6. Applying the Cybersecurity Framework to OT

Many public and private-sector organizations have adopted the NIST Cybersecurity Framework (CSF) [CSF] to guide cybersecurity activities and consider cybersecurity risks. The Framework consists of five concurrent and continuous Functions – Identify, Protect, Detect, Respond, and Recover – for presenting industry standards, guidelines, and practices in a manner that allows for the communication of cybersecurity activities and outcomes across the organization. When considered together, these Functions provide a high-level, strategic view for cybersecurity risk management. The Framework further identifies underlying key Categories and Subcategories for each Function and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory.

The five Functions include 23 Categories of cybersecurity outcomes and Subcategories that further divide the Categories into more specific technical or management activities. For this section, each subsection references a CSF Function and Category and includes the CSF two-letter abbreviations for reference.

The CSF Functions guide the following actions:

Identify (ID) – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Protect (PR) – Develop and implement appropriate safeguards to ensure delivery of critical services.

Detect (DE) – Develop and implement appropriate activities to identify the occurrence of the cybersecurity event.

Respond (RS) – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Recover (RC) – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

This section discusses all CSF Functions and selected CSF Categories and Subcategories. Additionally, some Categories include additional OT-specific considerations that are not included in the CSF.

6.1. Identify (ID)

The Identify Function provides foundational activities to effectively use the CSF. The intended outcome of the Identify Function is to develop an organizational understanding to manage cybersecurity risks to systems, people, assets, data, and capabilities.

6.1.1. Asset Management (ID.AM)

The ability for organizations to properly and consistently identify and manage data, personnel, devices, systems, and facilities based on their relative importance provides a foundational capability to support an organizational cybersecurity program. Additionally, updating inventory information when components are added, removed, or changed (e.g., patched, new firmware installed, component swapped during maintenance) helps organizations accurately manage their overall environmental risks. Organizations should consider including the following to support their asset management capability:

- Unique identifiers to differentiate and track assets
- Hardware inventory management to track computing and network devices within the environment, including device details and location. Device details may include vendor, model, serial number, purchase information, and manufacturing/build information (e.g., provenance information).
- Software and firmware inventory management to track the software and firmware installed with the OT components, including version numbers, location information, and software bill of materials (SBOM)
- Vendor information to establish a repository of vendor information, points of contact, warranty information, locations of recall, and update information
- Documented roles and responsibilities to identify specific individuals, teams, or organization groups who represent the asset owner and those with operation, maintenance, and cybersecurity roles and responsibilities

Supplemental guidance for ID.AM can be found in the following documents:

- NIST SP 1800-5, *IT Asset Management*
- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*

OT-Specific Recommendations and Guidance

Organizations should consider the criticality of a complete and accurate asset inventory for managing risk within the OT environment. Accurate inventory information supports multiple risk management objectives, including risk assessment, vulnerability management, and obsolescence tracking.

While automated tools for supporting asset management are generally preferable, organizations should consider how the tool collects information and whether the collection method (e.g., active scanning) may have a negative impact on their OT systems. Performing a test using the automated asset management tools on offline systems or components is recommended prior to deployment within the OT production environment. When automated tools are not feasible due to network architectures or other OT environment issues, the organization should consider manual processes for maintaining a current inventory.

6.1.1.1. Mapping Data Flows (ID.AM-3)

Data flow diagrams help a manufacturer understand the flow of data between networked components. Documenting data flows enables organizations to understand the expected behavior of their networks. This understanding of how devices communicate assists with troubleshooting as well as response and recovery activities. This information can be leveraged during forensic activities or used for analysis to identify anomalies.

OT-Specific Recommendations and Guidance

Organizations should consider the impact of the use of automated data flow mapping tools that use active scanning or require network monitoring tools (e.g., in-line network probes) on OT systems. Impacts could be due to the nature of the information, the volume of network traffic, or the momentary disconnection of manufacturing system components from the network. Consider using data flow mapping tools that utilize these methods during planned downtime.

6.1.1.2. Network Architecture Documentation (Supports the Outcome of ID.AM)

Network architecture documentation tools help a manufacturer identify, document, and diagram the interconnections between networked devices, corporate networks, and other external connections. A comprehensive understanding of the interconnections within the environment is critical for the successful deployment of cybersecurity controls. This information is equally important for effective network monitoring.

OT-Specific Recommendations and Guidance

Network architecture documentation tools that use automated topology discovery technologies can only capture details from IP-based networked devices. Many OT environments contain isolated systems, components, or systems connected on non-IP networks. The OT environment may not be technically capable of using automated network architecture documentation tools, and manual processes may be required to document these components.

Asset owners may also want to consider how automated scanning activities may potentially impact the OT system by testing automation tools in a non-production environment. Based on testing results, asset owners should consider utilizing automated OT network architecture documentation tools during planned downtime.

Organizations may also want to consider physically inspecting OT network connections or analyzing network logs to document the OT network architecture, especially if the network is not large or complicated. Incorporating OT network activity monitoring may help organizations identify the addition or removal of devices within the environment between planned scanning activities.

6.1.2. Governance (ID.GV)

Effective governance involves organizational leadership incorporating risk management objectives into the strategic planning process along with resiliency, privacy, and cybersecurity objectives, as well as providing the required resources to effectively implement and sustain the cybersecurity program. From this process, organizational leadership develops and disseminates policies that establish security requirements for their environments. These policies may include the identification and assignment of roles, responsibilities, management commitment, and compliance. The policies may also reflect coordination among the organizational entities responsible for the different aspects of security (e.g., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring).

Sections 3 and 4 provide additional details for governance. Supplemental guidance for ID.GV can be found in the following documents:

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
- NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OT-Specific Recommendations and Guidance

Organizations should consider:

- Ensuring that the cybersecurity program is given sufficient resources to support the organization's IT and OT risk management strategy
- Ensuring that policies take the full life cycle of the OT systems into consideration
- Ensuring that legal and regulatory cybersecurity requirements that affect OT operations are understood and managed
- Establishing one or more senior official positions that are responsible and accountable for the organization's governance and risk management for IT and OT cybersecurity programs
- Establishing communication and coordination between IT and OT organizations
- Cross-training IT and OT personnel to support the cybersecurity program

6.1.3. Risk Assessment (ID.RA)

A cybersecurity risk assessment is performed to identify risks and estimate the magnitude of harm to operations, assets, or individuals that might result from cyber incidents, such as unauthorized access, use, disclosure, disruption, modification, or destruction of an information system or data. Organizations should consider the frequency with which to update risk assessments and test system cybersecurity controls.

Supplemental guidance for ID.RA can be found in the following documents:

- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

OT-Specific Recommendations and Guidance

In OT environments, risks and impacts may be related to safety, health, and the environment, in addition to business and financial impacts. As a result, organizations may find that conducting a cost-benefit analysis for some types of risks is not possible. In these cases, organizations should consider reviewing past cyber and non-cyber incidents that have resulted in the loss of power, control, upstream feed, or downstream capacity, as well as major equipment failures. A PHA, FMEA, or analysis of past events can be used to understand the potential impact of a cyber incident. ISA 62443-3-2 provides guidance on how to assess cyber risk in an environment with these potential consequences.

Risk assessments also require the identification of both vulnerabilities and threats to the OT environment. Maintaining an accurate inventory of the IT and OT assets within the environment of operation – including the product vendor, model numbers, firmware, OSs, and software versions installed on the assets – facilitates the identification, tracking, and remediation of vulnerabilities. OT-specific vulnerability information is available through multiple methods, including:

- Using OT-specific tools to automate asset inventory creation, cross-correlation of the inventory with known vulnerabilities and threats, and regular updates
- Monitoring security groups, associations, and vendors for security alerts and advisories
- Reviewing the NVD database for detailed information on known vulnerabilities for hardware and software assets

Threat information that is relevant to the environment can be obtained from both internal resources and external threat intelligence information-sharing forums. Organizations should consider participating in cyber threat information sharing [SP800-150].

6.1.4. Risk Management Strategy (ID.RM)

The risk management strategy guides how risk is framed, assessed, responded to, and monitored and provides a consistent approach to making risk-based decisions across the organization. Risk tolerance, assumptions, constraints, priorities, and trade-offs are identified for investment and operational decision making. Additionally, the risk management strategy identifies acceptable risk assessment methodologies, potential risk responses, and a process to continuously monitor the security posture (or implementation of security countermeasures and outcomes) of the organization.

Section 3 describes the overall risk management process for supporting an effective cybersecurity program. The following NIST documents provide additional implementation guidance for developing a risk management strategy:

- NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST IR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*

OT-Specific Recommendations and Guidance

When establishing an OT risk management strategy, organizations should consider:

- Ensuring that the risk tolerance of an OT environment is informed by the organization's role in critical infrastructure and sector-specific risk analysis
- Documenting failure scenarios that involve IT components within the OT environment and their effect on operations and safety
- Establishing processes to periodically update information to determine the current risk posture for the environment and coordinate required adjustments to risk management and management controls

Overall risk can also be reduced by addressing likelihood and consequence. For OT systems, the risk management strategy should consider non-security and safety controls (e.g., pressure relief valves, manual valves) that can also help reduce the consequence of a failure.

6.1.5. Supply Chain Risk Management (ID.SC)

Supply chains are multifaceted and built on a variety of business, economic, and technological factors. Organizations choose their suppliers, and consumers choose their sources based on a range of factors that vary from corporate preferences and existing business relationships to more discrete considerations, such as the existence of limited sources of supply or other unique characteristics.

The Subcategories (outcomes) that fall within the CSF Supply Chain Risk Management Category provide the basis for developing processes and procedures for managing supply chain risk. These risks include the insertion of counterfeits, unauthorized production, malicious insiders, tampering, theft, and the insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cyber supply chain. These risks must be identified, assessed, and managed. The CSF Category also addresses supplier and third-party partner contracts, assessments, evaluations, and response and recovery planning.

Additionally, organizations should investigate SBOMs and distributed ledger (e.g., blockchain) technologies to support supply chain risk management. For example, SBOM information can identify software components and their relationships or dependencies on other components. Having this information available can help an organization determine whether a device is affected by reported software vulnerabilities.

