NISTIR 8183A
Volume 1

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide:
Volume 1 – General Implementation Guidance

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Jeffrey Cichonski
Michael Pease
Neeraj Shah
Wesley Downard

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-1

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

NISTIR 8183A
Volume 1

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide:
Volume 1 – General Implementation Guidance

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Michael Pease
Intelligent Systems Division
Engineering Laboratory

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

Neeraj Shah
Strativia, LLC
Largo, Maryland

Wesley Downard
G2, Inc.
Annapolis Junction, Maryland

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-1

September 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8183A, Volume 1
81 pages (September 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-1

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: CSF_Manufacturing_Profile_Implementation@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This guide provides general implementation guidance (Volume 1) and example proof-of-concept solutions demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Impact Level. Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to complement but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Keywords

Computer security; Cybersecurity Framework (CSF); distributed control systems (DCS); industrial control systems (ICS); information security; manufacturing; network security; programmable logic controllers (PLC); risk management; security controls; supervisory control and data acquisition (SCADA) systems.

Supplemental Content

Additional volumes of this publication include:

NISTIR 8183A Volume 2, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case.* https://doi.org/10.6028/NIST.IR.8183A-2

NISTIR 8183A Volume 3, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case.* https://doi.org/10.6028/NIST.IR.8183A-3

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. A special acknowledgement to the members of the International Society of Automation (ISA) 99, Industrial Automation and Control Systems Security Committee and the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG) for their exceptional contributions to this publication.

Note to Readers

This guide describes a proof-of-concept solution for securing manufacturing environments that has only been tested in a lab environment. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape. We welcome feedback on its contents and your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to CSF_Manufacturing_Profile_Implementation@nist.gov.

Revision to Include Updates in Cybersecurity Framework Version 1.1

The Cybersecurity Framework Manufacturing Profile, NISTIR 8183, was drafted and released when the Cybersecurity Framework was at Version 1.0. This guide provides implementation guidance and example proof-of-concept solutions with respect to the language in the original Cybersecurity Framework Manufacturing Profile.

The Cybersecurity Framework Manufacturing Profile, NISTIR 8183, is scheduled to be revised to include the updates in the Cybersecurity Framework Version 1.1, and will be published as NISTIR 8183, Revision 1.

Once NISTIR, 8183, Revision 1 has been released, this implementation guide will be revised to include the updates in the Cybersecurity Framework Version 1.1 as well, and will be published as NISTIR 8183A, Revision 1.

Table of Contents

Executive Summary

This guide provides general implementation guidance (Volume 1) and example proof-of-concept solutions demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [8] Low Impact Level. A manufacturing system could be classified as Low potential impact if the loss of integrity, availability, or confidentiality could be expected to have a limited adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment. A limited adverse effect means that, for example, the loss of integrity, availability, or confidentiality might:

- result in degradation in mission capability to an extent and duration that the system can perform its primary functions, but the effectiveness of the functions is noticeably reduced,
- result in minor damage to operational assets,
- result in minor financial loss, or
- result in minor harm to individuals.

Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape.

The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to complement but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

The CSF Manufacturing Profile focuses on desired cybersecurity outcomes and can be used as a roadmap to identify opportunities for improving the current cybersecurity posture of the manufacturing system. The Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals. Relevant and actionable security practices that can be implemented to support key business/mission goals are then identified.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these products, nor does it guarantee compliance with any regulatory initiatives. Each organization’s information security experts should identify the products that will best integrate with their existing tools and manufacturing system infrastructure. Your organization may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

1. Introduction

The Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," [1] directed the development of the voluntary Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk [1] for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

The Cybersecurity Framework is a voluntary risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks [2]. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without imposing additional regulatory requirements.

To address the needs of manufacturers, a Manufacturing Profile [8] of the Cybersecurity Framework was developed, through collaboration between government and the private sector, to be an actionable approach for implementing cybersecurity controls into a manufacturing system and its environment. The Profile defines specific cybersecurity activities and outcomes for the protection of the manufacturing system, its components, facility, and environment. Through use of the Profile, the manufacturer can align cybersecurity activities with business requirements, risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to cybersecurity from standards, guidelines, and industry best practices.

1.1 Purpose and Scope

Many small and medium-sized manufacturers have expressed challenges in implementing a standards-based cybersecurity program. This guide provides general implementation guidance (Volume 1) and example proof-of-concept solutions demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [8] Low Impact Level. A manufacturing system could be classified as Low potential impact if the loss of integrity, availability, or confidentiality could be expected to have a limited adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment. A limited adverse effect means that, for example, the loss of integrity, availability, or confidentiality might:

- result in degradation in mission capability to an extent and duration that the system can perform its primary functions, but the effectiveness of the functions is noticeably reduced,
- result in minor damage to operational assets,
- result in minor financial loss, or
- result in minor harm to individuals.

Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these products, nor does it guarantee compliance with any regulatory initiatives. Each organization's information security experts should identify the products that will best integrate with their existing tools and manufacturing system infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these guidelines in whole or can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

This project is guided by the following assumptions:

- the solutions were developed in a lab environment,
- the environment is based on a typical small manufacturer's environment,
- the environment does not reflect the complexity of a production environment, and
- an organization can access the skills and resources required to implement a manufacturing cybersecurity solution.

1.2 Audience

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- control engineers, integrators, and architects who design or implement secure manufacturing systems,
- system administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure manufacturing systems,
- managers who are responsible for manufacturing systems,
- senior management who are trying to understand implications and consequences as they justify and implement a manufacturing systems cybersecurity program to help mitigate impacts to business functionality, and
- researchers, academic institutions and analysts who are trying to understand the unique security needs of manufacturing systems.

1.3 Document Structure

The remainder of Volume 1 is divided into the following major sections:

- Section 2 provides an overview of manufacturing systems.
- Section 3 provides an overview of the CSF Manufacturing Profile.
- Section 4 discusses the project's CSF Manufacturing Profile implementation approach.
- Section 5 provides an overview of the policy and procedure documents needed to meet the requirements specified in the CSF Manufacturing Profile Low Impact Level.
- Section 6 provides the technical capabilities needed to meet the requirements specified in the CSF Manufacturing Profile Low Impact Level.
- Section 7 examines potential solutions that can address the requirements specified in the CSF Manufacturing Profile Low Impact Level.
- Section 8 provides an overview of the laboratory environment used for implementations.
- Appendix A provides a list of acronyms and abbreviations used in this document.
- Appendix B provides a glossary of terms used in this document.
- Appendix C provides a list of references used in the development of this document.

Volume 2 of this guide provides a proof-of-concept CSF Manufacturing Profile Low Impact Level implementation for a process-based manufacturing system.

Volume 3 of this guide provides a proof-of-concept CSF Manufacturing Profile Low Impact Level implementation for a discrete-based manufacturing system.

2. Overview of Manufacturing Systems

Manufacturing is a large and diverse industrial sector. Manufacturing industries can be categorized as either *process-based, discrete-based,* or a combination of both [3].

Process-based manufacturing industries typically utilize two main process types:

- **Continuous Manufacturing Processes.** These processes run continuously, often with phases to make different grades of a product. Typical continuous manufacturing processes include fuel or steam flow in a power plant, petroleum in a refinery, and distillation in a chemical plant.
- **Batch Manufacturing Processes.** These processes have distinct processing steps, conducted on a quantity of material. There is a distinct start and end to a batch process with the possibility of brief steady state operations during intermediate steps. Typical batch manufacturing processes include food, beverage, and biotech manufacturing.

Discrete-based manufacturing industries typically conduct a series of operations to create a distinct product. Electronic and mechanical parts assembly and parts machining are typical examples of this type of industry. Both process-based and discrete-based industries utilize similar types of control systems, sensors, and networks. Additionally, some facilities are a hybrid of discrete and process-based manufacturing.

Manufacturing systems are usually located within a confined factory or plant-centric area. Communications in manufacturing industries are typically performed using fieldbus and local area network (LAN) technologies that are reliable and high speed. Wireless networking technologies are also gaining popularity in manufacturing industries. Fieldbus includes, for example, DeviceNet, Modbus, and Controller Area Network (CAN) bus.

The manufacturing sector of the critical infrastructure community includes public and private owners and operators, along with other entities. Members of the distinct critical infrastructure sector perform functions that are supported by industrial control systems (ICS) and by information technology (IT). This reliance on technology, communication, and the interconnectivity of ICS and IT has changed and expanded the potential vulnerabilities and increased potential risk to manufacturing system operations.

3. CSF Manufacturing Profile Overview

The Manufacturing Profile [8] was developed to be an actionable approach for implementing cybersecurity controls into a manufacturing system and its environment. The specific statements in the Subcategories in Section 7 of the Manufacturing Profile were derived from the security controls of the NIST Special Publication (SP) 800-53 Rev.4 [4] and are customized to the manufacturing domain using relevant informative references. The general informative references of ISA/IEC 62443 [5] from the Cybersecurity Framework are also listed in the References column. COBIT 5 is sourced for Subcategories that have no corresponding 800-53 references. Additional input came from NIST SP 800-82, Rev.2, Section 6.2 (Guidance on the Application of Security Controls to ICS) and Appendix G (ICS Overlay) [3]. For informative references to an entire control family or set of controls (such as Subcategory ID.GV-1's informative reference to all "policy and procedures" controls), the approach took a holistic view of the controls comprising the family/set.

The Manufacturing Profile expresses tailored values for cybersecurity controls for the manufacturing system environment. These represent the application of the Categories and Subcategories from the Cybersecurity Framework based on domain-specific relevance, business drivers, risk assessment, and the manufacturer's priorities. Users of the Profile can also add Categories and Subcategories as needed to address unique and specific risks.

4. CSF Manufacturing Profile Implementation Approach

Meeting the Manufacturing Profile Subcategory requirements can be accomplished by developing and implementing policies and procedures and/or implementing technical solutions, depending on the particular Subcategory language.

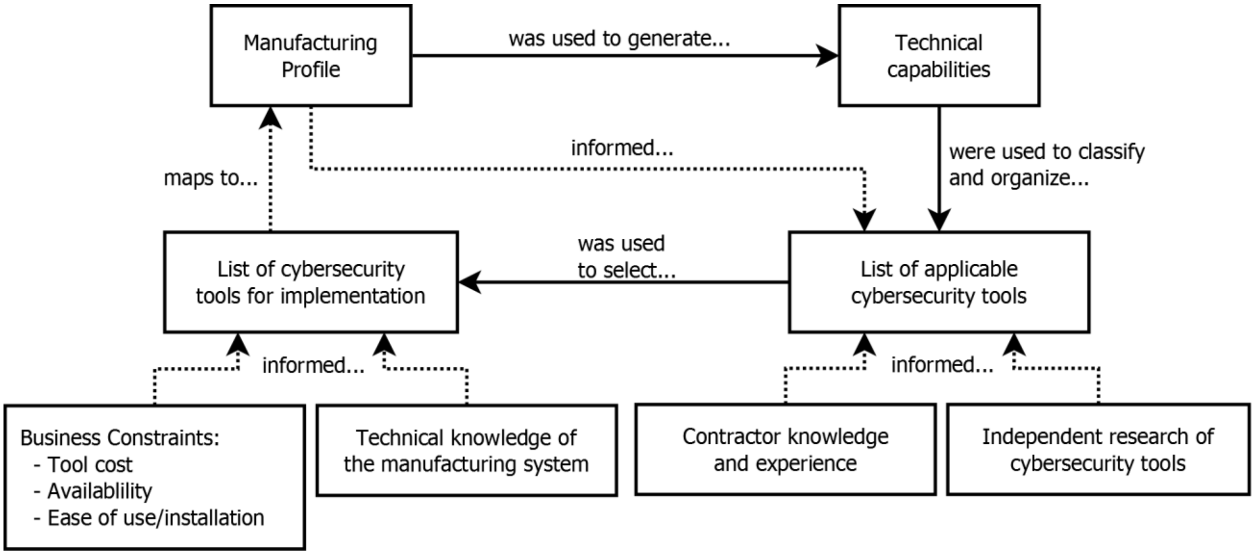
Manufacturing Profile
was used to generate...
Technical capabilities
maps to...
informed...
were used to classify and organize...
was used to select...
List of cybersecurity tools for implementation
List of applicable cybersecurity tools
informed...
informed...
Business Constraints:
- Tool cost
- Availablility
- Ease of use/installation
Technical knowledge of the manufacturing system
Contractor knowledge and experience
Independent research of cybersecurity tools

Figure 4-1. Approach used for identifying, planning and implementing technical cybersecurity capabilities

Figure 4-1 provides a visual representation of the approach used for identifying, planning and implementing technical cybersecurity capabilities as well as identifying the complementary cybersecurity processes and procedures. The Cybersecurity Framework Manufacturing Profile [8] was the principal resource describing the cybersecurity outcomes desired in both of NIST's manufacturing testbed scenarios. The outcomes described in the Manufacturing Profile are grounded by and cross referenced with prescriptive cybersecurity controls from standards relevant to ICS owners and operators.

