or external impartial personnel. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the manufacturing system under assessment or to the determination of security control effectiveness.	Not Applicable - Process Requirement
		PR.IP-8	Low, Moderate and High	
			Collaborate and share information about manufacturing system related security incidents and mitigation measures with designated sharing partners. Employ automated mechanisms where feasible to assist in information collaboration. Manufacturing systems are often connected to business systems or interconnected. Any single system can be an attack vector for all systems. It is therefore necessary to provide a uniform defense encompassing all baselines.	Not Applicable - Process Requirement. However, IDN delivers verifiable and absolute segmentation of manufacturing systems from the rest of the network, thereby reducing the attack surface and eliminating the possibility of lateral movement across the network.

PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-9	Low	
			Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as providing a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information. Address maintaining essential functions despite system disruption, and the eventual restoration of the manufacturing system. Define incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.	Not Applicable - Process Requirement
			Moderate and High	
			Coordinate contingency plan development with stakeholders responsible for related plans.	Not Applicable - Process Requirement
		PR.IP-10	Low	
			Test response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans.	Not Applicable - Process Requirement. However, with simple creation of test environments and automated disaster recovery, Tempered Networks can assist with this process.
			Moderate and High	
			Coordinate testing of response and recovery plans with relevant stakeholders. Related plans include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.	Not Applicable - Process Requirement
		PR.IP-11	Low, Moderate and High	
			Develop and maintain a personnel security program for the manufacturing system. Personnel security program should include policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions.	Not Applicable - Process Requirement

PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-12	Low	
			Establish and maintain a process that allows continuous review of vulnerabilities, and defines strategies to mitigate them.	Not Applicable - Process Requirement
			Moderate	
			Restrict access to privileged vulnerability data.	Not Applicable - Process Requirement
			High	
			Identify where manufacturing system vulnerabilities may be exposed to adversaries.	Not Applicable - Process Requirement
	Maintenance (PR.MA)	PR.MA-1	Low	
			Schedule, perform, document and review records of maintenance and repairs on manufacturing system components. Establish a process for maintenance personnel authorization, and escort non-authorized maintenance personnel. Verify impacted security controls following maintenance or repairs.	Not Applicable - Process Requirement
			Moderate	
			Enforce approval requirements, control, and monitoring of maintenance tools for use on the manufacturing system. Maintenance tools can include, for example, hardware/software diagnostic test equipment, hardware/software packet sniffers and laptops. Perform preventative maintenance at defined intervals. Inspect maintenance tools brought into the facility. Scan maintenance tools and portable storage devices for malicious code before they are used on the manufacturing system.	Not Applicable - Process Requirement
			High	
			Employ automated mechanisms where feasible to schedule, conduct, and document maintenance and repairs; and to produce records of maintenance activity. Prevent the unauthorized removal of maintenance equipment containing manufacturing system information.	Not Applicable - Process Requirement

PROTECT	Maintenance (PR.MA)	PR.MA-2	Low and Moderate	
			Enforce approval requirements, control, and monitoring, of remote maintenance activities. Employ strong authenticators, record keeping, and session termination for remote maintenance.	Not Applicable - Process Requirement. However, IDN delivers a simple solution for remote access to any system or device on the network, from anywhere in the world, with the ability to instantly revoke access after the work is done.
			High	
			Require that diagnostic services pertaining to remote maintenance be performed from a system that implements a security capability comparable to the capability implemented on the manufacturing system.	Not Applicable - Process Requirement
	Protective Technology (PR.PT)	PR.PT-1	Low	
			Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or manufacturing components associated with the event. Ensure that audit processing failures on the manufacturing system generate alerts and trigger defined responses. Generate time stamps from an internal system clock that is mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	Tempered Networks delivers user activity logs pertaining to all events, with UTC timestamp.
			Moderate	
			Review and update audit events. Employ automated mechanisms to integrate audit review, analysis, and reporting. Compare and synchronize the internal system clocks to an authoritative time source. Authoritative time sources include for example, an internal NTP server, radio clock, atomic clock, GPS time source.	Not Applicable - Process Requirement
			High	
			Integrate analysis of audit records with physical access monitoring. Conduct time correlation of audit records. Enable authorized individuals to extend audit capabilities when required by events.	Not Applicable - Process Requirement