Supplemental guidance for Supply Chain Risk Management can be found in the following documents:

- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
- NIST IR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*

OT-Specific Recommendations and Guidance

Organizations should consider documenting and tracking serial numbers, checksums, digital certificates/signatures, or other identifying features that can enable them to verify the authenticity of vendor-provided OT hardware, software, and firmware. Organizations should also consider whether OT is purchased directly from the original equipment manufacturer (OEM) or an authorized third-party distributor or reseller. Suppliers should be assessed or reviewed to ensure that they continue to follow best practices.

Many OT components and devices utilize open-source libraries to support their functional capabilities. Organizations should identify the open-source dependencies for their OT components and establish monitoring for open-source information, such as vendor websites or cyber news sources, to ensure that no known vulnerabilities or counterfeits have been disclosed. Additionally, organizations might consider utilizing an industry-recognized certification process for OT products to support supply chain risk management.

6.2. Protect (PR)

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology

6.2.1. Identity Management and Access Control (PR.AC)

Identity Management and Access Control (PR.AC) identifies outcomes around establishing and managing the identification mechanisms and credentials for users, devices, and services. Identity management supports the cybersecurity principle of positively and uniquely identifying and authorizing a person, process, or device before granting physical or logical access to resources such as the system, information, or location being protected. Access controls represent the policies, processes, and technologies for specifying the use of system resources by only authorized users, programs, processes, or other systems. PR.AC controls allow organizations to manage logical and physical access to support system risk management requirements.

Supplemental guidance for implementing identity management and access control outcomes can be found in the following documents:

- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification*
- NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*

OT-Specific Recommendations and Guidance

Organizations should consider the life cycle for managing OT credentials, including issuance, revocation, and updates across the OT environment.

Organizations should also consider the centralization of identification and authentication for users, devices, and processes within the OT environments to improve account management and monitoring capabilities. Common network technologies – such as Active Directory, Lightweight Directory Access Protocol (LDAP), and similar technologies – can be utilized to support the centralization of identity management across environments. Organizations should weigh the increased risks of authenticated accounts from IT environments having access within the OT environment against the benefits of using centralized accounts.

When OT cannot support authentication or the organization determines that it is not advisable due to adverse impacts on performance, safety, or reliability, the organization should select compensating countermeasures, such as the use of physical security (e.g., control center keycard access for authorized users) to provide an equivalent security capability or level of protection for the OT. This guidance also applies to the use of session lock and session termination in an OT.

A unique challenge in OT is the need for immediate access to an HMI in emergency situations. The time needed to enter a user's credentials may impede response or intervention by the operator, resulting in negative consequences to safety, health, or the environment.

6.2.1.1. Logical Access Controls (PR.AC)

Logical access controls restrict logical access to an organization's systems, data, and networks. ACLs are sometimes used to support logical access controls. An ACL is a list of one or more rules for determining whether an access request should be granted or denied, and it is used to support the principle of least functionality and control access to restricted areas. ACLs are commonly used with isolation technologies, such as firewalls, where an ACL might specify the source, destination, and protocol allowed through the isolation device to or from the protected network segment. ACLs may also be used for physical or logical access to areas or information, such as network file shares, databases, or other data repositories and applications.

Role-based access control (RBAC) also supports logical access controls. RBAC is a technology that has the potential to reduce the complexity and cost of security administration in networks with large numbers of intelligent devices. RBAC is built on the principle that employees change roles and responsibilities more frequently than the duties within those roles and responsibilities. Under RBAC, security administration is simplified using roles, hierarchies, and constraints to organize user access levels.

Additionally, attribute-based access control (ABAC) is an access control approach in which access is determined based on the attributes associated with subjects (requesters) and the objects being accessed. Each object and subject has a set of associated attributes, such as location, time of creation, and access rights. Access to an object is authorized or denied depending on whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and the requesting subject.

For federal employees and contractors, Personal Identity Verification (PIV), used in accordance with FIPS 201, may be required to achieve access control. Organizations may also consider one or more of these techniques when determining how to support local access controls within their environments. Supplemental guidance for access controls can be found in the following documents:

- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification*
- NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*
- NIST SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*
- NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*
- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

OT-Specific Recommendations and Guidance

Organizations should consider the following:

- Some logical access controls, such as RBAC, support the principle of least privilege and the separation of duties by

providing a uniform means to manage access to OT devices while reducing the cost of maintaining individual device access levels and minimizing errors. These logical access controls can also restrict OT user privileges to only those required to perform each person's job (i.e., configuring each role based on the principle of least privilege). The level of access can take several forms, including viewing, using, and altering specific OT data or device functions.

- Solutions that provide credential management, authentication, authorization, and system use monitoring technical capabilities. These technologies may help manage risks associated with OT devices and protocols by providing a secure platform to allow authorized personnel to access the OT devices.
- Access control systems that verify the identity of the individual, process, or device before granting access to minimize latency or delays in processing OT system access or commands.
- Highly reliable systems that do not interfere with the routine or emergency duties of OT personnel. Solutions should be designed to reduce the impact of determining identity and authorization on OT operations and safety.

To support access controls, an organization is not limited to a single access control approach. In some cases, applying different access control techniques to different zones based on criticality, safety, and operational requirements is more efficient and effective. For example, ACLs on network zone firewalls combined with RBAC on engineering workstations and servers and ABAC integrated into physical security to sensitive areas may achieve the risk-based access control requirements of an organization.

6.2.1.2. Physical Access Controls (PR.AC-2)

Physical security controls are physical measures that limit physical access to assets to prevent undesirable effects, including unauthorized physical access to sensitive locations; the unauthorized introduction of new systems, infrastructure, communications interfaces, or removable media; and unauthorized disruption of the physical process. Physical access controls include controls for managing and monitoring physical access, maintaining logs, and handling visitors.

The deployment of physical security controls is often subject to specific environmental, safety, regulatory, legal, and other requirements that must be identified and addressed for a given environment. Physical security controls may be broadly applied or specific to certain assets.

The initial layers of physical access control are often determined based on the risk of access to the overall facility, not just OT components. Some regulations, such as NERC CIP-006-5 (Physical Security of BES Cyber Systems) or from the Nuclear Regulatory Commission (NRC), may also determine the strength and quantity of barriers used for the physical protection of a facility.

OT-Specific Recommendations and Guidance

The physical protection of the cyber components and data associated with OT must be addressed as part of the overall security for OT environments. Security at many OT facilities is closely tied to operational safety. A primary goal is to keep personnel out of hazardous situations without preventing them from doing their jobs or carrying out emergency procedures.

Physical access controls are often applied to the OT environment as compensating controls when legacy systems do not support modern IT logical access controls (e.g., an asset could be locked in a cabinet when the USB port or power button cannot be logically disabled). When implementing these mitigations, organizations should consider whether the OT component being protected can be compromised using a wireless or network connection that might bypass the physical security controls.

A defense-in-depth solution to physical security should consider the following attributes:

- **Protection of physical locations.** Classic physical security considerations typically include an architecture of layered security measures that create several physical barriers around buildings, facilities, rooms, equipment, or other informational assets. Physical security controls should be implemented to protect physical locations and may include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, door and cabinet locks, guards, or other measures.
- **Physical access control.** Equipment cabinets should be locked when not required for operation or safety, and wiring should be neat and contained within cabinets or under floors. Additionally, consider keeping all computing and networking equipment in secured areas. Keys of OT assets, like PLCs and safety systems, should be in the “Run” position at all times unless they are being actively programmed.
- **Access monitoring systems.** Access monitoring systems include electronic surveillance capabilities, such as still and video cameras, sensors, and identification systems (e.g., badge readers, biometric scanners, electronic keypads). Such devices typically do not prevent access to a particular location. Rather, they store and record either the physical presence or the lack of physical presence of individuals, vehicles, animals, or other physical entities. Adequate lighting should be provided based on the type of access monitoring device deployed. These systems can also sometimes alert or initiate action upon the detection of unauthorized access.
- **People and asset tracking.** Locating people and vehicles in a facility can be important for both safety and security reasons.

Asset location technologies can be used to track the movements of people and vehicles to ensure that they stay in authorized areas, to identify personnel who may need assistance, and to support emergency response.

The following are additional physical security considerations:

- **Portable devices.** Organizations should apply a verification process that includes, at a minimum, scanning devices (e.g., laptops, USB storage, etc.) for malicious code prior to allowing the device to connect to OT devices or networks.
- **Cabling.** While unshielded twisted pair communications cables may be acceptable in an office environment, they may not be suitable for some OT environments due to their susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Organizations should consider using alternative cabling or shielding that provides suitable protection against environmental threats. Additionally, organizations should consider color-coded cables, connectors, conduits, and labeling to clearly delineate OT and IT network segments and reduce the risk of potential cross-connections.
- **Control centers and control rooms.** Providing physical security for control centers and control rooms can reduce the potential of many threats, including unauthorized access. Access to these areas should be limited to authorized personnel due to the increased probability of finding sensitive servers, network components, control systems, and consoles that support continuous monitoring and rapid response. Gaining physical access to a control room or OT system components often implies gaining logical access to the system or system components. In extreme cases, organizations may need to consider designing control centers to be blast-proof or provide an off-site emergency control center so that control can be maintained if the primary control center becomes uninhabitable.

6.2.1.3. Network Segmentation and Isolation (PR.AC-5)

As discussed in Section 5, a common architecture for supporting a defense-in-depth cybersecurity approach involves the use of network segmentation or zoning to organize devices by location or function. Network segmentation is typically implemented physically using different network switches or logically using virtual local area network (VLAN) configurations. When properly configured, network segmentation helps enforce security policies and segmented traffic at the Ethernet layer and facilitates network isolation.

For network isolation, organizations typically utilize their mapped data flows to identify required communications between segments. Network isolation devices, such as gateways (including unidirectional gateways or data-diodes) and firewalls, are then configured to enforce these communication restrictions by monitoring all communication traffic and only permitting explicitly authorized communication between segments.