The initial step of this planning process was focused on researching what cybersecurity related tools, configurations, and best practices are required to achieve the specific outcomes or Profile Subcategories. The Profile Subcategories and specific language provided by mapped cybersecurity controls provided insight into classifications of technical capabilities needed to be implemented in the testbed environments. From these high-level classifications of capabilities, NIST researchers identified and built a list of commercial products and open source tools that fit into each of these classifications. The list of solutions was then used to inform implementation planning and select specific solutions, tools, and products for implementation in the testbed environment. The selection of these technologies for implementation was informed by: technical knowledge of the testbed; solution cost; availability; maturity; level of expertise required for implementation and management; and the lab IT administrator's expertise.

The mapping of technical solutions to Profile Subcategories in most cases did not provide exact one-to-one coverage. In most scenarios, during the planning process there was a realization that implementing one technical capability might only satisfy portions of multiple Subcategories and in some scenarios implementation of multiple technical capabilities were required in order to achieve the outcome described by a Profile Subcategory. Some Profile Subcategories (e.g., PR.DS-3) required the implementation of a technical capability complemented by the addition of a cybersecurity policy or procedure. While this mapping adds complexity to the planning process it enables system owners to gain an understanding of what technical solutions will enable them to achieve the most Subcategory outcomes. Priorities can be assigned based the specific mission and business objectives of the organization.

Section 5 provides an overview of the six policy and procedure documents needed to meet the requirements specified in the CSF Manufacturing Profile Low Impact Level.

Section 6 provides the technical capabilities needed to meet the requirements specified in the CSF Manufacturing Profile Low Impact Level.

Section 7 examines potential solutions that can address the requirements specified in the CSF Manufacturing Profile Low Impact Level.

5. Policy/Procedural Capabilities Overview

For the implementation of the two use cases, six policy and procedural documents were produced for each:

5.1 Cybersecurity Program Document

The Cybersecurity Program document establishes guidelines and principles for initiating, implementing, maintaining, and improving information security management of the organization. It is a documented set of the organization’s security policies, procedures, guidelines and standards. The program is intended to protect the confidentiality, integrity and availability of information resources.

5.2 Cybersecurity Policy Document

The Cybersecurity Policy document defines the cybersecurity requirements for the proper and secure use of the Information Technology services in the organization. Its goal is to protect the organization and its users to the maximum extent possible against cybersecurity threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

5.3 Cybersecurity Operations Document

The Cybersecurity Operations document defines the operational steps management and employees will follow ensuring consistency with response to events occurring within the manufacturing system. This document contains content which should be referred to often to help ensure all employees and individuals performing work within the manufacturing system are familiar with cybersecurity operations.

5.4 Risk Management Document

The Risk Management Strategy document defines how risks associated with the organization will be identified, analyzed, and managed. It outlines the risk management strategy for the organization. In addition, it provides standard terminology, clear roles and responsibilities and details of the risk management process. This document can be used by the management to understand risks, estimate impacts, and define responses to issues. It is designed to guide the project team and stakeholders.

5.5 Incident Response Plan Document

The Incident Response Plan document describes the plan for responding to information security incidents within an organization. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The purpose of this plan is to detect and react to cybersecurity incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

5.6 System Recovery Plan Document

The System Recovery Plan is designed to ensure the continuation of vital manufacturing/business processes in the event a cybersecurity incident occurs. Its purpose is to provide a structured approach for responding to cybersecurity incidents by leveraging the infrastructure inventory and configuration information relevant to the organization's IT and OT environments to restore operational capabilities.

This plan has been developed to accomplish the following objectives:

- limit the magnitude of any loss by minimizing the duration of a manufacturing interruption,
- assess damage, repair the damage, and restore manufacturing system,
- manage the recovery operation in an organized and effective manner, and
- prepare personnel to respond effectively in system recovery situations.

6. Technical Capabilities Overview

This section discusses the technical capabilities identified by the team necessary to meet the CSF Manufacturing Profile language. For each technical capability, an overview of the capability is provided, the security benefits of implementing the capability is listed, any potential system impacts the capability could have on the manufacturing system are discussed, and the CSF Manufacturing Profile Subcategories that are addressed when the capability is implemented are listed.

6.1 Hardware Inventory Management

Hardware inventory management tools enable a manufacturer to track computing and network devices within the manufacturing system, including device details and location information.

6.1.1 Security Benefit

Hardware inventory management tools are used to track physical computing and network devices within the manufacturing system, detect new or unauthorized devices, detect the removal of devices, and track specific device details. Having a complete inventory of what computing and network devices exist in an environment will facilitate a comprehensive deployment of cybersecurity protections.

6.1.2 Potential System Impacts

Hardware inventory management tools that use active scanning can potentially impact the manufacturing system. Care must be taken before using these tools to identify manufacturing system devices on an operational system. Impacts could be due to the nature of the information or the volume of network traffic. Consider using hardware inventory tools that use active scanning during planned downtime for detailed data collection. Passive hardware inventory tools could be used for continuous monitoring of the manufacturing system.

6.1.3 Manufacturing Profile Subcategories

ID.AM-1, PR.DS-3, DE.CM-7

6.2 Software and Firmware Inventory Management

Software and firmware inventory management tools enable a manufacturer to track software and firmware installed within the manufacturing system computing and network devices, including identification, version numbers, and location information.

6.2.1 Security Benefit

Software and firmware inventory management tools enable a manufacturer to track installed software and firmware on systems within the manufacturing system, detect new or unauthorized software, track software versions, and facilitate the remote removal of software. Some software inventory tools also allow the tool to extend its scanning into the system itself (i.e. scan system peripherals, installed RAM and processors, and network configurations).

6.2.2 Potential System Impacts

Software and firmware inventory management tools that use active scanning can potentially impact the manufacturing system. Care must be taken before using these tools on an operational system. Impacts could be due to the nature of the information or the volume of network traffic. Consider using software and firmware inventory management tools that use active scanning during planned downtime.

6.2.3 Manufacturing Profile Subcategories

ID.AM-2, PR.DS-3, DE.CM-7

6.3 Systems Development Lifecycle Management

Systems development lifecycle management tools enable a manufacturer to track the scope of activities associated with hardware and software components of the manufacturing system, encompassing each component's initiation, development and acquisition, implementation, operation and maintenance, and its ultimate decommissioning and disposal.

6.3.1 Security Benefit

Systems development lifecycle management tools provide hardware and software tracking from the point of purchase/installation until removal/decommissioning. Tracking that updates like firmware, bios, drivers, software updates, and patches have been applied ensures better protection against known and unknown vulnerabilities and helps manufacturers better understand the risks to their systems.

6.3.2 Potential System Impacts

Systems development lifecycle management tools should not impact the manufacturing system, as they are not typically installed or operated on the manufacturing system.

6.3.3 Manufacturing Profile Subcategories

PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-6, DE.CM-7

6.4 Network Architecture Documentation

Network architecture documentation tools enable a manufacturer to identify, document, and diagram the interconnections between networked manufacturing system devices, corporate networks, and other external network connections.

6.4.1 Security Benefit

Detailed documentation of the manufacturing environment's network devices and interconnections is an important component of the Manufacturing Profile. A comprehensive understanding of the interconnections within the environment is critical for successful deployment of cybersecurity controls. This information is equally important for effective monitoring.

6.4.2 Potential System Impacts

Network architecture documentation tools that use automated topology discovery technologies can potentially impact the manufacturing system. Care must be taken before using these tools on an operational system. Impacts could be due to the nature of the information or the volume of network traffic. Consider using network architecture documentation tools that use automated topology discovery technologies during planned downtime. Physical inspections of network connections or analysis of network logs could also be used to document the network architecture, especially if the network is not large or complicated.

6.4.3 Manufacturing Profile Subcategories

ID.AM-3, ID.AM-4

6.5 Configuration Management

Configuration management tools enable a manufacturer to establish and maintain the integrity of manufacturing system hardware and software components by control of processes for initializing, changing, monitoring, and auditing the configurations of the components throughout the system development life cycle.

6.5.1 Security Benefit

Configuration management helps ensure that systems are deployed in a secure consistent state and maintain this state throughout their lifetime. It reduces the risk of outages due to configuration issues and security breaches through improved visibility and tracking changes to the system. In addition, it results in an improved experience for staff by detecting and correcting improper configurations that could negatively impact performance or security.

6.5.2 Potential System Impacts

Configuration management tools can potentially impact the manufacturing system. These tools transfer numerous different types of data over the manufacturing system network, as well as potentially large amounts of data. These tools may also impact manufacturing system operations by attempting to change configurations or manipulating active files within devices. Processes that validate configurations prior to deployment and during scheduled maintenance downtimes could be leveraged to minimize these impacts.

6.5.3 Manufacturing Profile Subcategories

ID.AM-3, ID.AM-4, PR.IP-1, PR.IP-4, PR.MA-1

6.6 Baseline Establishment

Baseline establishment tools enable a manufacturer to support the management of baseline configurations of the manufacturing system. The tools track information about the manufacturing system components (e.g. software license information, software version numbers, Human-Machine Interface (HMI) and other ICS component applications, software, operating systems), current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.

6.6.1 Security Benefit

The use of baselines is one of the methods used for implementing configuration management in an automated way. When systems are deployed in a secure state with a secure baseline, they are much more likely to be resistant to cybersecurity threats. Baselining results in efficient change management and improves ability to recover quickly from an outage or cybersecurity incident.

6.6.2 Potential System Impacts

Baseline establishment tools that use active scanning can potentially impact the manufacturing system. Care must be taken before using these tools on an operational system. Impacts could be due to the nature of the information or the volume of network traffic. Consider using baseline establishment tools that use active scanning during planned downtime.

6.6.3 Manufacturing Profile Subcategories

ID.AM-3, PR.IP-1, DE.AE-1, DE-CM-7

6.7 Change Control

Change control tools enable a manufacturer to document, track, and coordinate changes to manufacturing system hardware and software components.

6.7.1 Security Benefit

Changes often create unintended side effects that can cause outages or interruptions in operation. Many outages can be prevented with effective configuration and change control programs. A change control process ensures that changes are documented and appropriate personnel review and approve of changes.

6.7.2 Potential System Impacts

The creation, modification, and storage of change control documentation and procedures does not have the ability to impact the manufacturing system.

6.7.3 Manufacturing Profile Subcategories

PR.IP-1, PR.IP-3, PR.MA-1, DE.CM-7

6.8 Configuration Backups

Configuration backup tools enable a manufacturer to gather and archive configuration settings from hardware and software components within the manufacturing system, typically in a data format specified by the original equipment manufacturer (OEM) of the component.

6.8.1 Security Benefit

Configuration backups allow the manufacturer to restore device configuration settings from a known good state from a specific point in time. This is useful for quick recovery to a known operational state when incidents occur.

6.8.2 Potential System Impacts

Backup tools and methods used to obtain configuration backups can potentially impact the manufacturing system as they could utilize excessive processing power or network bandwidth, and sometimes require physical access to the device. Configuration backups should be planned around scheduled downtime.

6.8.3 Manufacturing Profile Subcategories

PR.IP-1, PR.IP-4

6.9 Data Backup

Data backup tools enable a manufacturer to collect and store files and programs from the manufacturing system to facilitate recovery after an incident.

6.9.1 Security Benefit

Data backups allow data to be restored from an earlier point in time to help organizations recover from incidents. These backups are an added layer of assurance in the case of a ransomware incident or hardware failure, ensuring critical data is backed up and stored offline. In addition, data recovered from backups can also be leveraged for forensic investigations.

6.9.2 Potential System Impacts

Backup tools and methods used to obtain data backups can potentially impact the manufacturing system as they could utilize excessive processing power or network bandwidth, and sometimes require physical access to the device. Remote backups typically require a software agent to be installed on the device. If possible, software agents should be configured to use the minimum amount of processing power required for proper operation. Network-based data backups should be configured to use the minimum amount of network bandwidth required for proper operation. Data backups should be planned around scheduled downtime if possible.

6.9.3 Manufacturing Profile Subcategories

PR.IP-4

6.10 Data Replication

Data replication tools enable a manufacturer to copy and transfer backup data to a physical location external to the manufacturing system.

6.10.1 Security Benefit

Data replication lets organizations store their data in multiple locations. Providing physical separation and offline storage locations increases assurance to the data's integrity. This can be accomplished via encryption tools that are used at both the hardware and software level thereby providing a guarantee to organizations that their data is safe from unauthorized access.

Replicating data to an offsite location makes the data disaster proof in the event of fire, flood or other natural or man-made disasters

6.10.2 Potential System Impacts

The duplication of data and configuration backups should not impact the manufacturing system as this operation is typically performed outside of the manufacturing system.