PROTECT	Protective Technology (PR.PT)	PR.PT-2	Low	
			Employ technical safeguards to restrict the use of portable storage devices.	Not Applicable - Process Requirement.
			Moderate and High	
			Protect and control portable storage devices containing manufacturing system data while in transit and in storage. Scan all portable storage devices for malicious code before they are used on the manufacturing system	Not Applicable - Process Requirement
		PR.PT-3	Low	
			Employ technical safeguards to control access to the manufacturing system and assets.	No unauthorized device can participate within the IDN fabric and access the manufacturing systems without being whitelisted first using the unique crypto-ID assigned to the device(s).
			Moderate and High	
			Disable defined functions, ports, protocols, and services within the manufacturing system deemed to be unnecessary. Employ technical safeguards to enforce a deny-all, permit-by-exception policy to only allow the execution of authorized software programs.	Not Applicable - Process Requirement. However, Tempered Networks security model is by default deny-all, only allowing whitelisted devices to communicate.
		PR.PT-4	Low	
			Monitor and control communications at the external boundary and at key internal boundaries within the manufacturing system.	The concept of external and internal boundaries change with IDN. By moving the security perimeter down to the individual device, with micro-segmentation across any network, IDN introduces a perimeter of one that is much more secure than other endpoint and segmentation technologies.

PROTECT	Protective Technology (PR.PT)	PR.PT-4	Moderate and High	
			Control the flow of information within the manufacturing system and between interconnected systems. Information flow may be supported, for example, by labeling or coloring physical connectors as an aid to manual hookup. Inspection of message content may enforce information flow policy. For example, a message containing a command to an actuator may not be permitted to flow between the control network and any other network. Physical addresses (e.g., a serial port) may be implicitly or explicitly associated with labels or attributes (e.g., hardware I/O address). Manual methods are typically static. Label or attribute policy mechanisms may be implemented in hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers. Limit external connections to the system. Manage the interface for external telecommunication services by establishing a traffic flow policy, protecting the confidentiality and integrity of the information being transmitted, reviewing and documenting each exception to the traffic flow policy.	The flow of information within the manufacturing system and between interconnected systems is based on simple segmentation and whitelisting of devices that are allowed to communicate through their unique cryptographic identities. This enables organizations to have absolute control over network traffic flow with verifiable isolation of individual systems.
DETECT	Anomalies and Events (DE.AE)	DE.AE-1	Low, Moderate and High	
			Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	Not Applicable - Process Requirement
		DE.AE-2	Low	
			Review and analyze detected events within the manufacturing system to understand attack targets and methods.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms where feasible to review and analyze detected events within the manufacturing system.	Not Applicable - Other Technology

DETECT	Anomalies and Events (DE.AE)	DE.AE-3	Low and Moderate	
			Ensure that event data is compiled and correlated across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/ administrator reports.	Not Applicable - Process Requirement
			High	
			Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; manufacturing system monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.	Not Applicable - Process Requirement
		DE.AE-4	Low	
			Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.	Not Applicable - Process Requirement
			Moderate	
			Employ automated mechanisms to support impact analysis.	Not Applicable - Process Requirement
			High	
			Correlate detected event information and responses to achieve perspective on event impact across the organization.	Not Applicable - Process Requirement
		DE.AE-5	Low	
			Define incident alert thresholds for the manufacturing system.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms where feasible to assist in the identification of security alert thresholds.	Not Applicable - Process Requirement

DETECT	Security Continuous Monitoring (DE.CM)	DE.CM-1	Low	
			Conduct ongoing security status monitoring of the manufacturing system network to detect attacks and indicators of potential attacks. Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system. Generate audit records for defined cybersecurity events. Monitor network communications at the external boundary of the system and at key internal boundaries within the system. Heighten system monitoring activity whenever there is an indication of increased risk.	No unauthorized device can participate within the IDN fabric and access the manufacturing systems without being whitelisted first using the unique crypto-ID assigned to the device(s). Tempered Networks transforms vulnerable IP-enabled devices into hardened, invisible assets. Cloaked endpoints and networks have no visible TCP/IP footprint and are invisible to the underlying network and any untrusted devices or systems.
			Moderate	
			Employ automated mechanisms to support detection of cybersecurity events. Generate system alerts when indications of compromise or potential compromise occur.	Not Applicable - Other Technology. However, using the RESTful API, organizations can integrate the IDN solution with other third-party monitoring tools (e.g. SIEMs, IPS/IDS) for real-time network changes based on events detected by these systems.
			High	
			Monitor for and report atypical usage of the manufacturing system.	Not Applicable - Other Technology
		DE.CM-2	Low	
			Conduct ongoing security status monitoring of the manufacturing system facility to detect physical security incidents.	Not Applicable - Other Technology
			Moderate and High	
			Employ independent teams to monitor the security of the physical environment. Monitor physical intrusion alarms and surveillance equipment. Monitor physical access to the manufacturing system and devices in addition to the facility.	Not Applicable - Other Technology. However, Tempered Networks can securely connect and segment the intrusion alarms and surveillance equipment from the rest of the network, enabling organizations to centrally manage those controls from anywhere in the world.