Supplemental guidance for access controls can be found in the following documents:

- NIST SP 800-41, Rev. 1, *Guidelines on Firewalls and Firewall Policy*
- NIST SP 800-207, *Zero Trust Architecture*
- NIST SP 1800-15, *Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*

OT-Specific Recommendations and Guidance

The use of network segmentation and isolation should support an organization's OT cybersecurity defense-in-depth architecture, as described in Section 5.

While VLANs can be a cost-effective solution for OT network segmentation, organizations should consider utilizing physically separate switches for segmenting high-criticality devices, such as those that support safety systems.

When configuring network isolation devices, organizations may find it difficult to determine which network traffic is necessary for proper OT operations. In these situations, organizations might consider temporarily allowing and recording all communication between the network segments. This can provide reviewable logs to identify and document authorized communication for implementing network isolation rules. This activity may also reveal previously unknown or undocumented communication that needs to be reviewed by the organization.

Organizations should also consider whether regulatory requirements stipulate the type of network isolation devices required for OT environments or specific network segments. If organizations choose to utilize firewalls to support network isolation, modern firewalls should be considered, such as stateful and deep packet inspection devices and devices specifically designed to support OT environments. Organizations should enforce a deny-all, permit-by-exception policy where possible and also review the Centre for the Protection of National Infrastructure's

(CPNI) *Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide* to assist with their firewall implementations.

Network isolation devices may not protect against all network-based risks. For example, network isolation does not mitigate risks associated with lateral movement within a network segment, such as the propagation of a worm or other malicious code. Additionally, some IT protocols and many industrial communications protocols have known security vulnerabilities that might be exploitable through network isolation devices. Organizations should consider limiting the flow of insecure protocols, restricting information flow to be unidirectional, and utilizing secure and authenticated protocols for supporting information exchange between the OT environment and other network segments.

6.2.1.4. User, Device, and Asset Authentication (PR.AC-7)

Various authentication methods can be implemented within OT environments, including, but not limited to the methods discussed in this section.

6.2.1.4.1. Physical Token Authentication

Physical token authentication primarily addresses the easy duplication of a secret code or sharing it with others (e.g., a password to a "secure" system being written on the wall next to a PC or operator station). With physical token authentication, the security token cannot be duplicated without special access to equipment and supplies.

A second benefit is that the secret within a physical token can be very large, physically secure, and randomly generated. Because it is embedded in metal or silicon, it does not have the same risks that manually entered passwords do. Traditional passwords can become lost or stolen without notice, leaving credentials more vulnerable to exploitation. If a security token is lost or stolen, the token owner is aware of the missing token and can notify security personnel to disable access.

Common forms of physical or token authentication include:

- Traditional physical locks and keys
- Security cards (e.g., magnetic, smart chip, optical coding)
- Radio frequency devices in the form of cards, key fobs, or mounted tags
- Dongles with secure encryption keys that attach to the USB, serial, or parallel ports of computers
- One-time authentication code generators (e.g., key fobs)

For single-factor authentication with a physical token, the greatest weakness is that physically holding the token means access is granted (e.g., anyone who finds a set of lost keys can now access whatever those keys open). Physical token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used alongside the token.

When token-based access control employs cryptographic verification, the access control system should conform to the requirements of NIST SP 800-78-4 [SP800-78-4].

6.2.1.4.2. Biometric Authentication

Biometric authentication enhances software-only solutions, such as password authentication, by offering an additional authentication factor and removing the need for people to memorize complex secrets. In addition, because biometric characteristics are unique to a given individual, biometric authentication addresses the issues of lost or stolen physical tokens and smart cards. Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases security.

Noted issues with biometric authentication include:

- Distinguishing a real object from a fake one (e.g., distinguishing a real human finger from a silicon rubber cast of one or a real human voice from a recorded one)
- Generating type-I and type-II errors, which is the probability of rejecting a valid biometric image and accepting an invalid biometric image, respectively. Biometric authentication devices should be configured to the lowest crossover between these two probabilities, also known as the crossover error rate.
- Handling environmental factors, such as temperature and humidity, to which some biometric devices are sensitive
- Addressing industrial applications where employees may have to wear safety glasses and/or gloves and industrial chemicals are present
- Retraining biometric scanners that occasionally "drift" over time. Human biometric traits may also shift over time, necessitating periodic scanner retraining.
- Requiring face-to-face technical support and verification for device training, unlike a password that can be given over a phone or an access card that can be handed out by a receptionist
- Denying needed access to the OT system because of a temporary inability of the sensing device to acknowledge a legitimate user
- Being socially acceptable. Users consider some biometric authentication devices more acceptable than others. For example, retinal scans may be considered very low on the scale of acceptability, while thumbprint scanners may be considered high on the scale of acceptability. Users of biometric authentication devices will need to take social acceptability for their target group into consideration when selecting among biometric authentication technologies.

When token-based access control employs biometric verification, the access control system should conform to the requirements of NIST SP 800-76-2 [SP800-76-2].

OT-Specific Recommendations and Guidance

While biometrics can provide a valuable authentication mechanism, organizations may need to carefully assess the technology for use with

industrial applications. Physical and environmental issues within OT environments may decrease the reliability of biometric authorized authentication. Organizations may need to coordinate with system vendors or manufacturers regarding their specific physical and environmental properties and biometric authentication requirements.

6.2.1.4.3. Smart Card Authentication

Smart cards come in a variety of form factors, from USB devices to embedded chips on cards the size of credit cards that can be printed and embossed. Smart cards can be customized, individualized, and issued in-house or outsourced to service providers who manufacture hundreds or thousands per day. Smart cards enhance software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets by:

- Isolating security-critical computations that involve authentication, digital signatures, and key exchange from other parts of the system that do not have a need to know
- Enabling the portability of credentials and other private information between computer systems
- Providing tamper-resistant storage for protecting private keys and other forms of personal information

Most issues regarding the use of smart cards are logistical and focus on issuing cards, particularly replacing lost or stolen cards.

OT-Specific Recommendations and Guidance

Although smart cards offer useful functionality, their implementation in OT must consider the overall security context of the OT environment. The necessary identification of individuals, issuance of cards, revocation if compromise is suspected, and the assignment of authorizations to authenticated identities represents a significant initial and ongoing challenge. In some cases, corporate IT or other resources may be available to assist in the deployment of smart cards and the required public key infrastructures. Organizations should also consider the impact on OT operational capabilities if dependency on IT systems and services are required to support the smart card technology.

Additionally, if smart cards are implemented in an OT setting, organizations should consider provisions for managing lost or damaged cards, the costs to incorporate and sustain a respective access control system, and a management process for card distribution and retrieval. These procedures should consider the ability to grant temporary access to OT personnel to prevent operational or safety disruptions.

A common approach in the Federal Government is based on the standardization on Federal PIV smart cards, which allows organizations to use the same credential mechanism in multiple applications with one to three factors for authentication (i.e., Card-Only, Card+PIN,

Card+PIN+Biometric), depending on the risk level of the protected resource. If the Federal PIV is used as an identification token, the access control system should conform to the requirements of FIPS 201 [FIPS201] and NIST SP 800-73-4 [SP800-73-4] and employ either cryptographic verification or biometric verification.

6.2.1.4.4. Multi-Factor Authentication

There are several possible factors for determining the authenticity of a person, device, or system, including something you know (e.g., PIN number or password), something you have (e.g., key, dongle, smart card), and something you are (i.e., a biological characteristic, such as a fingerprint or retinal signature). When two or more factors are used, the process is known as multi-factor authentication (MFA). In general, the more factors that are used in the authentication process, the more robust the process.

OT-Specific Recommendations and Guidance

Organizations need to consider whether MFA is required for protecting OT environments in whole or in part. MFA is an accepted best practice for remote access to OT applications. When determining the placement and usage of MFA within an OT environment, organizations may need to consider different authentication scenarios since some OT components support only a single factor or no authentication. Organizations may consider adjusting credential requirements based on the type of access or other mitigating factors for the environment. For example, remote access to the OT environment may require MFA, while local access may only require a user ID and password due to other mitigating factors, such as physical access controls before gaining physical access to the area where the user ID and password may be used.

6.2.1.4.5. Password Authentication

While password authentication schemes are arguably the most common and simplest form of authentication, numerous vulnerabilities are associated with the use of and reliance on password-only authentication. For example, systems are often delivered with default passwords that can be easily guessed, discovered, or researched. Another weakness is the ease of third-party eavesdropping. Passwords typed at a keyboard can be visually observed by others or recorded using keystroke loggers.

Some network services and protocols transmit passwords as plaintext (unencrypted), allowing any network capture tool to expose the passwords. Additionally, passwords may be shared and not changed frequently. The use of shared credentials, including shared passwords, limits the ability to positively identify the individual person, process, or device that accessed a protected resource. Defense in depth is often utilized to prevent password authentication from being the only control in place to prevent unauthorized modification.

OT-Specific Recommendations and Guidance

Many OT systems do not offer password recovery mechanisms, so the secure and reliable handling of passwords is critical to maintaining continuous operation. Organizations are encouraged to change the default password on OT equipment to make it more difficult for an adversary to guess the password. Once changed, the password needs to be made available to those who need to know. Organizations may want to consider using a password management tool that is secure and accessible by those who need to know.

Some OT OSs make setting secure passwords difficult if the password size is smaller than current password standards and the system allows only group passwords at each level of access rather than individual passwords. Some industrial (and internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted protocols.

Additionally, special considerations may be required when applying policies based on login password authentication within the OT environment. Without an exclusion list based on machine identification (ID), non-operator login can result in policies such as auto-logoff timeout and administrator password replacement being pushed down, which can be detrimental to the operation of the OT system.

The following are general recommendations and considerations with regard to the use of passwords:

- Change all default passwords in OT components.
- Passwords should have appropriate length, strength, and complexity balanced with security and operational ease of access within the capabilities of the software and underlying OS.
- Passwords should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
- Passwords should be used with care on specialized OT devices, such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out or access is delayed during critical events. Organizations should consider physical or network isolation for devices where password protection is not recommended.
- Copies of shared or administrator passwords must be stored in a secure location with limited access that can also be accessed in an emergency. Organizations may also need to consider procedures to periodically change passwords when a password is

compromised or an individual with access leaves the organization.