6.10.3 Manufacturing Profile Subcategories

PR.IP-4

6.11 Network Segmentation and Segregation

Network segmentation and segregation solutions enable a manufacturer to separate the manufacturing system network from other networks (e.g., corporate networks, guest networks), segment the internal manufacturing system network into smaller networks, and control the communication between specific hosts and services.

6.11.1 Security Benefit

Properly segmenting a network provides increased access control, making it easier for IT administrators to restrict and monitor user access to systems. Network segmentation and segregation can help limit the scope of an incident and also improve network performance because broadcast domain traffic can be minimized.

6.11.2 Potential System Impacts

Network segmentation and segregation can potentially impact the manufacturing system. Care must be taken when planning and deploying network segmentation and segregation. Increased network latency may occur, depending on the topology, hardware, and configuration of network devices.

6.11.3 Manufacturing Profile Subcategories

PR.AC-5

6.12 Network Boundary Protection

Network boundary protection solutions enable a manufacturer to restrict data communication traffic to and from manufacturing system network(s). Network boundary protection capabilities include, but are not limited to, the use of firewalls, demilitarized zones (DMZ), and intrusion detection and prevention systems.

6.12.1 Security Benefit

Firewalls allow organizations to segment their networks, restricting access to only authorized connections. These devices monitor and log traffic accessing or attempting to access the network. This functionality provides forensic data that can be critical for response and recovery activities. More advanced firewalls, commonly called Next Generation Firewalls (NGFW), include antivirus and malware protection with datasets continuously upgraded to detect new threats. These NGFWs can provide other advanced security protections such as intrusion detection, deep packet inspection, virtual private network (VPN) services, and denial of service protection. The physical and logical isolation characteristics of a DMZ are important because they enable access only to designated servers and information stored within the isolated DMZ with no visibility directly into the sensitive manufacturing network. Having a DMZ network reduces and controls access to those internal systems from outside of the organization. Intrusion detection and prevention systems can monitor, detect, analyze, and prevent unauthorized network or system access.

6.12.2 Potential System Impacts

Network boundary protections can potentially impact the manufacturing system. Care must be taken when planning and deploying network boundary protections. Increased network latency may be caused by in-line boundary protection devices (e.g., firewalls), especially if the capabilities of the device and network do not match (e.g., a 100 Mbps Ethernet device on a 1 Gbps network).

6.12.3 Manufacturing Profile Subcategories

PR.AC-5, PR.PT-4, DE.CM-1

6.13 Secure Remote Access

Secure remote access solutions enable a manufacturer to establish secure communications channels through which information can be transmitted over untrusted networks, including public networks such as the Internet.

6.13.1 Security Benefit

Establishing these secure communications channels or encrypted tunnels allows a manufacturer to grant access to sensitive components in the manufacturing system for outside entities that can be used for activities including vendor upgrades, technical support, and remote employee access. When accessing the manufacturing system through a secure channel like a Virtual Private Network (VPN), data is encrypted and protected from a potential malicious actor.

More advanced implementations of this capability might use Secure Socket Layer (SSL) based VPNs that perform security health checks on remote access devices, ensuring infected machines are not accessing critical system components.

6.13.2 Potential System Impacts

Secure remote access solutions can potentially impact the manufacturing system. Care must be taken if remote access is permitted while the manufacturing system is operational. Activities performed over a remote access connection may generate excessive network traffic. Remote access for maintenance activities should be tightly controlled and planned around scheduled downtime.

6.13.3 Manufacturing Profile Subcategories

PR.AC-5, PR.MA-2

6.14 Managed Network Interfaces

Managed network interface solutions enable a manufacturer to control connections and information transmitted and received through individual physical ports on a network device.

6.14.1 Security Benefit

Managed network interfaces provide control over what is connected to a specific network and is critical to ensure unauthorized devices cannot be easily added to a network. When an unauthorized device is plugged into the network interface the managed interface will not send traffic until the port has been configured. Managed interfaces help ensure only identified devices can send traffic over a network.

6.14.2 Potential System Impacts

Managed network interface solutions can potentially impact the manufacturing system. Managed network interfaces can increase complexity during maintenance activities (e.g., upgrading network-based components, connecting maintenance computers to a local network).

6.14.3 Manufacturing Profile Subcategories

PR.AC-5

6.15 Map Data Flows

Data flow diagrams enable a manufacturer to understand the flow of data between networked components of the manufacturing system.

6.15.1 Security Benefit

Documenting data flows enables organizations to understand 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.

6.15.2 Potential System Impacts

Data flow mapping tools that use active scanning or require network monitoring tools (e.g., such in-line network probes) can potentially impact the manufacturing system. Care must be taken before using these tools to identify data flows on an operational system. Impacts could be due to the nature of the information, the volume of network traffic, or momentary disconnection of manufacturing system components from the network. Consider using data flow mapping tools that utilize these methods during planned downtime.

6.15.3 Manufacturing Profile Subcategories

ID.AM-3, ID.AM-4, PR.AC-5, DE.AE-1

6.16 Time Synchronization

Time synchronization solutions enable a manufacturer to synchronize time for all manufacturing system components to generate accurate timestamps.

6.16.1 Security Benefit

Time synchronization is critical for authentication protocols such as Kerberos in order to prevent replay attacks. Time synchronization is also useful when correlating events or logs for investigation purposes.

6.16.2 Potential System Impacts

Time synchronization should not impact the manufacturing system, but the effects of unsynchronized time or misconfigurations can potentially impact services that require the time to be synchronized.

6.16.3 Manufacturing Profile Subcategories

PR.PT-1

6.17 Credential Management

Credential management tools enable a manufacturer to manage the life cycle of user authentication and authorization credentials.

6.17.1 Security Benefit

Credential management tools enable manufacturers to securely store and perform lifecycle management activities of credentials such as required password changes, defining privilege levels on a per user basis and the capability to revoke credentials. Some credentials management solutions minimize the attack surface by eliminating static and long-lived privilege grants.

6.17.2 Potential System Impacts

Credential management tools should not impact the manufacturing system, as they are not typically installed or operated within the manufacturing system. Updates to credentials should not be deployed while the manufacturing system is operational. Solutions that can automatically rotate credentials should be configured to only change credentials during scheduled maintenance downtimes.

6.17.3 Manufacturing Profile Subcategories

PR.AC-1, PR.MA-1, PR.MA-2

6.18 Authentication and Authorization

Authentication and authorization tools enable a manufacturer to verify user identities and enforce the principles of least privilege. The tools and techniques supporting authentication and authorization enable a manufacturer to set user privileges and positively determine if a user has permission to access a system resource. Where feasible, centralized authentication and authorization mechanisms should be considered as part of the system architecture.

6.18.1 Security Benefit

With a centralized authentication system, users can access systems through a single set of login credentials. Additionally, centralized authentication and authorization functionality on a single platform provides authorized administrators with a consistent method for managing user access. Least privilege ensures users and programs are given only the permissions required to perform their task.

6.18.2 Potential System Impacts

Authentication and authorization tools can potentially impact the manufacturing system. These tools typically require a software agent to be installed on the device or require network processes that might induce latency or interrupt manufacturing processes. Backup authentication and authorization servers should be considered to prevent operator “loss of view” and “loss of control” incidents. Manufacturers should determine where authentication and authorization are not advisable for performance, safety, or reliability reasons.

6.18.3 Manufacturing Profile Subcategories

PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

6.19 Anti-virus/malware

Anti-virus/malware tools enable a manufacturer to monitor computing devices to identify major types of malware and prevent or contain malware incidents.

6.19.1 Security Benefit

Malware is the most common threat for many manufacturers. Anti-virus/malware tools can protect devices from being infected with malware, such as ransomware, viruses, worms, trojans, and malicious mobile code.

6.19.2 Potential System Impacts

Anti-virus/malware tools can potentially impact the manufacturing system. Anti-virus/malware tools may require a software agent to be installed on the device or may perform authenticated scanning via the network. If possible, these tools should be configured to use the minimum amount of processing power required for proper operation. Anti-virus/malware tools that utilize network-based authenticated scanning may generate excessive network traffic. These tools should be configured to use the minimum amount of network bandwidth required for proper operation. It is recommended that scans be planned around scheduled downtime.

6.19.3 Manufacturing Profile Subcategories

DE.CM-4

6.20 Risk Assessment

Risk assessment tools enable a manufacturer to perform risks assessments of the manufacturing system.

6.20.1 Security Benefit

A risk assessment will evaluate an organization’s security posture by considering external and internal threats. In doing so, a risk assessment will identify current security vulnerabilities, control gaps, and noncompliance with standards. It is performed either via audits consisting of surveys, discussions, and/or questionnaires. Risk assessments are part of an overall risk management process, providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. The results of these assessments can be leveraged to create awareness amongst employees and be used as a training tool as well. Performing regular risk assessments can reduce incidents in the workplace.

6.20.2 Potential System Impacts

Risk assessment tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system.

6.20.3 Manufacturing Profile Subcategories

ID.RA-1

6.21 Vulnerability Scanning

Vulnerability scanning tools enable a manufacturer to scan, detect, and identify software flaws or misconfigurations that cause a weakness in the security of the manufacturing system.

6.21.1 Security Benefit

Identification of known security vulnerabilities present in the manufacturing network can be used to help inform patch management activities.

6.21.2 Potential System Impacts

Vulnerability scanning tools can impact an operational system. Vulnerability scanning tools may require a software agent to be installed on the device or may perform authenticated scanning via the network. Vulnerability scanning tools may generate excessive network traffic or, in extreme cases, cause device failures due to the intrusive methods used during scanning. These tools should be configured to use the minimum amount of network bandwidth required for proper operation. It is recommended that scans be planned around scheduled downtime and not be performed while the manufacturing system is operational.

6.21.3 Manufacturing Profile Subcategories

ID.RA-1, DE.CM-8

6.22 Vulnerability Management

Vulnerability management tools enable a manufacturer to document, manage, and mitigate vulnerabilities discovered in the manufacturing system.

6.22.1 Security Benefit

Vulnerability management tools allow a manufacturer to apply security updates to its systems and identify where compensating controls are needed to protect equipment that cannot be updated.

6.22.2 Potential System Impacts

Vulnerability management can potentially impact the manufacturing system. A patch may remove a vulnerability, but it can also introduce a risk from a production or safety perspective.

Patching a vulnerability may also change the way the operating system or application functions. It is recommended to consult with the product vendor to see if they have a list of approved patches and a vulnerability management process. It is recommended that vulnerability management be planned around scheduled downtime and integrated with the system development lifecycle, configuration management, and change management processes.

6.22.3 Manufacturing Profile Subcategories

ID.RA-1, DE.CM-4, RS.MI-3

6.23 Incident Management

Incident management tools enable a manufacturer to document, track, and coordinate the mitigation of an adverse event in manufacturing system devices or networks.

6.23.1 Security Benefit

Incident management tools enable manufacturers to minimize downtimes due to incidents and increase the efficiency and productivity of the manufacturing system. Information gained during incident handling can be used to better prepare for handling any future incident. Incident response plans enable organizations to act proactively before an incident or immediately after an incident is noticed to limit the impact from incidents.

6.23.2 Potential System Impacts

Incident management tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system.

6.23.3 Manufacturing Profile Subcategories

RS.MI-2, RS.MI-3

6.24 Network Monitoring

Network monitoring tools enable a manufacturer to capture, store, and audit network traffic from the manufacturing system networks, and monitor for indicators of potential cybersecurity incidents.

6.24.1 Security Benefit

Network monitoring tools can identify suspicious traffic and other threat vectors, allowing manufacturers to respond fast to an incident. They can help to reduce incidents caused by human error, configuration issues and other environmental factors. Effective network monitoring helps to detect, diagnose, and resolve network performance issues, reducing incidents by proactively identifying threats and bottlenecks.

6.24.2 Potential System Impacts

Network monitoring tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system. However, certain methods of capturing network traffic (e.g., in-line network probes, mirror ports) can increase processing load on network devices and can increase network latency.

6.24.3 Manufacturing Profile Subcategories

PR.DS-5, PR.MA-2, PR.PT-4, DE.CM-1, DE.CM-6, DE.CM-7

6.25 System Use Monitoring

System use monitoring solutions enable a manufacturer to monitor, store, audit, and restrict the activities of manufacturing system users.

6.25.1 Security Benefit

Monitoring systems and users within the manufacturing system helps to ensure users and systems are behaving as expected. This capability can also aid in troubleshooting when an issue occurs by providing information about which users were working within the system during the time period. Monitoring also helps show if there are misconfigurations or other potential errors introduced in the manufacturing system.

6.25.2 Potential System Impacts

System use monitoring tools can potentially impact the manufacturing system. These tools typically require a software agent to be installed on the device, utilizing processing power and network bandwidth. If possible, software agents should be configured to use the minimum amount of processing power required for proper operation.

6.25.3 Manufacturing Profile Subcategories

PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

6.26 Maintenance Tracking

Maintenance tracking solutions enable a manufacturer to schedule, track, authorize, monitor, and audit maintenance and repair activities to manufacturing system computing devices.