DETECT	Security Continuous Monitoring (DE.CM)	DE.CM-3	Low, Moderate and High	
			Conduct security status monitoring of personnel activity associated with the manufacturing system. Enforce software usage and installation restrictions.	Not Applicable - Process Requirement
		DE.CM-4	Low	
			Deploy malicious code protection mechanisms throughout the manufacturing system where safe and feasible to detect and eradicate malicious code. Update malicious code protection mechanisms whenever new releases are available in accordance with the configuration management policy and procedures for the manufacturing system. Manage for false positives during malicious code detection and eradication.	Not Applicable - Other Technology. However, IDN was designed to significantly reduce the total available attack surface and eliminate the possibility of lateral movement by malware through hardened segregration of networked systems and devices.
			Moderate and High	
			Automatically update malicious code protection mechanisms where safe and feasible.	Not Applicable - Other Technology
		DE.CM-5	Low	
			None	Not Available
			Moderate and High	
			Define acceptable and detect unacceptable mobile code and mobile code technologies. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript. Enforce usage restrictions and establish implementation guidance for acceptable mobile code and mobile code technologies for use with the manufacturing system. The use of mobile code technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the manufacturing system.	Not Applicable - Process Requirement

DETECT	Security Continuous Monitoring (DE.CM)	DE.CM-6	Low Moderate and High	
			Conduct ongoing security status monitoring of external service provider activity on the manufacturing system. Detect attacks and indicators of potential attacks from external service providers. Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.	Tempered Networks does not provide any detection capabilities. However, with secure remote access from anywhere in the world that is segmented down to the individual device, granting or revoking device access for external service providers is simple and fast.
		DE.CM-7	Low	
			Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software. Monitor for system inventory discrepancies. Deploy monitoring devices strategically within the manufacturing system to collect essential information to detect specific events of interest.	Tempered Networks does not provide any detection capabilities. However, no unauthorized device(s) can participate within the IDN fabric without first being whitelisted based on their unique cryptographic identities.
			Moderate and High	
			Monitor for unauthorized configuration changes to the manufacturing system.	Not Applicable - Other Technology
		DE.CM-8	Low, Moderate and High	
			Conduct vulnerability scans on the manufacturing system where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process. Employ control system-specific vulnerability scanning tools and techniques where safe and feasible. Active vulnerability scanning, which introduces network traffic, is used with care on manufacturing systems to ensure that system functions are not adversely impacted by the scanning process.	Not Applicable - Other Technology
	Detection Processes (DE.DP)	DE.DP-1	Low, Moderate and High	
			Define roles and responsibilities for detection activities on the manufacturing system and ensure accountability.	Not Applicable - Process Requirement

DETECT	Detection Processes (DE.DP)	DE.DP-2	Low, Moderate and High	
			Conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements.	Not Applicable - Process Requirement
		DE.DP-3	Low, Moderate and High	
			Validate that event detection processes are operating as intended.	Not Applicable - Process Requirement
		DE.DP-4	Low	
			Communicate event detection information to defined personnel. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of VoIP, and malware disclosure.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms and system generated alerts to support event detection communication.	Not Applicable - Process Requirement
		DE.DP-5	Low	
			Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions. Ensure the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security detection processes.	Not Applicable - Process Requirement
			Moderate	
			Employ independent teams to assess the detection process.	Not Applicable - Process Requirement
			High	
			Conduct specialized assessments including in-depth monitoring, vulnerability scanning, malicious user testing, insider threat assessment, performance/load testing, and verification and validation testing on the manufacturing system.	Not Applicable - Process Requirement

RESPOND	Response Planning (RS.RP)	RS.RP-1	Low, Moderate and High	
			Execute the response plan during or after a cybersecurity event on the manufacturing system.	Not Applicable - Process Requirement
	Communications (RS.CO)	RS.CO-1	Low, Moderate and High	
			Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response.	Not Applicable - Process Requirement
		RS.CO-2	Low	
			Employ prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system. Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms to assist in the reporting of cybersecurity events.	Not Applicable - Process Requirement
		RS.CO-3	Low, Moderate and High	
			Share cybersecurity incident information with relevant stakeholders per the response plan.	Not Applicable - Process Requirement
		RS.CO-4	Low	
			Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include for example, mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms to support stakeholder coordination.	Not Applicable - Process Requirement