- Privileged (administrative) account passwords require additional protection, such as stronger password requirements, more frequent changing, and additional physical safeguards.
- Passwords should not be sent across any network unless they are protected by some form of FIPS-approved encryption or salted cryptographic hash that is specifically designed to prevent replay attacks.

6.2.2. Awareness and Training (PR.AT)

The Awareness and Training category provides policies and procedures for ensuring that all users are given basic cybersecurity awareness and training.

Supplemental guidance can be found in the following documents:

- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
- NIST SP 800-181, Rev. 1, *Workforce Framework for Cybersecurity (NICE Framework)*

OT-Specific Recommendations and Guidance

Personnel should receive security awareness and training for the OT environment and specific applications. In addition, organizations should identify, document, and train all personnel who have significant OT roles and responsibilities. Awareness and training should cover the physical process being controlled as well as the OT system.

Security awareness is a critical part of OT incident prevention, particularly when it comes to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information, such as passwords. This information can then be used to compromise otherwise secure systems.

OT security-specific awareness and training programs could include a basic understanding of social engineering techniques, how to identify anomalous behavior in the OT environment, when and how to connect and disconnect the OT environment from external security domains, password complexity and management requirements, and reporting practices. All personnel with OT responsibilities should be provided with training, which may be tailored based on roles and responsibilities. Roles to consider in the training program could include senior executives, privileged account users, third-party providers, physical security personnel, control engineers, operators, and maintainers.

6.2.3. Data Security (PR.DS)

Providing data security includes protecting the confidentiality, integrity, and availability of data at rest and data in transit, protecting assets after removal, and preventing data leaks.

Cryptography can support data security requirements. Encryption, digital signatures, hashing, and other cryptographic functions are available to prevent unauthorized access or the modification of data at rest and in transit [RFC4949]. When cryptography is selected, organizations should use a certified cryptographic system. Federal organizations are required to comply with FIPS 140-3 [FIPS140-3] and the Cryptographic Module Validation Program (CMVP). Additionally, cryptographic hardware should be protected from physical tampering and uncontrolled electronic connections.

Supplemental guidance for data security can be found in the following documents:

- NIST SP 800-47, Rev. 1, *Managing the Security of Information Exchanges*
- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*
- NIST SP 800-209, *Security Guidelines for Storage Infrastructure*

OT-Specific Recommendations and Guidance

Identify critical physical and electronic file types and data to protect while at rest. This may include personally identifiable information and sensitive, proprietary, or trade secret information (e.g., PLC program code, robot programs, computer-aided drafting [CAD] or computer-aided manufacturing [CAM] files, operating manuals and documentation, electrical diagrams, network diagrams, historical production data [IR8183A]). Organizations should consider centralizing critical data within secure storage locations.

When OT data is stored in the cloud or on vendor servers, organizations should consider performing a risk analysis to determine how the data is protected by the service provider and whether additional countermeasures should be implemented to manage risk to an acceptable level.

Monitor information flows from the OT security domain to other security domains and connections between security domains. Technologies such as data diodes, firewalls, and ACLs can be used to restrict the information flow. Examples of critical interfaces and interconnections may include interfaces between IT and OT, OT and external industry partners, or OT and third-party support vendors.

To protect data on system components at end of life, an asset disposal program should be implemented, including considerations for wiping, sanitizing, or otherwise destroying critical data and media prior to disposal. The asset disposal program should include any removeable media, mobile devices, and traditional OT hardware.

Cryptography

Critical OT data should be protected while in transit, especially over third-party network segments and other untrusted or vulnerable network paths (e.g., cellular, wireless, internet, WAN). Identify critical data, and implement cryptographic mechanisms (e.g., encryption) to prevent unauthorized access or the modification of system data and audit records. Encryption provides a mechanism for ensuring confidentiality and integrity for data in transit.

OT applications often focus on the availability of data. Before deploying encryption in OT, ensure that confidentiality or integrity is the goal of applying the security control. The use of encryption within an OT environment could introduce communications latency due to the additional time and computing resources required to encrypt, decrypt, and authenticate each message. Encryption may also cause performance degradation of the end device or system. Before deploying encryption within an OT environment, solutions should be tested to determine whether latency is acceptable for the application. Encryption at OSI Layer 2 rather than Layer 3 may be implemented to help reduce encryption latency.

Additionally, while encryption provides confidentiality between encryption and decryption devices, anomaly detection tools that support OT environments may be unable to read encrypted data. Encryption should, therefore, be carefully planned and implemented to manage operational risks.

Organizations should also consider that cryptography may introduce key management issues. Sound security policies require key management processes that can become more difficult as the geographic size of the OT increases. Because site visits to change or manage keys can be costly and slow, organizations should consider whether cryptographic protection with remote key management may be beneficial, such as when the protected units become so numerous or geographically dispersed that managing keys is difficult or expensive.

For OT, encryption can be deployed as part of a comprehensive, enforced security policy. A cryptographic key should be long enough so that guessing it or determining it through analysis takes more effort, time, and cost than the value of the protected asset.

6.2.4. Information Protection Processes and Procedures (PR.IP)

Policies, processes, and procedures should be maintained and used to manage the protection of information systems and assets. Countermeasures and outcomes should be in place to manage configuration changes throughout the life cycle of the component and system. Backups should be maintained, and response and recovery plans should be prepared and tested. A plan should be

developed and implemented for vulnerability management throughout the life cycle of the components.

6.2.4.1. Least Functionality (PR.IP-1)

The principle of least functionality involves configuring systems to only provide essential functions and services. Some default functions and services may not be necessary to support essential organizational missions, functions, or operations. These functions include network ports and protocols, software, and services.

Supplemental guidance can be found in the following document:

- NIST SP 800-167, *Guide to Application Whitelisting*

> **OT-Specific Recommendations and Guidance**
>
> Systems and devices in the OT environment include many functions and services that are unnecessary for their proper operation, some of which may be enabled by default and without the organization's knowledge. Any functions or services that are not required for proper operation should be disabled to reduce exposure.
>
> Care should be taken when disabling these functions and services, as unintended impacts may result if a critical function or service is unknowingly disabled (e.g., disabling all external communications to a PLC may also disable the ability to communicate with associated HMIs). Devices should be subjected to extensive testing before being deployed on the OT network.

6.2.4.2. Configuration Change Control (Configuration Management) (PR.IP-3)

Configuration management helps ensure that systems are deployed and maintained in a secure and consistent state to reduce risks from outages due to configuration issues and security breaches through improved visibility and tracking of changes to the system. In addition, configuration management can detect improper configurations before they negatively impact performance, safety, or security. Configuration management tools enable an asset owner to establish and maintain the integrity of system hardware and software components by controlling the processes for initializing, changing, monitoring, and auditing the configurations of the components throughout the system life cycle.

Supplemental guidance for configuration management can be found in the following documents:

- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 1800-5, *IT Asset Management*

> **OT-Specific Recommendations and Guidance**
>
> Organizations should document the approved baseline configuration for their OT devices and establish the system development life cycle

(SDLC) approach to document, test, and approve changes before deploying them to the OT environment.

Some organizations may maintain logbooks or other similar methods to document changes to OT components. Organizations should consider centralizing the tracking and documentation of changes to the OT environment to improve visibility and ensure proper testing and approvals for system changes. Such a process may help organizations to prevent accidental reconfiguration or identify the intentional reconfiguration of components to unapproved or untested versions.

If the use of automated configuration management tools are deemed to be appropriate, processes should be in place to validate configurations prior to deployment. Many changes to OT can be made only during scheduled maintenance downtimes to minimize impacts. When considering automated configuration management tools, organizations should also consider potential impacts to the OT system. In some cases, these tools transfer numerous types and potentially large amounts of data over the manufacturing system network. Additionally, some tools may also have the potential to impact OT system operations by attempting to change device configurations or manipulating active files.

6.2.4.3. Backups (PR.IP-4)

Conducting, maintaining, and testing backups is a critical outcome for the recovery process if a cyber or reliability incident occurs.

Supplemental guidance for determining the priority and strategy for backups can be found in the following documents:

- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-209, *Security Guidelines for Storage Infrastructure*

OT-Specific Recommendations and Guidance

A list of all maintained backups should be developed, including installation media, license keys, and configuration information. Additional measures should be taken to ensure that backups are readily available when needed, such as:

- Verify the backups for reliability and integrity (if technically possible).
- Establish an on-site location for backups that is accessible to all personnel who may need access during a recovery event.
- Establish an alternate secondary storage location for additional copies of backups to ensure that the same incident that disrupts the primary data cannot modify or destroy the backup (e.g., store PLC logic and configuration files at an off-site, geographically

diverse location that cannot be destroyed by the same [hurricane, wildfire, tornado] that may destroy the PLC).

- Test the restoration process from backup data as part of contingency plan testing.
- Ensure that backup procedures are included in configuration or change management processes.
- Secure backups according to access control requirements.
- Monitor environmental conditions where backup media is stored.

6.2.4.4. Physical Operating Environment (PR.IP-5)

Managing the physical operating environment includes emergency protection controls, such as emergency shutdown of the system, backup for power and lighting, controls for temperature and humidity, and protection against fire and water damage. Organizations should develop policies and procedures to ensure that environmental operating requirements for assets are achieved.

OT-Specific Recommendations and Guidance

Organizations should consider the following factors when identifying potential countermeasures to protect the physical operating environment:

- **Environmental factors.** Environmental factors can be important. For example, if a site is dusty, systems should be placed in a filtered environment, especially if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems. In addition, environments that contain systems and media (e.g., backup tapes, floppy disks) should have stable temperature and humidity. An alarm to the OT system should be generated when environmental specifications, such as temperature or humidity, are exceeded.
- **Environmental control systems.** HVAC systems for control rooms must support OT personnel during normal operation and emergency situations, which could include the release of toxic substances. Risk assessments should consider the risk of operating an HVAC system (e.g., air intakes) in an occupied shelter during a toxic release, as well as continued operation during a power outage (e.g., using an uninterruptible power supply in critical environments). Additionally, fire systems must be carefully designed to avoid causing more harm than good (e.g., to avoid mixing water with incompatible products). HVAC and fire systems have significant roles that arise from the interdependence of process control and security. For example, fire prevention and HVAC systems that support industrial control computers need to be protected against cyber incidents.