6.26.1 Security Benefit

Tracking changes to devices within the manufacturing system ensures any maintenance logs or changes performed are properly documented. Tracking these events provides an audit trail that can aid in troubleshooting, response, and recovery activities. Maintenance tracking can provide visibility into when components should be serviced and help inform end of life decisions. This type of tracking can also enable coordination in advance as to not cause disruption within the manufacturing system.

6.26.2 Potential System Impacts

Maintenance tracking tools should not impact the manufacturing system, as they are typically operated and accessed outside of the manufacturing system.

6.26.3 Manufacturing Profile Subcategories

PR.MA-1, PR.MA-2

6.27 Physical Access Control

Physical access control solutions enable a manufacturer to deny or restrict access to the manufacturing system by unauthorized individuals.

6.27.1 Security Benefit

Limiting physical access to only authorized individuals protects the manufacturing system from malicious actors gaining physical access to critical components. These protections also help prevent accidental or unintentional damage.

6.27.2 Potential System Impacts

Physical access control tools should not impact the manufacturing system.

6.27.3 Manufacturing Profile Subcategories

PR.AC-2, PR.DS-5, PR.MA-1

6.28 Physical Access Monitoring

Physical access monitoring solutions enable a manufacturer to record, monitor, archive, and audit physical access to the manufacturing system by all individuals.

6.28.1 Security Benefit

The ability to record, monitor, archive and audit physical access to the manufacturing facility and locations provides visibility into the physical presence of individuals. These logs can be correlated to help identify malicious threat actors and other harmful activity.

6.28.2 Potential System Impacts

Physical access monitoring tools should not impact the manufacturing system.

6.28.3 Manufacturing Profile Subcategories

PR.AC-2, PR.PT-1, DE.CM-2, DE.CM-3

6.29 Ports and Services Lockdown

Ports and services lockdown solutions enable a manufacturer to discover and disable nonessential physical and logical network ports and services.

6.29.1 Security Benefit

The ability to discover and disable unused physical ports within the manufacturing system will prevent rogue devices from being able to connect to the network. These types of devices could create a potential entry point for malicious threat actors. A comprehensive understanding of which logical ports are in use and the services required within the network provides additional defense in depth protection.

6.29.2 Potential System Impacts

Locking-down ports and services can potentially impact the manufacturing system. Care must be taken to understand the role of all ports and services before they are disabled to verify they are not required for manufacturing system operations.

6.29.3 Manufacturing Profile Subcategories

PR.IP-1, PR.PT-3

6.30 Media Protection

Media protection solutions enable a manufacturer to restrict the use of portable media within the manufacturing system.

6.30.1 Security Benefit

Media protection solutions reduce the threat of unknown and potentially malicious devices from being connected to the manufacturing system equipment.

6.30.2 Potential System Impacts

Media protection solutions can potentially impact the manufacturing system. Media protection for privileged users may be impactful to the manufacturing system by limiting their ability to respond to a manufacturing system event or incident. Care must be taken to verify privileged users have the access required to perform their roles and functions.

6.30.3 Manufacturing Profile Subcategories

PR.PT-2

6.31 Encryption

Encryption solutions enable a manufacturer to protect sensitive manufacturing system data so that only authorized users can access it.

6.31.1 Security Benefit

Encryption provides data confidentiality when data is in use, in transit or at rest by converting plaintext into ciphertext that can only be viewed by recipients having the correct keys. If data is compromised or leaked, the likelihood of sensitive information being exposed would be minimized.

6.31.2 Potential System Impacts

Tools that perform methods of encryption can potentially impact the manufacturing system. Computational operations to encrypt and decrypt data require processing power and memory. These effects can be exacerbated when they are executed on embedded devices. Depending on the encryption and decryption methods used, time-sensitive data communications may also be impacted. Additionally, physical network hardware used to encrypt traffic between multiple devices may increase network latency. While encryption is an effective data confidentiality and integrity tool, the implementation must be carefully planned to minimize any potential disruption to the manufacturing processes.

6.31.3 Manufacturing Profile Subcategories

PR.DS-5

6.32 Data Loss Prevention

Data loss prevention solutions enable a manufacturer to detect and prevent the unauthorized access and transmission of sensitive manufacturing system data.

6.32.1 Security Benefit

Detects and prevents exposure of sensitive information across network devices.

6.32.2 Potential System Impacts

Network-based data loss prevention tools that monitor and detect data loss should not typically impact the manufacturing system. Endpoint-based data loss prevention tools can potentially impact the manufacturing system, as they utilize processing power and/or network bandwidth. If possible, these tools should be configured to use the minimum amount of processing power required for proper operation.

6.32.3 Manufacturing Profile Subcategories

PR.DS-5

6.33 Media Sanitization

Media sanitization solutions enable a manufacturer to render data written on media unrecoverable.

6.33.1 Security Benefit

Media sanitization solutions ensure confidential information is removed or destroyed from any device containing storage media (e.g., USB flash drives, internal or external hard drives, memory cards). Devices not sanitized appropriately can become a security concern when decommissioned items are no longer in the company's possession.

6.33.2 Potential System Impacts

Media sanitization tools should not impact the manufacturing system, as they are typically operated outside of the manufacturing system. These processes should be integrated with the configuration and change management processes to ensure accountability and tracking of the components.

6.33.3 Manufacturing Profile Subcategories

PR.DS-3, PR-IP-6

6.34 Event Logging

Event logging solutions enable a manufacturer to capture, store, archive, and audit the events occurring within the manufacturing system and its networks.

6.34.1 Security Benefit

Event logging provides important information regarding operations of the system. This information can aid in improving reporting, log collection, analysis, and can help prevent security breaches. Robust logging capabilities help meet any compliance requirements as well as reduce the impact of security incidents.

6.34.2 Potential System Impacts

Event logging solutions can potentially impact the manufacturing system. For the event logger to operate properly, devices within the manufacturing system must generate messages destined for the logger. Network bandwidth will be consumed to send these messages, and the amount of traffic is highly dependent on the number of hosts and the configured logging level (e.g., critical errors, warnings, debug). A risk-based decision must be made between the amount of consumed network bandwidth and the desired logging level. Processing load may increase on devices that send a large number of messages to the event logger.

6.34.3 Manufacturing Profile Subcategories

PR.PT-1, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

6.35 Forensics

Forensic solutions enable a manufacturer to identify, collect, examine, and analyze data from the manufacturing system to determine the cause of an incident.

6.35.1 Security Benefit

Collection of forensics-related data within a network environment provides the ability to examine network data for additional evidence needed to determine malicious activities and identify potential actors. Collections of device and network logs can help identify threat actors for prosecution. Forensics-related data are also useful if the incident requires help from an outside incident response company.

6.35.2 Potential System Impacts

Forensic tools should not impact the manufacturing system, as they are typically operated outside of the manufacturing system.

6.35.3 Manufacturing Profile Subcategories

DE.AE-2, RS.AN-3

			Hardware Inventory	Software Inventory	Systems Development Lifecycle Management	Network Architecture Documentation	Configuration Management	Baseline Establishment	Change Control	Configuration Backups	Data Backup	Data Replication	Network Segmentation and Segregation	Network Boundary Protection	Secure Remote Access	Managed Network Interfaces	Map Data Flows	Time Synchronization	Credential Management	Authentication and Authorization	Anti-virus/malware	Risk Assessment	Vulnerability Scanning	Vulnerability Management	Incident Management	Network Monitoring	System Use Monitoring	Maintenance Tracking	Physical Access Control	Physical Access Monitoring	Ports and Services Lockdown	Media Protection	Encryption	Data Loss Prevention	Media Sanitization	Event Logging	Forensics
ID	Asset Management	ID.AM-1 |●|																																			
		ID.AM-2	|●|																																		
		ID.AM-3				●	●	●									●																				
		ID.AM-4				●	●										●																				
	Risk Assessment	ID.RA-1																				●	●	●													
PR	Access Control	PR.AC-1																	●	●							●										
		PR.AC-2																											●	●							
		PR.AC-5											●	●	●	●	●																				
	Data Security	PR.DS-3	●	●	●																														●		
		PR.DS-5																							●	●		●				●	●			
	Information Protection Processes and Procedures	PR.IP-1			●		●	●	●	●																					●						
		PR.IP-2			●																																
		PR.IP-3						●																													
		PR.IP-4					●			●	●	●																									
		PR.IP-6			●																														●		
	Maintenance	PR.MA-1					●		●										●	●								●	●								
		PR.MA-2													●				●	●						●	●	●									
	Protective Technology	PR.PT-1																●												●						●	
		PR.PT-2																														●					
		PR.PT-3																		●											●						
		PR.PT-4												●						●						●											
DE	Anomalies and Events	DE.AE-1						●									●																				
		DE.AE-2																																			●
		DE.AE-3																																		●	
	Security Continuous Monitoring	DE.CM-1												●												●										●	
		DE.CM-2																											●								
		DE.CM-3																		●							●			●							
		DE.CM-4																			●			●													
		DE.CM-6																								●										●	
		DE.CM-7	●	●	●			●	●																	●											
		DE.CM-8																					●														
	Detection Processes	DE.DP-3																																		●	
RS	Analysis	RS.AN-3																																		●	●
	Mitigation	RS.MI-2																							●												
		RS.MI-3																						●	●												

Table 6-1. Mapping of CSF Manufacturing Profile Subcategories to Technical Capabilities

Table 6-1 summarizes the information discussed in this Section and shows the coverage of CSF Manufacturing Profile Subcategories addressed when the technical capabilities are implemented as part of a cybersecurity program.

7. Capabilities Mapping to Manufacturing Profile

This section examines the policies and procedures, described in Section 5, and/or technical solutions, described in Section 6, required to meet the language specified in each particular Subcategory, and lists potential solutions that fulfil the requirements that are accessible by small manufacturers. Accessibility criteria included cost, ease of use, and level of effort to implement. The list of potential solutions is not intended to be all inclusive, but to provide examples. Specific solutions that were implemented in the lab environment for each use case are included in Volume 2 and Volume 3.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	**Asset Management (ID.AM)**	**ID.AM-1**	**Low** Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.	These Subcategory requirements can be met by implementing solutions that provide the **Hardware Inventory** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, Nmap, LANSweeper, Spiceworks, OCSinventory-ng, Excel (manual entry) Solutions that were implemented in use cases: Open-AudIT
		ID.AM-2	**Low** Document an inventory of manufacturing system software components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, HMI and other ICS component applications, software, operating systems. System software inventory is reviewed and updated as defined by the organization.	These Subcategory requirements can be met by implementing solutions that provide the **Software Inventory** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, Nmap, LANSweeper, Spiceworks, OCSinventory-ng, Excel (manual entry) Solutions that were implemented in use cases: Open-AudIT

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	**Asset Management (ID.AM)**	**ID.AM-3**	**Low** Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.	These Subcategory requirements can be met by implementing solutions that provide the **Network Architecture Documentation, Configuration Management, Baseline Establishment, and Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: GRASSMARLIN, Microsoft Visio, Wireshark, Nmap, Open-AudIT, Tenable Nessus, Ntopng Solutions that were implemented in use cases GRASSMARLIN Microsoft Visio Wireshark Open-AudIT
		ID.AM-4	**Low** Identify and document all external connections for the manufacturing system. Examples of external systems include engineering design services, and those that are controlled under separate authority, personal devices, and other hosted services.	These Subcategory requirements can be met by implementing solutions that provide the **Network Architecture Documentation, Configuration Management, and Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: GRASSMARLIN, Microsoft Visio, Wireshark, Nmap, Open-AudIT, Tenable Nessus, Ntopng Solutions that were implemented in use cases GRASSMARLIN Microsoft Visio Wireshark Open-AudIT