RESPOND	Communica-tions (RS.CO)	RS.CO-5	Low, Moderate and High	
			Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness. For example, the DHS National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related cybersecurity incidents and mitigation measures.	Not Applicable - Process Requirement
	Analysis (RS.AN)	RS.AN-1	Low	
			Investigate cybersecurity-related notifications generated from detection systems.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms to assist in the investigation and analysis of cybersecurity-related notifications.	Not Applicable - Process Requirement
		RS.AN-2	Low	
			Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.	Not Applicable - Process Requirement
			Moderate and High	
			Employ automated mechanisms to support incident impact analysis.	Not Applicable - Process Requirement
		RS.AN-3	Low	
			Conduct forensic analysis on collected cybersecurity event information to determine root cause.	Not Applicable - Process Requirement
			Moderate and High	
			Provide on-demand audit review, analysis, and reporting for after-the-fact investigations of cybersecurity incidents.	Not Applicable - Process Requirement

RESPOND	Analysis (RS.AN)	RS.AN-4	Low, Moderate and High	
			Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.	Not Applicable - Process Requirement
	Mitigation (RS.MI)	RS.MI-1	Low, Moderate and High	
			Contain cybersecurity incidents to minimize impact on the manufacturing system.	With hardened segregration of manufacturing systems and other networked systems and devices, lateral movement of malware is eliminated. Cybersecurity incidents are contained to a specific overlay, without the ability to propogate throughout the network.
		RS.MI-2	Low	
			Mitigate cybersecurity incidents occurring on the manufacturing system.	With instant revocation that is point-and-click simple, organizations can immediately disconnect systems and devices from the rest of the manufacturing systems.
			Moderate and High	
			Employ automated mechanisms to support the cybersecurity incident mitigation process.	Tempered Networks enables organizations to revoke the infected systems immediately, either manually or automated through the RESTful API. This significantly reduces the impact of an attack, as well as ensures the availability and integrity of manufacturing systems.
		RS.MI-3	Low, Moderate and High	
			Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.	Not Applicable - Process Requirement
	Improvements (RS.IM)	RS.IM-1	Low, Moderate and High	
			Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	Not Applicable - Process Requirement

RESPOND	Improvements (RS.IM)	RS.IM-2	Low, Moderate and High	
			Update the response plans to address changes to the organization, manufacturing system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. Updates may include, for example, responses to disruptions or failures, and predetermined procedures. Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.	Not Applicable - Process Requirement
RECOVER	Recovery Planning (RC.RP)	RC.RP-1	Low and Moderate	
			Execute the recovery plan during or after a cybersecurity incident on the manufacturing system. Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.	Not Applicable - Process Requirement.
			High	
			Continue essential manufacturing functions and services with little or no loss of operational continuity, and sustain continuity until full system restoration.	Not Applicable - Process Requirement. However, Tempered Networks can create redundancies with automated disaster recovery and failover between primary and secondary systems (on-premise or in the cloud). With point-and-click simple network creation, organizations can recover operations easily, while maintaning system availability and integrity.
	Improvements (RC.IM)	RC.IM-1	Low, Moderate and High	
			Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly.	Not Applicable - Process Requirement

RECOVER	Improvements (RC.IM)	RC.IM-2	Low, Moderate and High	
			Update the recovery plan to address changes to the organization, manufacturing system, or environment of operation and problems encountered during plan implementation, execution, or testing. Ensure that updates are integrated into the recovery plans.	Not Applicable - Process Requirement
	Communica-tions (RC.CO)	RC.CO-1	Low	
			Centralize and coordinate information distribution, and manage the public facing representation of the organization. Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies.	Not Applicable - Process Requirement
			Moderate	
			Assign a Public Relations Officer.	Not Applicable - Process Requirement
			High	
			Pre-establish media contacts. Utilize external assets to manage public relations.	Not Applicable - Process Requirement
		RC.CO-2	Low, Moderate and High	
			Employ a crisis response strategy to protect against negative impact and repair organizational reputation. Crisis response strategies include, for example, actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.	Not Applicable - Process Requirement
		RC.CO-3	Low, Moderate and High	
			Communicate recovery activities to all relevant stakeholders, and executive and management teams.	Not Applicable - Process Requirement