- **Power.** Reliable power for OT is essential, so a UPS should be provided for critical systems. If the site has an emergency generator, the UPS battery life may only need to last for a few seconds. However, if the site relies on external power, the UPS battery life may need to last for hours. At a minimum, it should be sized so that the system can be shut down safely.

6.2.4.5. Response and Recovery Plans (PR.IP-9) and Response and Recovery Plan Testing (PR.IP-10)

Organizations should develop and maintain response plans, including incident response and business continuity. Response plans should be measured against the service being provided, not just the system that was compromised. Organizations should consider a systematic approach to response planning, such as the process described in CISA's Cybersecurity Incident and Vulnerability Response Playbooks [CISA-CIVR]. Common planning steps include preparation, detection and analysis, containment, recovery, post-incident activity, communication, and coordination. Organizations should also regularly review and update their response plans.

The response plans should be documented in paper form or on an offline system (i.e., air gapped) that cannot be compromised during a cyber attack. Individuals should be trained on where to find the response plan and the actions to take as part of an incident response. Additionally, during the preparation of the incident response plan, input should be obtained from the various stakeholders, including operations, engineering, IT, system support vendors, management, organized labor, legal, and safety. These stakeholders should also review and approve the plan.

Business continuity planning addresses the overall issue of maintaining or reestablishing production in the case of an interruption. An outage can take days, weeks, or months to recover from a natural disaster or minutes or hours to recover from a malware infection or a mechanical or electrical failure. Business continuity plans (BCPs) are often written to cover many types of incidents involving several different disciplines. The BCP for cybersecurity incidents should broadly cover long-term outages, including disaster recovery, and short-term outages that require operational recovery. It is important to work with physical security on developing the BCP related to cybersecurity incidents. This collaboration with physical security should include the identification of critical equipment and the associated countermeasures in place to prevent an incident.

Before creating a BCP to address potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs. There are two distinct types of objectives: system recovery and data recovery. System recovery involves the recovery of communication links and processing capabilities and is usually specified in terms of a recovery time objective (RTO). Management should define the acceptable RTO, and technical personnel should work to achieve that target. Data recovery involves the recovery of data that describes production or product conditions in the past and is usually specified in terms of a recovery point objective (RPO). This is defined as the time for which an absence of data can be tolerated. The RTO and RPO may justify investment in spare inventory if recovery objectives cannot be met by other means.

Once the recovery objectives are defined, a list of potential interruptions should be created, and the recovery procedure should be developed and described. A contingency plan is then created

for the variety of potential interruptions. The contingency plan should be reviewed with managers to ensure that the cost to meet the contingency plan is approved. For many smaller-scale interruptions, a critical spares inventory will likely prove adequate to meet the recovery objectives. For larger-scale recovery, vendor relationships will likely be leveraged. For all types of recovery, backups are critical.

A disaster recovery plan (DRP) is a documented process or set of procedures that comprise a comprehensive statement of recovery actions to be taken before, during, and after a disaster. The DRP is ordinarily documented in both electronic and paper form to ensure that it is readily available during any type of disaster (e.g., natural, environmental, or caused by humans, whether intentionally or unintentionally). Organizations should develop, maintain, and validate disaster recovery plans for their environments to help minimize an event impact by reducing the time required to restore capabilities.

Organizations may already have some emergency response plans in place and should consider leveraging existing plans when developing a response plan for cybersecurity events.

Supplemental guidance for response planning can be found in the following documents:

- NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide*
- NIST SP 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
- CISA, *Handling Destructive Malware*
- Federal Emergency Management Agency (FEMA) National Incident Management System (NIMS)
- FEMA National Preparedness Goal

OT-Specific Recommendations and Guidance

Incident response planning may include the following elements:

- **Identification and classification of incidents.** The various types of OT incidents should be identified and classified based on potential impact so that a proper response can be formulated for each potential incident.
- **Response actions.** Incident response can range from doing nothing to performing a full system shutdown, which could result in a shutdown of the physical process. The response taken will depend on the type of incident and its effect on the OT system and the physical process being controlled. A written plan that documents the response to each type of incident should be prepared. This will provide guidance during times when there might be confusion or stress due to the incident. This plan should include step-by-step actions to be taken by various stakeholders.

Reporting requirements should be documented along with contact information and the reporting format to reduce confusion.

Response actions should also include steps for detection, analysis, containment, eradication, recovery, and post-incident activity. Some considerations for OT may include:

- Determining a priority, such as returning to normal operations as quickly as possible or performing an investigation and preserving forensic data
- Communicating with the incident response team
- Disconnecting infected systems from the network
- Physically isolating operationally independent networks (e.g., enterprise from control or control from safety)
- Transitioning to manual operations
- Resourcing for additional operations support to manually validate data
- Notifying management, public relations, and/or outside companies and agencies as required

If an incident is discovered, organizations should conduct a focused risk assessment on the OT environment to evaluate the effects of the attack and the options to respond. For example, one possible response option is to physically isolate the system under attack. However, this may have a negative impact on the OT and may not be possible without impacting operational performance or safety. A focused risk assessment should be used to determine the response action.

The plan should also indicate requirements for the timely replacement of components in the case of an emergency. If possible, replacements for hard-to-obtain critical components should be kept in inventory.

The organization should have a means for prioritizing recovery activities. This prioritization may leverage existing documentation, such as risk assessments or startup procedures. For example, the focus may be to recover the systems that support critical utilities prior to the systems that support manufacturing based on the order of start-up activities.

Testing recovery plan procedures for OT components may be difficult due to operational and safety requirements. Organizations may need to determine if "bench tests" or other offline testing is possible to confirm the recovery procedures for OT components. At a minimum, organizations should verify the integrity of the backups if a full recovery test cannot be performed.

6.2.5. Maintenance (PR.MA)

The outcomes that fall within the CSF Maintenance Category provide guidance for performing routine and preventative maintenance on the components of an information system. This includes the usage of local and remote maintenance tools and the management of maintenance personnel.

OT-Specific Recommendations and Guidance

Maintenance tracking solutions enable an organization to schedule, track, authorize, monitor, and audit maintenance and repair activities to OT and ensure that maintenance logs or changes are properly documented. Documenting these events provides an audit trail that can aid in cybersecurity-related troubleshooting, response, and recovery activities. Maintenance tracking can also provide visibility into scheduled maintenance for OT devices and help inform end-of-life decisions.

The software used for OT maintenance activities should be approved and controlled by the organization. Approved software should be obtained directly from vendors and its authenticity verified (e.g., by validating certificates or comparing the hashes of installers).

Any maintenance performed on an OT device can inadvertently modify its configuration and result in an increased attack surface. The hardened state of the OT device should be maintained regardless of the maintenance performed. Device configuration should be verified after maintenance and software patching, as some features may have inadvertently been reenabled or new features installed. Best practices and other supporting documents should be obtained from the device vendor to guide and inform maintenance activities.

Limiting the use of certain devices for maintenance activities can help reduce the chances of device compromise by exposure to external networks, unauthorized users, or theft. Maintenance devices that remain secure within the OT environment reduce their exposure. Using maintenance devices outside of the OT environment or connecting the devices to non-OT networks should be restricted or minimized.

Any device connected to the OT system should be disconnected after the maintenance activities are completed, and any temporary connections should be removed.

The operation, capabilities, and features of the devices used for maintenance activities should be well understood. Devices may contain wireless radios and other communications devices that may be vulnerable to side-channel attacks or may allow simultaneous connections between networks (i.e., dual-homed). Vendor documentation should be thoroughly reviewed to understand these capabilities.

6.2.6. Protective Technology (PR.PT)

Technical mechanisms assist organizations with protecting the devices and information within their environments. These technologies alone may not be sufficient to sustain security capabilities as threats evolve and change. As such, organizations should manage the technical solutions that secure the organizational assets in a manner consistent with policies, procedures, and agreements.

6.2.6.1. Logging (PR.PT-1)

Logging enables an organization to capture events that occur within its systems and networks. Events can be generated by many different systems, including OSs, workstations, servers, networking devices, cybersecurity software, and applications.

Supplemental guidance can be found in the following document:

- NIST SP 800-92, *Guide to Computer Security Log Management*

OT-Specific Recommendations and Guidance

Capturing log events is critical to maintaining situational awareness of the OT system. Typical events include maintenance functions (e.g., access control, configuration changes, backup and restore), OS functions, and application (i.e., process) events. The specific types of events available for logging will vary between OT devices and should be chosen based on the capabilities of the device and the desired events to be captured.

To support log correlation, each log entry should identify the device that generated the event, the timestamp of the event, and the user or system account that generated the event. In general, each log entry should also include where the event occurred, the type of event, when the event occurred, the source of the event, the identity of any users or system accounts related to the event, and the outcome of the event.

Correlating events across multiple OT devices can be difficult if the event timestamps generated by the devices were not informed by a shared time source. The internal clocks of each device should be synchronized with a primary clock to support event correlation between devices. Log entries should also produce a consistent timestamp format (e.g., time zone format, string format, daylight saving).

The collection and event forwarding functions may impact the performance of the OT device. Depending on the frequency of events being logged, the log size may grow quickly and result in increasing space utilization. Disk space and memory are limited on most OT devices, so adequate storage should be locally or remotely provided to reduce the likelihood of exceeding the device capacity, which could ultimately result in the loss of logging capability. Transferring logs from the OT devices to alternate storage should be considered.

6.2.7. Media Protection (PR.PT-2)

Removable media is protected, and use is restricted in accordance with policy. This includes labeling media for distribution and handling requirements, as well as storage, transport, sanitization, destruction, and disposal of the media.

Supplemental guidance can be found in the following documents:

- NIST SP 800-88, Rev. 1, *Guidelines for Media Sanitation*
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
- NIST SP 800-209, *Security Guidelines for Storage Infrastructure*

OT-Specific Recommendations and Guidance

Processes and procedures for the handling of media assets should be developed and followed. Media assets include removable media and devices, such as floppy disks, CDs, DVDs, SD cards, and USB memory sticks, as well as printed reports and documents. Physical security controls should address specific requirements for the safe and secure maintenance of these assets and provide guidance for transporting, handling, and erasing or destroying these assets. Security requirements could include safe storage from loss, fire, theft, unintentional distribution, or environmental damage.