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	**Asset Management (ID.AM)**	**ID.AM-5**	**Low** Identify and prioritize manufacturing system components and functions based on their classification, criticality, and business value. Identify the types of information in possession, custody, or control for which security safeguards are needed (e.g. sensitive or protected information).	These Subcategory requirements can be met by developing policies and procedures in the **Asset Criticality Matrix** section of the **Risk Management** document
		ID.AM-6	**Low** Establish and maintain personnel cybersecurity roles and responsibilities for the manufacturing system. Include cybersecurity roles and responsibilities for third-party providers. Third-party providers are required to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the manufacturing system components. Third-party providers include, for example, service providers, contractors, and other organizations providing manufacturing system development, technology services, outsourced applications, or network and security management.	These Subcategory requirements can be met by developing policies and procedures in the **Role-based Security Responsibilities** section of the cybersecurity policy document
	Business Environment (ID.BE)	**ID.BE-1**	**Low** Define and communicate the organization's role in the supply chain. Identify the upstream and downstream supply channels that are outside of the organization's operations. Identify the overall mission supported by the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** section of the **Cybersecurity Program** document.
		ID.BE-2	**Low** Define and communicate the manufacturer's place in critical infrastructure and its industry sector. Define and communicate critical infrastructure and key resources relevant to the manufacturing system. Develop, document, and maintain a critical infrastructure and key resources protection plan.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** section of the **Cybersecurity Program** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	Business Environment (ID.BE)	ID.BE-3	**Low** Establish and communicate priorities for manufacturing missions, objectives, and activities with consideration for security and the resulting risk to manufacturing operations, components, and individuals. Identify critical manufacturing system components and functions by performing a criticality analysis.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** section of the **Cybersecurity Program** document.
		ID.BE-4	**Low** Identify and prioritize supporting services for critical manufacturing system processes and components. Provide an uninterruptable power supply for identified critical manufacturing system components to facilitate the transition of the manufacturing system to long-term alternate power in the event of a primary power source loss.	These Subcategory requirements can be met by developing policies and procedures in the **Organization Overview** and **Emergency Power** sections of the **Cybersecurity Program** document.
		ID.BE-5	**Low** Establish resilience requirements for the manufacturing system to support delivery of critical services.	These Subcategory requirements can be met by developing policies and procedures in the **System Recovery** document.
	Governance (ID.GV)	ID.GV-1	**Low** Develop and disseminate a security policy that provides an overview of the security requirements for the manufacturing system. The policy includes, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the manufacturing system. Review and update the security policy as determined necessary. Ensure the security policy is approved by a senior official with responsibility and accountability for the risk being incurred by manufacturing operations.	These Subcategory requirements can be met by developing policies and procedures in the **Cybersecurity Policy** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	Governance (ID.GV)	ID.GV-2	**Low** Develop and disseminate a security program for the manufacturing system that includes, for example, the identification of personnel security roles and assignment of responsibilities, management commitment, coordination among organizational entities, and compliance. This includes security requirements, roles and responsibilities for third-party providers. Review and update the security program as determined necessary.	These Subcategory requirements can be met by developing policies and procedures in the **Cybersecurity Program** document.
		ID.GV-3	**Low** Ensure that legal and regulatory requirements affecting the manufacturing operations regarding cybersecurity are understood and managed.	These Subcategory requirements can be met by developing policies and procedures in the **Applicable Laws and Regulations** section of the **Cybersecurity Program** document.
		ID.GV-4	**Low** Develop a comprehensive strategy to manage risk to manufacturing operations. Include cybersecurity considerations in the risk management strategy. Review and update the risk management strategy as determined necessary. Determine and allocate required resources to protect the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Management** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	**Risk Assessment (ID.RA)**	**ID.RA-1**	**Low** Develop a plan to identify, document, and report vulnerabilities that exist on the manufacturing system. Include the use of vulnerability scanning where safe and feasible on the manufacturing system, its components, or a representative system.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Risk Assessment, Vulnerability Scanning and Vulnerability Management** technical capabilities. Potential solutions for meeting these Subcategory requirements include: DHS Cybersecurity Evaluation Tool (CSET), NamicSoft, OpenVAS, Tenable Nessus, AlienVault OSSIM, Microsoft Excel (Manual) Solutions that were implemented in use cases: CSET NamicSoft Tenable Nessus Some of these Subcategory requirements can be met by developing policies and procedures in the **Vulnerability Management** section of the **Cybersecurity Operations** document.
		ID.RA-2	**Low** Establish and maintain ongoing contact with security groups and associations, and receive security alerts and advisories. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Implement a threat awareness program that includes a cross-organization information-sharing capability. Organizations should consider having both an unclassified and classified information sharing capability. Collaborate and share information about potential vulnerabilities and incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC) [6] serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [7] collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.	These Subcategory requirements can be met by developing policies and procedures in the **Information Sharing Plan** and **Security Awareness Training** sections **o**f the **Cybersecurity Program** document, **Risk Identification** section of the **Risk Management** document, and **Information Sharing Policy** section of the **Incident Response Plan** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
IDENTIFY	Risk Assessment (ID.RA)	ID.RA-3	**Low** Conduct and document periodic assessment of risk to the manufacturing system that takes into account threats and likelihood of impact to manufacturing operations and assets. The risk assessment includes threats from insiders and external parties.	These Subcategory requirements can be met by developing policies and procedures in the **Risk, Monitor and Control** section of the **Risk Management** document.
		ID.RA-4	**Low** Conduct criticality reviews of the manufacturing system that define the potential adverse impacts to manufacturing operations, assets, and individuals if compromised or disabled.	These Subcategory requirements can be met by developing policies and procedures in the **Periodic Reviews** section of the **Risk Management** document.
		ID.RA-5	**Low** Conduct risk assessments of the manufacturing system incorporating threats, vulnerabilities, likelihood, and impact to manufacturing operations, assets, and individuals. Disseminate risk assessment results to relevant stakeholders.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Monitor and Control** and **Risk Reporting** sections of the **Risk Management** document.
		ID.RA-6	**Low** Develop and implement a comprehensive strategy to manage risk to the manufacturing system that includes the identification and prioritization of risk responses.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Management** document.
	Risk Management Strategy (ID.RM)	ID.RM-1	**Low** Establish a risk management process for the manufacturing system that effectively identifies, communicates, and facilitates addressing risk-related issues and information among key stakeholders internally and externally.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Notification Process** section of the **Risk Management** document.
		ID.RM-2	**Low** Define the risk tolerance for the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Tolerance** section of the **Risk Management** document.
		ID.RM-3	**Low** Ensure the risk tolerance for the manufacturing system is informed by the organization's role in critical infrastructure and sector-specific risk analysis.	These Subcategory requirements can be met by developing policies and procedures in the **Risk Tolerance** section of the **Risk Management** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	Access Control (PR.AC)	PR.AC-1	**Low** Establish and manage identification mechanisms and credentials for users and of the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Credential Management, Authentication and Authorization, and System Use Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Microsoft Active Directory, FreeIPA, OpenLDAP, native operating system/device capabilities. Solutions that were implemented in use cases: Microsoft Active Directory Native operating system/device capabilities
		PR.AC-2	**Low** Protect physical access to the manufacturing facility. Determine access requirements during emergency situations. Maintain and review visitor access records to the facility where the manufacturing system resides. Physical access controls may include, for example, lists of authorized individuals, identity credentials, escort requirements, guards, fences, turnstiles, locks, monitoring of facility access.	These Subcategory requirements can be met by implementing solutions that provide the **Physical Access Control and Physical Access Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: lists of authorized individuals, sign in/out sheets, identity credentials, escort requirements, guards, fences, turnstiles, locks, electronic access control systems, cameras, monitoring of facility access. Solutions that were implemented in use cases: Locks Fences Electronic Access Control System Sign in/out sheet
		PR.AC-3	**Low** Establish usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the manufacturing system. Provide an explicit indication of active remote access connections to users physically present at the devices. Remote access methods include, for example, wireless, dial-up, broadband, VPN connections, mobile device connections, and communications through external networks.	These Subcategory requirements can be met by developing policies and procedures in the **Remote Access** section of the cybersecurity policy document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	Access Control (PR.AC)	PR.AC-4	**Low** Define and manage access permissions for users of the manufacturing system. Identify and document user actions that can be performed on the manufacturing system without identification or authentication (e.g. during emergencies).	These Subcategory requirements can be met by developing policies and procedures in the **Personnel Actions** section of the **Cybersecurity Operations** document.
		PR.AC-5	**Low** Protect network integrity of the manufacturing system, incorporating network segmentation and segregation where appropriate. Identify and control connections between system components. Monitor and control connections and communications at the external boundary and at key internal boundaries within the manufacturing system. Employ boundary protection devices. Boundary protection mechanisms include, for example, routers, gateways, unidirectional gateways, data diodes, and firewalls separating system components into logically separate networks or subnetworks.	These Subcategory requirements can be met by implementing solutions that provide the **Network Segmentation and Segregation, Network Boundary Protection, Secure Remote Access, Managed Network Interfaces, Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: routers, gateways, unidirectional gateways, data diodes, firewalls, DMZ, switches, SNORT, BRO, VPNs, remote desktops, Native operating system/device capabilities, GRASSMARLIN, Microsoft Visio, Wireshark, Ntopng Solutions that were implemented in use cases: Routers Firewalls DMZ Switches VPNs TeamViewer Native operating system/device capabilities GRASSMARLIN Microsoft Visio Wireshark
	Awareness and Training (PR.AT)	PR.AT-1	**Low** Provide security awareness training for all manufacturing system users and managers. Training could include, for example, a basic understanding of the protections and user actions needed to maintain security of the system, responding to suspected cybersecurity incidents, and awareness of operational security.	These Subcategory requirements can be met by developing policies and procedures in the **Security Awareness Training** section of the **Cybersecurity Program** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	**Awareness and Training (PR.AT)**	**PR.AT-2**	**Low** Ensure that users with privileged access to the manufacturing system understand the requirements and responsibilities of their assignments. Establish standards for measuring, building, and validating individual qualifications for privileged users.	These Subcategory requirements can be met by developing policies and procedures in the **Security Awareness Training** section of the **Cybersecurity Program** document.
		PR.AT-3	**Low** Establish and enforce security requirements for third-party providers and users. Ensure that third-party providers understand their responsibilities regarding the security of the manufacturing system and the responsibilities of their assignments. Require notifications be given for any personnel transfers, termination, or transition involving personnel with physical or logical access to the manufacturing system components. Ensure that providers of external system services comply with defined security requirements. Monitor and audit external service providers for security compliance.	These Subcategory requirements can be met by developing policies and procedures in the **Security Awareness Training and Third party responsibilities and requirements** section of the **Cybersecurity Program** document.
		PR.AT-4	**Low** Ensure that senior executives understand the requirements for the security and protection of the manufacturing system, and their responsibilities for achieving them.	These Subcategory requirements can be met by developing policies and procedures in the **Commitment from Management** section of the **Cybersecurity Program** document.
		PR.AT-5	**Low** Ensure that personnel responsible for the physical protection and security of the manufacturing system and facility are trained for, and understand their responsibilities. Establish standards for measuring, building, and validating individual qualifications for physical security personnel.	These Subcategory requirements can be met by developing policies and procedures in the **Employee Requirements** section of the cybersecurity policy document.
	Data Security (PR.DS)	**PR.DS-1**	**Low** None	N/A
		PR.DS-2	**Low** None	N/A

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	Data Security (PR.DS)	PR.DS-3	**Low** Enforce accountability for all manufacturing system components throughout the system lifecycle, including removal, transfers, and disposition. Sanitize portable media prior to disposal, release, or reuse. All system components entering and exiting the facility are authorized, monitored, and controlled, and records are maintained of those items.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Hardware Inventory, Software Inventory, Systems Development Lifecycle Management, and Media Sanitization** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, AlienVault OSSIM, MS Excel (Manual), media sanitization tools. Solutions that were implemented in use cases: Open-AudIT DBAN Some of these Subcategory requirements can be met by developing policies and procedures in the **Lifecycle Accountability of Devices** section of the **Cybersecurity Policy** document and **Media Sanitization** section of the **Cybersecurity Operations** document.
		PR.DS-4	**Low** Ensure that adequate resources are maintained for manufacturing system information processing, networking, telecommunications, and data storage. Off-load audit records from the manufacturing system for processing to an alternate system.	These Subcategory requirements can be met by developing policies and procedures in the **Monitoring the Manufacturing System** and **Resources are Maintained** sections of the **Cybersecurity Operations** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	Data Security (PR.DS)	PR.DS-5	**Low** Protect the manufacturing system against data leaks. Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use. Develop and document access agreements for all users of the manufacturing system.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Network Monitoring, System Use Monitoring, Physical Access Control, Encryption, and Data Loss Prevention** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Security Onion, SNORT, Suricata, Zeek Network Security Monitor, Native operating system/device capabilities, lists of authorized individuals, sign in/out sheets, identity credentials, escort requirements, guards, fences, turnstiles, locks, electronic access control systems, cameras, monitoring of facility access, Microsoft EFS, Microsoft BitLocker, AxCrypt, VeraCrypt, GTB Inspector, Comodo DOME Solutions that were implemented in use cases: Security Onion Microsoft EFS Locks Fences Electronic Access Control System Sign in/out sheets GTB Inspector VeraCrypt Some of these Subcategory requirements can be met by developing policies and procedures in the **User Access Agreement** section of the **Cybersecurity Policy** document.
		PR.DS-6	**Low** None	N/A
		PR.DS-7	**Low** None	N/A

