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.