OT devices should be protected against the misuse of media. The use of any unauthorized removable media or device on any node that is part of or connected to the OT should not be permitted. Solutions could be either procedural or technical to prevent the introduction of malware or the inadvertent loss or theft of data.

Physically protecting media or encrypting the data on media is critical to protecting the OT environment. Gaining access to media that contains OT data could provide a malicious actor with valuable information for launching an attack.

6.2.8. Personnel Security

Cybersecurity should be included in human resources practices to reduce the risk of human error, theft, fraud, or other intentional or unintentional misuse of information systems.

Supplemental guidance for the Personnel Security controls can be found in the following documents:

- NIST SP 800-35, *Guide to Information Technology Security Services*
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification*
- NIST SP 800-76-2, *Biometric Specifications for Personal Identity Verification*
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*

OT-Specific Recommendations and Guidance

A general personnel security program should address policy, position risk designations, personnel screening, terminations, transfers, access agreements, and third-party roles and responsibilities. OT personnel should communicate with human resources, IT, and physical security to ensure that personnel security requirements are being met.

An organization should consider establishing an access agreement and request form for managing physical and/or logical access to OT equipment. Organizations should also screen the personnel assigned to critical positions who control and maintain the OT.

Additionally, each employee should receive training that is relevant to and necessary for their job functions. Employees should demonstrate competence in their job functions to retain physical and logical access to OT. Organizations should consider adopting a framework, such as the National Initiative for Cybersecurity Education (NICE) Framework, for training their OT personnel.

6.2.9. Wireless Communications

Wireless communications utilize radio frequency (RF) to support data transmission. This can include a Wireless Fidelity (Wi-Fi) local area network communication based on IEEE 802.11 protocols and may also include cellular or other radio-based communications. RF-based communications provide enhanced flexibility over traditional physical (i.e., wired) communication capabilities. However, RF communications are also more susceptible to interference and may allow unauthorized personnel to eavesdrop.

Supplemental guidance for wireless communications can be found in the following documents:

- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- NIST SP 800-121, Rev. 2, *Guide to Bluetooth Security*
- NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*
- NIST SP 800-187, *Guide to LTE Security*

OT-Specific Recommendations and Guidance

The use of temporary or permanent wireless communication within an OT is a risk-based decision determined by the organization. Generally, devices that utilize wireless communication should be placed in a separate network segment and only be deployed where the residual risks to health, safety, the environment, and finances are low.

Prior to installation, a wireless survey should be performed to identify antenna locations and signal strength for adequate coverage and to minimize the exposure of the wireless network to interference from OT environmental factors and eavesdropping. Attackers typically use

directional antennas to extend the effective range of a wireless network beyond the standard range.

Organizations may choose to implement a wireless mesh network to improve resiliency or to eliminate areas with poor signal strength. Mesh networks can provide fault tolerance through alternate route selection and preemptive fail-over of the network. Organizations should also consider the performance and security impacts associated with the use of mesh networks. For example, when roaming between access points, devices may experience temporary communication loss. Roaming may also require different security controls to reduce the transition time. Organizations will need to find the appropriate balance between functional capabilities and cybersecurity to achieve the risk tolerance.

Wireless LANs

- Wireless device communications should be encrypted, and the encryption must not degrade the operational performance of the end devices. To reduce encryption latency, encryption should be considered at OSI Layer 2 rather than at Layer 3. The use of hardware accelerators to perform cryptographic functions should also be considered.
- Wireless access points should establish independent network segments (rather than extending an existing segment) and be used in combination with a boundary protection device to restrict and control communication.
- Wireless access points should be configured to have a unique service set identifier (SSID) and enable media access control (MAC) address filtering at a minimum.
- Wireless devices may require different security controls and should be zoned accordingly.
- An adaptive routing protocol should be considered if the devices are to be used for wireless mobility. The convergence time of the network should be as fast as possible to support rapid network recovery in the event of a failure or power loss.

Wireless Field Networks

When implementing a wireless field network, the following security features should be considered:

- Selecting a standard, non-proprietary protocol (e.g., IEEE 802.15.x)
- Ensuring that encryption is used between field instruments and wireless access points
- Allowlisting devices into the wireless device manager so that rogue devices cannot connect

- Implementing appropriately complex passwords and join keys

Most wireless field networks are inherently less reliable than their wired counterparts due to their susceptibility to signal jamming, distance limitations, and line-of-sight requirements. Work with the system vendor to design a wireless network that is appropriate for the application.

6.2.10. Remote Access

Security controls should be implemented to prevent unauthorized remote access to the organization's networks, systems, and data. A virtual private network (VPN) is a set of protocols designed to support secure remote access to network environments. A VPN can provide both strong authentication and encryption to secure communication data by establishing a private network that operates as an overlay on a public infrastructure. The most common types of VPN technologies are:

- **Internet Protocol Security (IPsec).** IPsec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion (i.e., payload) of each packet while leaving the packet header untouched. The more secure tunnel mode adds a new header to each packet and encrypts both the original header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet.
- **Transport Layer Security (TLS).** Sometimes referred to by the legacy terminology of Secure Sockets Layer (SSL), TLS provides a secure channel between two machines that encrypts the contents of each packet. TLS is most often recognized for securing Hypertext Transfer Protocol (HTTP) traffic in a protocol implementation known as HTTP Secure (HTTPS). However, TLS is not limited to HTTP traffic and can be used to secure many application-layer programs. Only TLS 1.2 or above should be considered.
- **Secure Shell (SSH).** SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Linux-based servers. SSH is a secure alternative to a telnet application, is included in most UNIX distributions, and is typically added to other platforms through a third-party package.

Supplemental guidance for access controls can be found in the following documents:

- NIST SP 800-52, Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*
- NIST SP 800-77, Rev. 1, *Guide to IPsec VPNs*
- NIST SP 800-113, *Guide to SSL VPNs*

OT-Specific Recommendations and Guidance

Many OT security architectures are designed with multiple levels, such as in the Purdue model. This can significantly limit access, which can minimize accidental or unauthorized disruptions to operations. A process

should be developed and communicated to the organization for requesting and enabling remote access. Remote access should be provided only if justified and limited to what is required for the business need. Remote access should not circumvent or negate safety or security controls. Multi-factor authentication should be considered for remote access to the OT system.

In critical situations or when vendor support is needed, temporary remote access may be requested to perform maintenance. In such cases, procedures should still be followed to ensure that secure connections are being utilized.

There are several different techniques for implementing temporary remote access, including:

- Users or protocols (e.g., RDP, SSH) that are temporarily permitted through the OT or enterprise firewall
- Screen-sharing technologies
- Modems
- VPNs

Regardless of the technology, organizations should consider the following:

- Implementing unique usernames and complex passwords
- Removing, disabling, or modifying any default credentials
- Updating any software and firmware to the latest versions
- Removing access when no longer required. Consider implementing automatic timers for removing access or managing change processes to manually confirm the removal of access.
- Monitoring remote activities
- Ensuring that operations personnel are aware of planned remote activity in the OT environment
- Initiating the connection from the OT environment
- Labeling remote connection devices so that operations may disconnect quickly in the case of unauthorized use

Dial-Up Modems

If dial-up modems are used in OT environments, consider using callback systems. This ensures that a dialer is an authorized user by having the modem establish the working connection based on the dialer's information and a callback number stored in the OT-approved authorized user list.

If feasible, disconnect modems when not in use, or consider automating this disconnection process by having modems disconnect after being on for a given amount of time. Sometimes, modem connections are part of the legal support service agreement with the vendor (e.g., 24/7 support with 15-minute response time). Personnel should be aware that disconnecting or removing the modems may require contracts to be renegotiated.

VPNs

VPN devices used to protect OT systems should be thoroughly tested to verify that the VPN technology is compatible with the application and that implementation of the VPN devices does not negatively impact network traffic characteristics.

VPN technology can also be applied between network segments. For example, a remote site might have a boundary protection device on-site that uses a VPN to establish a secure tunnel over an untrusted network (e.g., the internet) to a VPN-enabled device in the main control center at a different location.

6.2.11. Flaw Remediation and Patch Management

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. A systematic approach to managing and using software patches can help organizations improve the overall security of their systems in a cost-effective way. Organizations that actively manage and use software patches can reduce the chances that the vulnerabilities in their systems can be exploited, and they can save time and money that might be better spent responding to vulnerability-related incidents.

NIST SP 800-40, Rev. 4 [SP800-40r4] provides guidance for CIOs, CISOs, and others who are responsible for managing organizational risk related to the use of software. This publication frames patching as a critical component of preventive maintenance for computing technologies – a cost of doing business and a necessary part of what organizations need to do in order to achieve their missions. This publication also discusses common factors that affect enterprise patch management and recommends creating an enterprise strategy to simplify and operationalize patching while also improving risk reduction. This guidance may also be useful to business and mission owners, security engineers and architects, system administrators, and security operations personnel.

Supplemental guidance for flaw remediation and patch management can be found in the following document:

- NIST SP 800-40, Rev. 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*

OT-Specific Recommendations and Guidance

Significant care should be exercised when applying patches to OS components. Patches should be adequately tested (e.g., offline system testing) to determine the acceptability of any performance impacts.

Regression testing is also advised. It is not uncommon for patches to have an adverse impact on other software. A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective. Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functionality. Many OT systems utilize older versions of OSs that are no longer supported by the vendor, so patches may not be available.

Organizations should implement a systematic, accountable, and documented OT patch management process for managing exposure to vulnerabilities. The patch management process should include guidance on how to monitor for patches, when to apply patches, how to test the patches (e.g., with vendors or on offline systems), and how to select compensating controls to limit exposure of the vulnerable system when patching is delayed.

Many OT vulnerabilities are published to CISA as advisories. However, not all vendors report known vulnerabilities to CISA. Organizations can often stay informed of vulnerabilities by subscribing to vendor-specific notifications in addition to CISA alerts and advisories. Private cybersecurity companies also offer services to assist organizations with staying informed about known vulnerabilities within their OT environment. An organization is responsible for staying informed and determining when patches should be applied as part of their documented patch management process.