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	**Information Protection Processes and Procedures (PR.IP)**	**PR.IP-1**	**Low** Develop, document, and maintain a baseline configuration for the manufacturing system. Baseline configurations include for example, information about manufacturing system components (e.g. software license information, software version numbers, HMI and other ICS component applications, software, operating systems), current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Configure the manufacturing system to provide only essential capabilities. Review the baseline configuration and disable unnecessary capabilities.	These Subcategory requirements can be met by implementing solutions that provide the **Systems Development Lifecycle Management, Configuration Management, Baseline Establishment, Change Control, Configuration Backups, and Ports and Services Lockdown** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, Microsoft Excel (Manual), I-doit, Salt, Puppet, Ansible, GRASSMARLIN, Wireshark, Nmap and Native operating system/device capabilities Solutions that were implemented in use cases: Open-AudIT Microsoft Excel GRASSMARLIN Wireshark Native operating system/device capabilities
		PR.IP-2	**Low** Manage the manufacturing system using a system development life cycle that includes security considerations. Include security requirements into the acquisition process of the manufacturing system and its components.	These Subcategory requirements can be met by implementing solutions that provide the **Systems Development Lifecycle Management** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, MS Excel (Manual) Solutions that were implemented in use cases: Open-AudIT

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	Information Protection Processes and Procedures (PR.IP)	PR.IP-3	**Low** Employ configuration change control for the manufacturing system and its components. Conduct security impact analyses in connection with change control reviews.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Change Control** technical capability. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, GRASSMARLIN, Wireshark, I-doit, Salt, Puppet, Ansible. Solutions that were implemented in use cases: Open-AudIT GRASSMARLIN Wireshark Some of these Subcategory requirements can be met by developing policies and Procedures in the **Change Control** section of the **Cybersecurity Operations** document.
		PR.IP-4	**Low** Conduct and maintain backups for manufacturing system data. Manufacturing system data includes for example software, configurations and settings, documentation, system configuration data including computer configuration backups, application configuration backups, operational control limits, control bands and set points for pre-incident operation for all ICS programmable equipment	These Subcategory requirements can be met by implementing solutions that provide the **Configuration Management, Change Control, Configuration Backups, Data Backup, and Data Replication** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, I-doit, Salt, Puppet, Ansible, Veeam Backup and Replication, Bacula Systems, Clonezilla, Commvault Backup & Recovery, Redo backup, and Native operating system/device capabilities. Solutions that were implemented in use cases: Open-AudIT Veeam Backup and Replication Native operating system/device capabilities.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	**Information Protection Processes and Procedures (PR.IP)**	**PR.IP-5**	**Low** Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls for the manufacturing system. Fire suppression mechanisms should take the manufacturing environment into account (e.g., water sprinkler systems could be hazardous in specific environments).	These Subcategory requirements can be met by developing policies and procedures in the **Fire and Safety Regulations** section of the **Cybersecurity Program** document.
		PR.IP-6	**Low** Ensure that manufacturing system data is destroyed according to policy.	These Subcategory requirements can be met by implementing solutions that provide the **Systems Development Lifecycle Management and Media Sanitization** technical capabilities Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, AlienVault OSSIM, MS Excel (Manual), media sanitization tools. Solutions that were implemented in use cases: Open-AudIT DBAN
		PR.IP-7	**Low** Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into protection process revisions. Ensure that the security plan for the manufacturing system facilitates the review, testing, and continual improvement of the security protection processes.	These Subcategory requirements can be met by developing policies and procedures in the **Periodic Reevaluation of the Program** section of the **Cybersecurity Program** document.
		PR.IP-8	**Low** Collaborate and share information about manufacturing system related security incidents and mitigation measures with designated sharing partners. Employ automated mechanisms where feasible to assist in information collaboration.	These Subcategory requirements can be met by developing policies and procedures in the **Information Sharing Policy** section of the **Incident Response Plan** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	**Information Protection Processes and Procedures (PR.IP)**	**PR.IP-9**	**Low** Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as providing a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information. Address maintaining essential functions despite system disruption, and the eventual restoration of the manufacturing system. Define incident types, resources and management support needed to effectively maintain and mature the incident response and contingency capabilities.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Response Plan** and **System Recovery Plan** documents.
		PR.IP-10	**Low** Review response and recovery plans to determine the effectiveness of the plans, and the readiness to execute the plans.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Management** section of the **Cybersecurity Program** document.
		PR.IP-11	**Low** Develop and maintain a personnel security program for the manufacturing system. Personnel security program should include policy, position risk designations, personnel screening, terminations and transfers, access agreements, third-party roles and responsibilities, and personnel sanctions.	These Subcategory requirements can be met by developing policies and procedures in the **Cybersecurity Program** document.
		PR.IP-12	**Low** Establish and maintain a process that allows continuous review of vulnerabilities, and defines strategies to mitigate them.	These Subcategory requirements can be met by developing policies and procedures in the **Vulnerability Management** section of the **Cybersecurity Operations** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
			Low	
PROTECT	**Maintenance (PR.MA)**	**PR.MA-1**	Schedule, perform, document and review records of maintenance and repairs on manufacturing system components. Establish a process for maintenance personnel authorization, and escort non-authorized maintenance personnel. Verify impacted security controls following maintenance or repairs.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Configuration Management, Change Control, Credential Management, Authentication and Authorization, Maintenance Tracking, and Physical Access Control** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, I-doit, Salt, Puppet, Ansible, GRASSMARLIN, Wireshark, Microsoft Active Directory, FreeIPA, OCSinventory-ng, Fiix, Freshservice, and Microsoft Excel. Solutions that were implemented in use cases: Open-AudIT Microsoft Excel GRASSMARLIN Wireshark Microsoft Active Directory Some of these Subcategory requirements can be met by developing policies and procedures in the **Physical Security** and **System Maintenance** section of the **Cybersecurity Policy** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	**Maintenance (PR.MA)**	**PR.MA-2**	**Low** Enforce approval requirements, control, and monitoring, of remote maintenance activities. Employ strong authenticators, record keeping, and session termination for remote maintenance.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Secure Remote Access, Credential Management, Authentication and Authorization, Network Monitoring, System Use Monitoring, and Maintenance Tracking** capabilities. Potential solutions for meeting these Subcategory requirements include: VPN, Remote desktop, Microsoft Active Directory, FreeIPA, OCSinventory-ng, Fiix, Freshservice, Microsoft Excel, and Native operating system/device capabilities. Solutions that were implemented in use cases: Cisco AnyConnect VPN TeamViewer Microsoft Active Directory Microsoft Excel Native operating system/device capabilities. Some of these Subcategory requirements can be met by developing policies and procedures in the **Remote Maintenance** and **System Maintenance** section of the **Cybersecurity Policy** document.
	Protective Technology (PR.PT)	**PR.PT-1**	**Low** Generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or manufacturing components associated with the event. Generate time stamps from an internal system clock that is mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	These Subcategory requirements can be met by implementing solutions that provide the **Time Synchronization, Physical Access Monitoring and Event Logging** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Native operating system/device capabilities, Electronic Access Control System, Sign in/out sheets, cameras, Graylog, Alienvault – OSSIM, SIEMonster Solutions that were implemented in use cases: Native operating system/device capabilities Electronic Access Control System Sign in/out sheets Graylog

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
PROTECT	**Protective Technology (PR.PT)**	**PR.PT-2**	**Low** Employ safeguards to restrict the use of portable storage devices.	These Subcategory requirements can be met by implementing solutions that provide the **Media Protection** technical capability. Potential solutions for meeting these Subcategory requirements include: USB Port Locks, Native operating system/device capabilities. Solutions that were implemented in use cases: USB Port Locks
		PR.PT-3	**Low** Configure the manufacturing system to provide only essential capabilities	These Subcategory requirements can be met by implementing solutions that provide the **Authentication and Authorization, and Ports and Services Lockdown** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Microsoft Active Directory, FreeIPA, Nmap, Native operating system/device capabilities Solutions that were implemented in use cases: Microsoft Active Directory Native operating system/device capabilities
		PR.PT-4	**Low** Monitor and control communications at the external boundary and at key internal boundaries within the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Network Boundary Protection, Authentication and Authorization, and Network Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: firewalls, Security Onion, SNORT, Suricata, Zeek Network Security Monitor, Microsoft Active Directory, FreeIPA Solutions that were implemented in use cases: Microsoft Active Directory Security Onion Firewalls

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
DETECT	**Anomalies and Events (DE.AE)**	**DE.AE-1**	**Low** Ensure that a baseline of network operations and expected data flows for the manufacturing system is developed, documented, and maintained to detect events.	These Subcategory requirements can be met by implementing solutions that provide the **Baseline Establishment and Map Data Flows** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, GRASSMARLIN, Wireshark, I-doit, Salt, Puppet, Ansible, Microsoft Visio, and Ntopng Solutions that were implemented in use cases: Open-AudIT GRASSMARLIN Wireshark Microsoft Visio
		DE.AE-2	**Low** Review and analyze detected events within the manufacturing system to understand attack targets and methods.	These Subcategory requirements can be met by implementing solutions that provide the **Forensics** technical capability. Potential solutions for meeting these Subcategory requirements include: Graylog, Wireshark, Security Onion, Zeek Network Security Monitor, CAINE (Computer Aided Investigative Environment) Solutions that were implemented in use cases: Graylog Wireshark Security Onion
		DE.AE-3	**Low** Ensure that event data is compiled across the manufacturing system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	These Subcategory requirements can be met by implementing solutions that provide the **Event Logging** technical capability. Potential solutions for meeting these Subcategory requirements include: Graylog, Alienvault – OSSIM, SIEMonster Solutions that were implemented in use cases: Graylog

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
DETECT	**Anomalies and Events (DE.AE)**	**DE.AE-4**	**Low** Determine negative impacts to manufacturing operations, assets, and individuals resulting from detected events, and correlate with risk assessment outcomes.	These Subcategory requirements can be met by developing policies and procedures in the **Monitoring the Manufacturing System** section of the **Cybersecurity Operations** document.
		DE.AE-5	**Low** Define incident alert thresholds for the manufacturing system.	Some of these Subcategory requirements can be met by developing policies and procedures in the **Incident Response Plan** document.
	Security Continuous Monitoring (DE.CM)	**DE.CM-1**	**Low** Conduct ongoing security status monitoring of the manufacturing system network to detect defined cybersecurity events and indicators of potential cybersecurity events. Detect unauthorized local, network, and remote connections, and identify unauthorized use of the manufacturing system. Generate audit records for defined cybersecurity events. Monitor network communications at the external boundary of the system and at key internal boundaries within the system. Heighten system monitoring activity whenever there is an indication of increased risk.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Network Boundary Protection, Network Monitoring, and Event Logging** technical capabilities. Potential solutions for meeting these Subcategory requirements include: firewalls, Security Onion, SNORT, Suricata, Zeek Network Security Monitor Graylog, Alienvault – OSSIM, SIEMonster Solutions that were implemented in use cases: Firewalls Security Onion Graylog Some of these Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document
		DE.CM-2	**Low** Conduct ongoing security status monitoring of the manufacturing system facility to detect physical security incidents.	These Subcategory requirements can be met by implementing solutions that provide the **Physical Access Monitoring** technical capability. Potential solutions for meeting these Subcategory requirements include: electronic access control systems, cameras, Sign in/out sheets Solutions that were implemented in use cases: Electronic access control system Sign in/out sheet

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
DETECT	**Security Continuous Monitoring (DE.CM)**	**DE.CM-3**	**Low** Conduct security status monitoring of personnel activity associated with the manufacturing system. Enforce software usage and installation restrictions.	These Subcategory requirements can be met by implementing solutions that provide the **Authentication and Authorization, System Use Monitoring, and Physical Access Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Microsoft Active Directory, FreeIPA, Symantec Endpoint Protection, Native operating system/device capabilities, electronic access control systems, cameras, Sign in/out sheets Solutions that were implemented in use cases: Active Directory Symantec Endpoint Protection Native operating system/device capabilities Electronic access control system Sign in/out sheet
		DE.CM-4	**Low** Deploy malicious code protection mechanisms throughout the manufacturing system where safe and feasible to detect and eradicate malicious code. Update malicious code protection mechanisms whenever new releases are available in accordance with the configuration management policy and procedures for the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Anti-virus/malware and Vulnerability Management** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Symantec Endpoint Protection, ClamAV, NamicSoft, OpenVAS, Tenable Nessus Solutions that were implemented in use cases: Symantec Endpoint Protection NamicSoft
		DE.CM-5	**Low** None	N/A

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
DETECT	**Security Continuous Monitoring (DE.CM)**	**DE.CM-6**	**Low** Conduct ongoing security status monitoring of external service provider activity on the manufacturing system. Detect defined cybersecurity events and indicators of potential cybersecurity events from external service providers. Monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.	These Subcategory requirements can be met by implementing solutions that provide the **Network Monitoring and Event Logging** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Security Onion, SNORT, Suricata, Zeek Network Security Monitor, Graylog, Alienvault – OSSIM, SIEMonster Solutions that were implemented in use cases: Security Onion Graylog
		DE.CM-7	**Low** Conduct ongoing security status monitoring on the manufacturing system for unauthorized personnel, connections, devices, access points, and software. Monitor for system inventory discrepancies.	These Subcategory requirements can be met by implementing solutions that provide the **Hardware Inventory, Software Inventory, Systems Development Lifecycle Management, Baseline Establishment, Change Control, and Network Monitoring** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Open-AudIT, LANSweeper, Spiceworks, OCSinventory-ng, AlienVault OSSIM, Microsoft Excel (Manual), I-doit, Salt, Puppet, Ansible, GRASSMARLIN, Wireshark, Security Onion, SNORT, Suricata, Zeek Network Security Monitor Solutions that were implemented in use cases: Open-AudIT GRASSMARLIN Wireshark Microsoft Excel Security Onion

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
DETECT	**Security Continuous Monitoring (DE.CM)**	**DE.CM-8**	**Low** Conduct vulnerability scans on the manufacturing system where safe and feasible. Include analysis, remediation, and information sharing in the vulnerability scanning process. Employ control system-specific vulnerability scanning tools and techniques where safe and feasible. Active vulnerability scanning, which introduces network traffic, is used with care on manufacturing systems to ensure that system functions are not adversely impacted by the scanning process.	Some of these Subcategory requirements can be met by implementing solutions that provide the **Vulnerability Scanning** capability. Potential solutions for meeting these Subcategory requirements include: Tenable Nessus, OpenVAS, AlienVault OSSIM Solutions that were implemented in use cases: Tenable Nessus Some Subcategory requirements can be met by developing policies and procedures in the **Vulnerability Management** section of the **Cybersecurity Operations** document.
	Detection Processes (DE.DP)	**DE.DP-1**	**Low** Define roles and responsibilities for detection activities on the manufacturing system and ensure accountability.	These Subcategory requirements can be met by developing policies and procedures in the **Role-based Security Responsibilities** section of the **Cybersecurity Policy** document.
		DE.DP-2	**Low** Conduct detection activities in accordance with applicable federal and state laws, industry regulations and standards, policies, and other applicable requirements.	These Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document.
		DE.DP-3	**Low, Moderate and High** Validate that event detection processes are operating as intended.	These Subcategory requirements can be met by implementing solutions that provide the **Event Logging** technical capability. Potential solutions for meeting these Subcategory requirements include: Graylog, Alienvault – OSSIM, SIEMonster Solutions that were implemented in use cases: Graylog

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
DETECT	Detection Processes (DE.DP)	DE.DP-4	**Low** Communicate event detection information to defined personnel. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of VoIP, and malware disclosure.	These Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document.
		DE.DP-5	**Low** Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions. Ensure the security plan for the manufacturing system provides for the review, testing, and continual improvement of the security detection processes.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Management** and **Periodic Reevaluation of the Program** section of the **Cybersecurity Program** document.
RESPOND	Response Planning (RS.RP)	RS.RP-1	**Low** Execute the response plan during or after a cybersecurity event on the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Purpose and Scope** section of the **Incident Response Plan** document.
	Communications (RS.CO)	RS.CO-1	**Low** Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event response.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
RESPOND	**Communications (RS.CO)**	**RS.CO-2**	**Low** Employ prompt reporting to appropriate stakeholders for cybersecurity events on the manufacturing system. Ensure that cybersecurity events on the manufacturing system are reported consistent with the response plan.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **Incident Response Plan** document.
		RS.CO-3	**Low** Share cybersecurity incident information with relevant stakeholders per the response plan.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications Policy** section of the **Incident Response Plan** document.
		RS.CO-4	**Low** Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include for example, mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **Incident Response Plan** document.
		RS.CO-5	**Low** Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity situational awareness. For example, the DHS National Cybersecurity & Communications Integration Center (NCCIC) [6] serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [7] collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related cybersecurity incidents and mitigation measures.	These Subcategory requirements can be met by developing policies and procedures in the **Continuous Monitoring** section of the **Cybersecurity Policy** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
RESPOND	**Analysis (RS.AN)**	**RS.AN-1**	**Low** Investigate cybersecurity-related notifications generated from detection systems.	These Subcategory requirements can be met by developing policies and procedures in the **Monitoring the Manufacturing System** section of the **Cybersecurity Operations** document.
		RS.AN-2	**Low** Understand the full implication of the cybersecurity incident based on thorough investigation and analysis results. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document.
		RS.AN-3	**Low** Conduct forensic analysis on collected cybersecurity event information to determine root cause.	These Subcategory requirements can be met by implementing solutions that provide the **Event Logging and Forensics** technical capabilities. Potential solutions for meeting these Subcategory requirements include: Graylog, Wireshark, Zeek Network Security Monitor, CAINE (Computer Aided Investigative Environment), Alienvault – OSSIM, SIEMonster, Security Onion Solutions that were implemented in use cases: Graylog Wireshark Security Onion
		RS.AN-4	**Low** Categorize cybersecurity incidents according to level of severity and impact consistent with the response plan.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Severity Classification** section of the **Incident Response Plan** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
RESPOND	**Mitigation (RS.MI)**	**RS.MI-1**	**Low** Contain cybersecurity incidents to minimize impact on the manufacturing system.	These Subcategory requirements can be met by developing policies and procedures in the **Incident Response Workflow** section of the **Incident Response Plan** document.
		RS.MI-2	**Low** Mitigate cybersecurity incidents occurring on the manufacturing system.	These Subcategory requirements can be met by implementing solutions that provide the **Incident Management** technical capability. Potential solutions for meeting these Subcategory requirements include: Sandia Cyber Omni Tracker (SCOT), The Hive Project, Request Tracker Incident Response (RTIR) Solutions that were implemented in use cases: The Hive Project
		RS.MI-3	**Low** Ensure that vulnerabilities identified while responding to a cybersecurity incident are mitigated or documented as accepted risks.	These Subcategory requirements can be met by implementing solutions that provide the **Vulnerability Management and Incident Management** technical capabilities. Potential solutions for meeting these Subcategory requirements include: NamicSoft, OpenVAS, Tenable Nessus, AlienVault OSSIM, Sandia Cyber Omni Tracker (SCOT), The Hive Project, Request Tracker Incident Response (RTIR) Solutions that were implemented in use cases: NamicSoft The Hive Project

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
RESPOND	**Improvements (RS.IM)**	**RS.IM-1**	**Low** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document.
		RS.IM-2	**Low** Update the response plans to address changes to the organization, manufacturing system, attack vectors, or environment of operation and problems encountered during plan implementation, execution, or testing. Updates may include, for example, responses to disruptions or failures, and predetermined procedures. Enable a process for the response plan to evolve to reflect new threats, improved technology, and lessons learned.	These Subcategory requirements can be met by developing policies and procedures in the **Policy** section of the **Incident Response Plan** document.
RECOVER	**Recovery Planning (RC.RP)**	**RC.RP-1**	**Low** Execute the recovery plan during or after a cybersecurity incident on the manufacturing system. Restore the manufacturing system within a predefined time-period from configuration-controlled and integrity-protected information representing a known, operational state for the components.	These Subcategory requirements can be met by developing policies and procedures in the **Objectives** section of the **System Recovery Plan** document.
	Improvements (RC.IM)	**RC.IM-1**	**Low** Incorporate lessons learned from ongoing recovery activities into system recovery procedures, training, and testing, and implement the resulting changes accordingly.	These Subcategory requirements can be met by developing policies and procedures in the **Plan Testing** and **Plan Maintenance** sections of the **System Recovery Plan** document.

Function	Category	Subcategory	Manufacturing Profile	Implementation Overview
RECOVER	**Improvements (RC.IM)**	**RC.IM-2**	**Low** Update the recovery plan to address changes to the organization, manufacturing system, or environment of operation and problems encountered during plan implementation, execution, or testing. Ensure that updates are integrated into the recovery plans.	These Subcategory requirements can be met by developing policies and procedures in the **Plan Testing** and **Plan Maintenance** sections of the **System Recovery Plan** document.
	Communications (RC.CO)	**RC.CO-1**	**Low** Centralize and coordinate information distribution, and manage the public facing representation of the organization. Public relations management may include, for example, managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of information provided to the media, ensuring personnel are familiar with public relations and privacy policies.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **System Recovery Plan** document.
		RC.CO-2	**Low** Employ a crisis response strategy to protect against negative impact and repair organizational reputation. Crisis response strategies include, for example, actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **System Recovery Plan** document.
		RC.CO-3	**Low** Communicate recovery activities to all relevant stakeholders, and executive and management teams.	These Subcategory requirements can be met by developing policies and procedures in the **Internal and External Communications** section of the **System Recovery Plan** document.

8. Laboratory Environment Overview

This section provides details on the laboratory environment (i.e., lab), located at the NIST main campus in Gaithersburg, Maryland. The lab contains a shared infrastructure of networked servers, measurement tools, industrial robots, hardware-in-the-loop simulators, and other technologies to support the Manufacturing Profile implementation on two manufacturing systems: a Process Control System (PCS) [12] and a Collaborative Robotics System (CRS) [11]. The PCS and CRS employ real-world industrial hardware (e.g., programmable logic controllers, robot arms, sensors), networking devices, and industrial protocols to emulate a process and discrete manufacturing system, respectively. Further details on the two systems are described in Section 8.1 and Section 8.2.

The network infrastructure, shown in Figure 8-1, is used for many research functions including: testing, deployment, and hosting of cybersecurity tools, measurement systems for network traffic, creation and manipulation of network traffic for inducing anomalous network activity, and archival storage of experiment data. A virtualization environment was implemented to support the numerous cybersecurity technologies and tools required for the implementation.

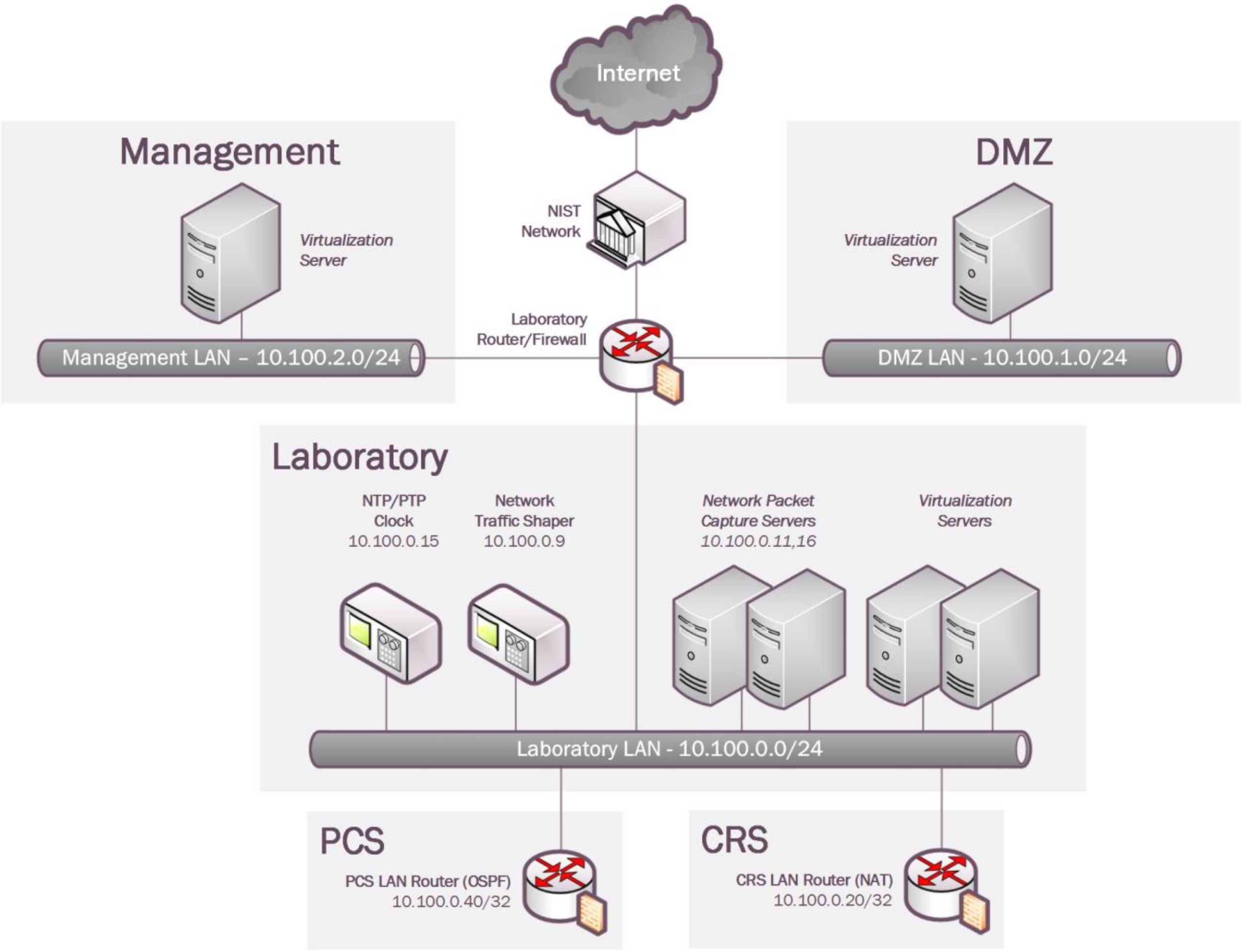
Internet
Management
Virtualization Server
Management LAN – 10.100.2.0/24
NIST Network
Laboratory Router/Firewall
DMZ
Virtualization Server
DMZ LAN - 10.100.1.0/24
Laboratory
NTP/PTP Clock 10.100.0.15
Network Traffic Shaper 10.100.0.9
Network Packet Capture Servers 10.100.0.11,16
Virtualization Servers
Laboratory LAN - 10.100.0.0/24
PCS
PCS LAN Router (OSPF) 10.100.0.40/32
CRS
CRS LAN Router (NAT) 10.100.0.20/32

Figure 8-1 Lab Network Infrastructure

The lab network infrastructure is separated into three independent network zones: Management zone, DMZ (Demilitarized Zone), and Laboratory zone. The Management zone contains hosts that are used to manage the numerous laboratory devices (e.g., network hardware, virtualization servers). The DMZ zone contains hosts that perform data-sharing functions between the lab network and the top-level network (in this case, the NIST Network). And the Laboratory zone contains the shared measurement servers and tools, and a virtualization infrastructure for hosting cybersecurity tools.