When and how to deploy patches should be determined by knowledgeable OT personnel. Consider separating the automated process for OT patch management from the automated process for non-OT applications. Patching should be deployed during planned OT outages.

Organizations may be required to follow industry-specific guidance on patch management. Otherwise, they may develop patch management procedures based on existing standards, such as NIST SP 800-40, Rev. 4 [SP800-40r4]; NERC CIP-007, or ISA 62443-2-3, Patch Management in the IACS Environment.

6.2.12. Time Synchronization

Time synchronization solutions enable an organization to synchronize time across many devices. This is important for many functions, including event and log correlation, authentication mechanisms, access control, and quality of service.

Supplemental guidance can be found in the following documents:

- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST IR 8323, *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*

OT-Specific Recommendations and Guidance

Synchronizing the internal clocks of OT systems and devices is critical for cyber event correlation and other OT functions (e.g., motion control). If a device or system clock is inaccurate, the timestamps generated by the clock for event and log entries will also be inaccurate, as well as any other functions that utilize the clock.

A common time should be used across all OT devices. Utilizing multiple time sources can benefit OT devices by reducing clock error and providing backup time sources if the primary time source is lost or if the time quality of a primary time source has degraded.

Authenticated Network Time Protocol (NTP) and secure Precision Time Protocol (PTP) (i.e., PTP with an authentication TLV [type, length, value]) can be used if there is a risk of malicious modification to the network time (e.g., RF jamming, packet spoofing, denial of service). Non-authenticated NTP is susceptible to spoofing and should be located behind the firewall.

Time sources located in the OT environment should be included in the system and network monitoring programs. If available, logs from each time source (e.g., syslog) should be forwarded to a log collection system.

6.3. Detect (DE)

The Detect Function enables the timely discovery of cybersecurity events by ensuring that appropriate activities are developed and implemented.

6.3.1. Anomalies and Events (DE.AE)

Organizations should understand different events, anomalies, and their potential impacts to systems and the environment to establish an effective detection capability. Within any environment, numerous non-malicious and potentially malicious events and anomalies occur almost continuously. Some examples of common events include:

Information Events

- Multiple failed logon attempts
- Locked-out accounts
- Unauthorized creation of new accounts
- Unexpected remote logons (e.g., logons of individuals who are on vacation, remote logon when the individual is expected to be local, remote logon for maintenance support when no support was requested)
- Cleared event logs
- Unexpectedly full event logs
- Antivirus or IDS alerts

- Disabled antivirus or other security controls
- Requests for information about the system or architecture (e.g., social engineering or phishing attempts)

Operational Events

- Unauthorized configuration changes
- Unauthorized patching of systems
- Unplanned shutdowns

Physical Access Events

- Physical intrusions

Networking Events

- Unexpected communication, including new ports or protocols being used without appropriate change management
- Unusually heavy network traffic
- Unauthorized devices connecting to the network
- Unauthorized communication to external IPs

Organizations should consider that not all events and anomalies are malicious or require investigation. Organizations should define incident alerting thresholds and response requirements for the events and anomalies that affect their systems and environment to establish an efficient incident detection capability.

Organizations should consider collecting and correlating event data from multiple sources and sensors using automated mechanisms where possible to improve detecting and alerting capabilities. For example, a centralized intrusion detection system could accept data feeds and logs from multiple devices and network segments to identify organization- or environment-specific events and sound an alarm. Detection tools should also be integrated with asset management tools. This integration can provide additional context to an event (e.g., where the system is located, which firmware version it runs, what the criticality of the system is) to help an organization determine the event impact.

Supplemental guidance can be found in the following documents:

- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems*
- NIST SP 1800-7, *Situational Awareness for Electric Utilities*

OT-Specific Recommendations and Guidance

Organizations should consider OT-specific events and anomalies for their processes and environments. Organizations should also note that some tools and alerts for behaviors or events that could indicate an intrusion may be normal behaviors and events within the OT environment. To reduce false positive and nuisance alarms, organizations

should establish their OT alerting thresholds based on baselines of normal network traffic and data flows in addition to normal human and OT process behavior. Additionally, OT components are often physically remote and not continually staffed. Alerting thresholds may need to take into consideration the response time associated with the alert. For example, a temperature alert threshold may have to be set to alert earlier based on the expected response time to correct the situation in order to avoid an incident.

Shared credentials are often used on OT systems. Anomalous behavior on shared accounts may be more difficult to determine, so organizations should consider whether additional controls are required, such as identifying the use of shared credentials using physical access monitoring.

6.3.2. Security Continuous Monitoring (DE.CM)

Organizations should implement continuous monitoring as part of the organizational risk management strategy to monitor the effectiveness of protective measures. This includes establishing the frequency for evaluating the implementation of the desired outcomes.

Continuous monitoring can be performed by internal or external resources to identify security gaps within the environment. Peer reviews (i.e., cold eyes reviews) between sites of the same organization are highly encouraged. When leveraging third-party services for security continuous monitoring, it is important to understand and evaluate how the organization's continuous monitoring data is protected by the third party. A third party that aggregates continuous monitoring information from multiple organizations may be a desirable target for adversaries.

Supplemental guidance can be found in the following documents:

- NIST SP 800-53A, Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- NIST SP 800-55, Rev. 1, *Performance Measurement Guide for Information Security*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*

OT-Specific Recommendations and Guidance

Organizations may find that automation within OT environments may not be possible due to the sensitivity of the systems or the resources required to support the automation. For example, some automated systems may utilize active scanning to support vulnerability or patch management or to validate device configurations. Solutions that perform active scanning or use local resources to support automation should be tested before deployment into the OT system.

Continuous monitoring can be achieved using automated tools, through passive scanning, or with manual monitoring performed at a frequency deemed commensurate with the risk. For example, a risk assessment may determine that the logs from isolated (i.e., non-networked), non-critical devices should be reviewed monthly by OT personnel to determine whether anomalous behavior is occurring. Alternatively, a passive network monitor might be able to detect vulnerable network services without having to scan the devices.

When organizations implement a sampling methodology, the criticality of the components should be considered. For example, the sampling methodology should not inadvertently exclude higher risk devices, such as Layer 3 or Layer 4 firewalls.

When using third parties to continuously monitor security controls, ensure that the personnel involved have the appropriate skillset to analyze OT environments.

6.3.2.1. Network Monitoring (DE.CM-1)

Network monitoring involves organizations reviewing alerts and logs and analyzing them for signs of possible cybersecurity incidents. Organizations should consider automation – including in-house developed, commercially available solutions or some combination of tools – to assist with monitoring efforts. Tools and capabilities that support behavior anomaly detection (BAD), security information and event management (SIEM), intrusion detection systems (IDS), and intrusion prevention systems (IPS) can assist organizations with monitoring traffic throughout the network and generate alarms when they identify anomalous or suspicious traffic. Some other capabilities to consider for network monitoring include:

- Asset management, including discovering and inventorying devices connected to the network
- Baselining typical network traffic, data flows, and device-to-device communications
- Diagnosing network performance issues
- Identifying misconfigurations or malfunctions of networked devices

Supplemental guidance can be found in the following documents:

- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST IR 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*

OT-Specific Recommendations and Guidance

Network monitoring can greatly enhance the ability to detect attacks entering or leaving the OT networks. It can also improve network efficiency by detecting non-essential traffic. OT cybersecurity personnel must be part of the diagnostic process of interpreting the alerts provided by network monitoring tools. Careful monitoring and an understanding

of the normal state of the OT network can help distinguish transient conditions from legitimate attacks and provide insight into events that are outside of the normal state.

Gaining access to network traffic is typically performed with network test access points (TAPs) and switched port analyzer (SPAN) ports, though performance impacts to the OT system may result from their use, especially with SPAN ports.

Network sensors should be placed to effectively monitor the OT network. Typical installations locate the network sensors between the control network and corporate network, but other locations can include network perimeters, key network segments (e.g., DMZ), and critical OT devices.

All sensors should be subjected to extensive testing and be implemented in a test environment before being deployed into the OT network. Configuring the sensor into a test or learning mode after it is installed on the network provides an opportunity to tune the device with real OT network traffic. Tuning can help reduce false positive alerts, reduce the alert "noise" from typical network traffic, and help identify implementation and configuration problems.

Failure modes of network sensors in the event of a sensor failure should be considered (e.g., does the sensor fail-safe or fail-open if the device fails).

6.3.2.2. System Use Monitoring (DE.CM-1 and DE-CM-3)

System use monitoring solutions enable an organization to monitor, store, and audit system events (e.g., system logs, running processes, file access and modification, system and application configuration changes) that occur within a system. Monitoring users and systems helps to ensure that they are behaving as expected and can aid in troubleshooting when events occur by providing information about which users were working within the system during the event. System and device misconfigurations can also be identified.

Compared to network monitoring, system use monitoring solutions can analyze activity that does not traverse the network. In host-based solutions, this can be achieved with real-time monitoring of inter-process communications and other internal OS data, while active scanning solutions gather information by querying the OS or application programming interfaces (APIs).

Supplemental guidance can be found in the following documents:

- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

OT-Specific Recommendations and Guidance

Situational awareness of the OT system is imperative to understanding the current state of the system, validating that it is operating as intended,

and ensuring that no policy violations or cyber incidents have hindered its operation. Strong device monitoring, logging, and auditing are necessary to collect, correlate, and analyze security-related information and provide actionable communication about the security status across the complete OT system. In the event of a cybersecurity incident, the information gathered by system use monitoring solutions can be used to perform forensic analysis of the OT system.

System use monitoring solutions can generate significant amounts of events, so these solutions should be used in combination with a control log management system, such as a SIEM, to help filter the types of events and reduce alert fatigue. The amount of tuning and customization of events and alerts depends on the type of OT system and the number of devices in the system.

System use monitoring solutions should be subjected to extensive testing and implemented in a test environment before being deployed to devices in the OT system. Concerns include the performance impacts of host-based agents on devices, the impact of active scanning on devices, and the capability of the network infrastructure bandwidth. Separate appliances can offload the processing. Host-based agents can impact the performance of the OT device because of the resources that they consume.

6.3.2.3. Malicious Code Detection (DE.CM-4)

When stored, processed, and transmitted, files and data streams should be scanned using specialized tools with a combination of heuristic algorithms and known malware signatures to detect and block potentially malicious code. Malicious code protection tools only function effectively when they are installed, configured, run full-time, and maintained properly against the state of known attack methods and payloads.

Supplemental guidance for anti-malware practices can be found in the following documents:

- NIST SP 800-83, Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- NIST SP 1058, *Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*

OT-Specific Recommendations and Guidance

While antivirus tools are common in IT computer systems, the use of antivirus with OT may require adopting special practices, including compatibility checks, change management, and performance impact metrics. These practices should be utilized to test new signatures and new versions of antivirus software.

Some OT vendors recommend and even support the use of vendor-specific antivirus tools. In some cases, OT system vendors may have performed regression testing across their product line for supported

versions of a particular antivirus tool and provide associated installation and configuration documentation.

Generally:

- General-purpose Windows, Unix, and Linux systems that are used as engineering workstations, data historians, maintenance laptops, and backup servers can be secured like commercial IT equipment by installing push or auto-updated antivirus software with updates distributed via an antivirus server located inside the process control network. Follow organization-developed procedures for transferring the latest updates from known vendor sites to the OT antivirus servers and other OT computers and servers.
- Follow vendor recommendations on all other servers and computers (e.g., DCS, PLC, instruments) that have time-dependent code, modified or extended OSs, or any other change that makes them different from a standard PC. Test the antivirus software and updates on an offline system if possible (e.g., install on a backup HMI and validate that performance is not degraded before applying to the primary HMI).

According to NIST SP 1058 [SP1058], antivirus software may negatively impact the time-critical control processes of an ICS. The SP also identified significant CPU usage when running manual scans and signature updates, which could have negative impacts on OT computers and servers. As a result:

- Configuration of the antivirus software should be tested on an offline system, if possible.
- Manual scanning and signature updates should be performed while the system is not critical for operations.
- Redundancy should be considered for critical systems that require ongoing antivirus updates such that signature updates can be performed without impacting operations (e.g., consoles and HMIs).
- When configuring file exclusion lists, determine which control application files should not be scanned during production time because of possible OT system malfunction or performance degradation.

CISA provides a recommended practice for updating antivirus in OT environments.

6.3.2.4. Vulnerability Scanning (DE.CM-8)

Vulnerabilities can be identified through a combination of automated and manual techniques. These vulnerability scans should be performed on an ongoing basis to capture new vulnerabilities as they are discovered.

OT-Specific Recommendations and Guidance

Some common ways to achieve vulnerability identification in the OT environment are:

- Continuous monitoring using passive or active scanning capabilities. Organizations should consider how vulnerability scanning tools may impact OT components and communications by testing them in an offline environment prior to implementing them in production.
    - Passive scanning tools typically utilize network traffic analyzers to detect assets and determine possible vulnerabilities affecting the assets.
    - Active scanning tools typically utilize an agent to connect to networked assets and perform detailed queries and analysis of the components to determine possible vulnerabilities affecting the assets.
- Performance testing, load testing, and penetration testing if the test will not adversely impact the production environment
- Regular audits, assessments, and peer reviews to identify gaps in security

6.3.3. Detection Process (DE.DP)

The detection process includes maintaining and testing processes, procedures, and tools to ensure that anomalous events are identified in a prompt manner and responsible parties (individuals) are alerted and held accountable for adequate responses. To ensure the ongoing awareness of anomalous events, define roles and responsibilities for accountability, periodically review that detection activities comply with the requirements, test the detection processes regularly, communicate detected events to appropriate personnel to act, and continuously improve detection capabilities.

6.4. Respond (RS)

The Respond Function supports the ability to take the appropriate course of action and activities to contain a cybersecurity incident when it occurs.

6.4.1. Response Planning (RS.RP)

When responding to events, organizations should attempt to capture the details associated with executing the documented response plans. This may help organizations identify gaps or potential opportunities for improvement in the response plan during the post-incident review process. Due to the time sensitivity of response efforts, organizations may want to consider other techniques (e.g., reviewing logs, reviewing video footage captured during the response activities, or interviewing response personnel) if capturing execution details impacts safety or increases the time to complete the response plan.

6.4.2. Response Communications (RS.CO)

Responding to a cybersecurity incident includes coordinating with internal and external stakeholders. An incident response team should be assembled. Depending on the complexity and impact of the incident, the incident response team could consist of one or many individuals who have been trained on incident response. The FEMA National Incident Management System (NIMS) can be used to standardize common terminology and roles for incident response.

Prior to an incident, organizations should consider how to communicate with response personnel and external entities, including:

- Developing an email distribution list for incident response
- Leveraging an emergency notification system
- Establishing backup communication plans for radio, phone, or email if primary communication systems fail
- Designating a spokesperson for external communications
- Designating a scribe for internal incident communications

OT-Specific Recommendations and Guidance

Organizations should consider FEMA's guidance on crisis communications when establishing their communication plans and strategies.

The personnel responsible for responding to an incident should be informed of and trained on their responsibilities.

The response plan should include a detailed list of organizations and personnel that should be contacted for incident response and reporting under various circumstances. Each individual should be assigned roles that are required for incident response, which could include incident commander; operations, planning, logistics, or finance/administration

section chief or member; and public information, safety, or liaison officer.

To support a response in an OT environment, an organization should consider including the following personnel in the response plan.

Internal Resources

- Designated Incident Commander
- Operations leadership
- Safety personnel
- On-call OT systems personnel
- On-call IT personnel
- Physical security personnel
- Administrative personnel
- Procurement personnel
- Public relations personnel
- Legal personnel

External Industry Partners

- OT technical support (e.g., vendors, integrators)
- Operational supply chain (e.g., suppliers, customers, distributors, business partners)
- Incident response team
- Surge support
- Impacted community (e.g., facility neighbors)

Organizations are required to report incidents involving federal agencies in accordance with PPD-21 [PPD-21] and PPD-41 [PPD-41]. CISA maintains the list of sector-specific contacts.

Legal departments can often assist with developing non-disclosure agreements or other contracts if an organization plans to utilize external resources for incident response. It may be beneficial to develop these contracts prior to an incident occurring so that incident response can be immediate. Private companies can be held on retainer in case of an OT incident.

6.4.3. Response Analysis (RS.AN)

Cybersecurity incidents are analyzed to ensure effective response and recovery activities that are consistent with the detection process and the response plan. Analysis includes reviewing notifications, determining whether an investigation is required, understanding potential impacts, performing forensics, categorizing the incident consistent with the response plan, and analyzing disclosed vulnerabilities.

Supplemental guidance for the response analysis controls can be found in the following document:

- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*

OT-Specific Recommendations and Guidance

When determining the overall impact of a cybersecurity incident, consider the dependencies of OT and its resulting impact on operations. For example, an OT system may be dependent on IT for business applications, such that an incident on the IT network results in an OT disconnect or shutdown.

If an organization does not have adequate resources or capabilities to conduct OT forensics, consider engaging external organizations to perform forensic analysis.

Organizations should identify and classify cyber and non-cyber incidents that affect the OT environment according to the incident response plan. When developing the OT incident response plan, potential classes of incidents could include accidental actions taken by authorized personnel, targeted malicious attacks, and untargeted malicious attacks.

6.4.4. Response Mitigation (RS.MI)

Mitigation activities are meant to prevent expansion of the incident, mitigate its effects, and resolve the incident and should be consistent with the response plan.

OT-Specific Recommendations and Guidance

OT components are often physically remote and not continually staffed. For these cases, consider how the organization would respond during an incident and the additional time required to coordinate the response. The system may need to be designed with the capability to minimize impacts until personnel can arrive on-site (e.g., remote shutdown or disconnects).

Cyber incident mitigation may involve process shutdowns or communication disconnects that impact operations. These impacts should be understood and communicated during incident mitigation.

6.4.5. Response Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities. Organizations should designate one or more individuals to be responsible for documenting and communicating response actions to the incident response team, which can later be reviewed for lessons learned.

6.5. Recover (RC)

Timely recovery to normal operations after a cybersecurity incident is critical. The Recover Function addresses developing and implementing activities to maintain system resilience and ensure timely restoration of capabilities and services affected by a cybersecurity incident.

6.5.1. Recovery Planning (RC.RP)

When recovering from events, organizations should attempt to capture details associated with the execution of the documented recovery plans. Capturing execution details may help organizations during the post-incident review process to determine whether any gaps or potential opportunities for improvement in the recovery plan should be considered. Due to the time sensitivity of recovery efforts, organizations may want to consider other techniques (e.g., reviewing logs, reviewing video footage captured during the recovery activities, or interviewing recovery personnel) if capturing execution details impacts safety or increases the time to complete the recovery plan.

Supplemental guidance for recovery planning can be found in the following documents:

- NIST SP 800-184, *Guide for Cybersecurity Event Recovery*
- NIST SP 800-209, *Security Guidelines for Storage Infrastructure*

6.5.2. Recovery Improvements (RC.IM)

As a recovery effort is ongoing, the recovery steps taken should be documented to identify lessons learned. These lessons can be used to improve recovery plans and processes.

Supplemental guidance for recovery improvements can be found in the following document:

- NIST SP 800-184, *Guide for Cybersecurity Event Recovery*

6.5.3. Recovery Communications (RC.CO)

Restoration activities are coordinated with internal and external parties. In addition to operational recovery, an organization may need to manage public relations and repair its reputation.

Supplemental guidance for recovery communications can be found in the following document:

- NIST SP 800-184, *Guide for Cybersecurity Event Recovery*

OT-Specific Recommendations and Guidance

A list of internal and external resources for recovery activities should be developed as part of the recovery planning effort. During an event, this list should be used to get all necessary personnel on-site, as required, to recover within the RTO and RPO.

Internal Communications

- OT personnel
- IT personnel
- Procurement
- Management with appropriate authority to approve the cost of recovery
- Storage or warehouse personnel

External Communications

- OT vendors
- Security companies that may be held on retainer for response and recovery efforts
- Storage or warehouse personnel
- Internet service providers
- Owners of the attacking systems and potential victims