Attached to the Laboratory zone are the local PCS and CRS networks, which operate independently of each other. The PCS network accesses the Laboratory LAN using the Open Shortest Path First (OSPF) routing protocol, and the CRS accesses the Laboratory LAN using Dynamic Network Address Translation (Dynamic NAT).

A dedicated network packet capture server is provided for both the PCS and CRS. Packets are captured using two methods: packet mirroring, and bump-in-the-wire network probes. Packet mirroring involves configuring network devices (e.g., routers, switches) to duplicate and forward the packet to another port. Network probes perform a similar function, but they must be physically connected to the network cable. In the lab, mirrored packets are aggregated into two streams (one containing PCS traffic, and the other containing CRS traffic) using a packet broker. Network traffic from the aggregator and network probes terminate at the network packet capture servers, where they are buffered, stored, and later processed to calculate the metrics and key performance indicators (KPI) required for experimental analysis.

8.1 Process-based Manufacturing System

The Process Control System emulates an industrial continuous manufacturing system, a manufacturing process to produce or process materials continuously, where the materials are continuously moving, chemically reacting, or undergoing mechanical or thermal treatment. Continuous manufacturing usually implies a 24x7 operation with infrequent maintenance shutdowns and is contrasted with batch manufacturing. Examples of continuous manufacturing systems include chemical production, oil refining, natural gas processing, and waste water treatment.

The PCS uses the Tennessee Eastman challenge problem [9] a real-world industrial chemical manufacturing process, as the simulation model for the chemical reaction. The system integrates the control algorithm developed by Ricker [10] to control the simulated chemical reaction. With the use of widely deployed industrial hardware like programmable logic controllers (PLCs) and industrial network switches as part of the control loop, this system emulates a complete setup of a continuous chemical manufacturing system. This hardware-in-the-loop configuration allows the testbed to measure the performance of the manufacturing system using real-world industrial hardware, while the chemical manufacturing process is simulated in software.

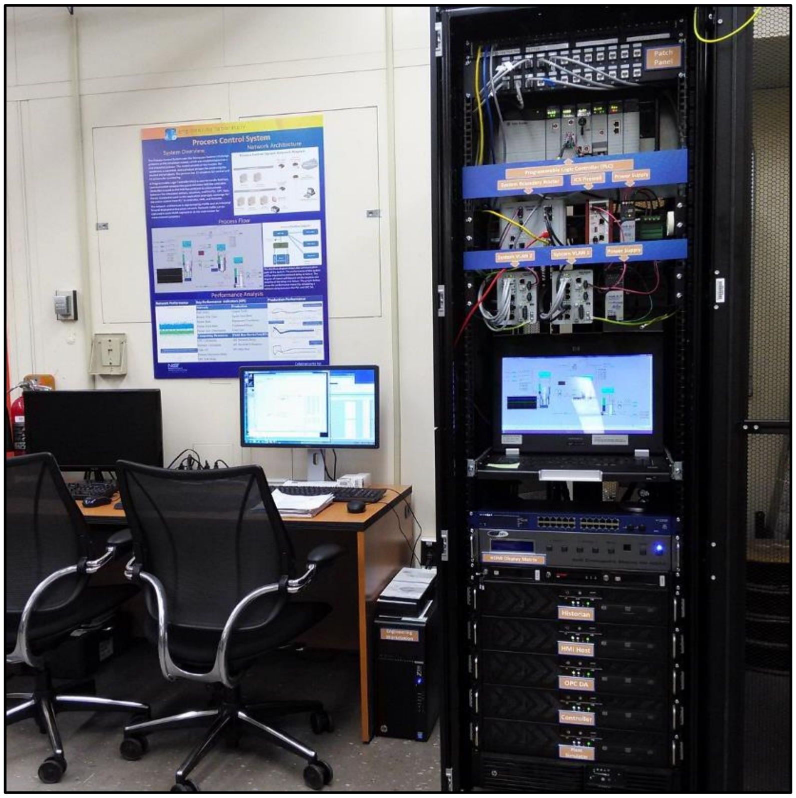

Figure 8-2 PCS System

8.1.1 Control System Operation

The PCS includes a software simulator to emulate the Tennessee Eastman chemical reaction process. The simulator is written in C code and is executed on a Windows 7 based computer. In addition, the system includes a Programmable Logic Controller (PLC), a software controller implemented in MATLAB, a human-machine interface (HMI), an Object Linking and Embedding for Process Control (OPC) Data Access (DA) server, a Data Historian, an engineering workstation, and several Virtual Local Area Network (VLAN) switches and network routers. The PCS is housed in a 19-inch rack system, shown in Figure 8-2.

The Tennessee Eastman Plant Simulator requires a controller to provide the control loops in order to operate continuously. A decentralized controller implemented in Simulink, developed by Ricker [10] is used as the process controller. The Ricker implementation matches the Plant Simulator accurately, and the controller is a separate software process that runs on a separate computer from the Plant Simulator.

To provide communication between the Plant Simulator and the Controller, a hardware PLC with industrial network protocol capability is used. The industrial protocol is used to communicate between the Plant Simulator and the PLC. The Plant Simulator sends its sensor information to the Controller, and the Controller algorithm uses the sensor inputs to compute the desired values of the actuators and sends them back to the Plant Simulator.

In the Plant Simulator computer, a multi-node DeviceNet card was installed. DeviceNet is a common industrial protocol used in the automation industry to exchange data between control devices. The multi-node card allows a single hardware device to emulate multiple virtual DeviceNet nodes. In our case, each sensor and actuator point is a dedicated node. Therefore, 53 virtual nodes (41 for sensors and 12 for actuators) were configured in the system. A software interface was developed to send and receive sensor and actuator values between the Plant Simulator and the PLC through DeviceNet.

An OPC DA Server runs on a Windows 7 computer, acting as the main data gateway for the PLC. The PLC communicates to the OPC DA server to update and retrieve all the sensor and actuator information, respectively. This sensor and actuator information is also known as a “tag” in PLC terminology. The Controller has a MATLAB Simulink interface that communicates with the OPC DA server directly.

A Human-Machine Interface (HMI) and a Data Historian are implemented in the system. The HMI provides a graphical user interface to present information to an operator or user about the state of the process. The Data Historian serves as the main database to record all the process sensor and actuator information. Both HMI and Data Historian have built-in interfaces to establish connections to the OPC DA to access all the process information.

An engineering workstation is used in the system for engineering support, such as PLC development and control, HMI development and deployment, and Data Historian data retrieval.

8.1.2 Network Architecture

The PCS network is segmented from the main Laboratory LAN by a boundary router. The router uses a dynamic routing protocol, Open Shortest Path First (OSPF), to communicate with the main top-level router. The network architecture is shown in Figure 8-3.

All network traffic needs to go through the boundary router to access the main Laboratory LAN.

There are two virtual network segments in the system. Each network is managed by an Ethernet switch. The HMI and the Controller are in virtual network VLAN-1, while the Plant Simulator, Data Historian, OPC DA Server, and PLC are in virtual network VLAN-2.

VLAN-1 simulates a central control room environment where the HMI and the controllers are virtually located in the same network segment. VLAN-2 simulates the process operation environment which typically consists of the operating plant, PLCs, OPC server, and the Data Historian.

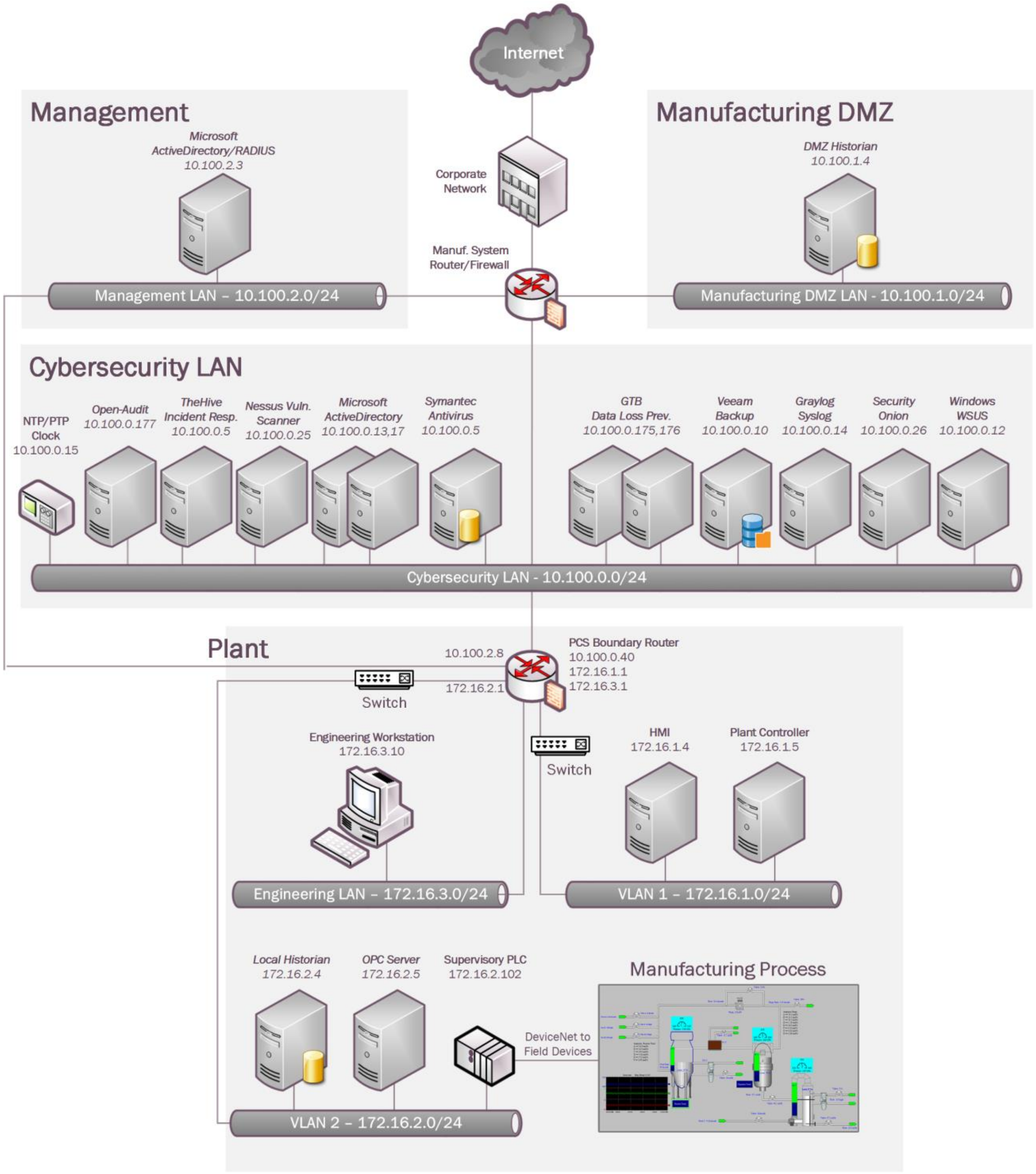
Internet
Management
Microsoft ActiveDirectory/RADIUS 10.100.2.3
Management LAN – 10.100.2.0/24
Corporate Network
Manuf. System Router/Firewall
Manufacturing DMZ
DMZ Historian 10.100.1.4
Manufacturing DMZ LAN - 10.100.1.0/24
Cybersecurity LAN
NTP/PTP Clock 10.100.0.15
Open-Audit 10.100.0.177
TheHive Incident Resp. 10.100.0.5
Nessus Vuln. Scanner 10.100.0.25
Microsoft ActiveDirectory 10.100.0.13,17
Symantec Antivirus 10.100.0.5
GTB Data Loss Prev. 10.100.0.175,176
Veeam Backup 10.100.0.10
Graylog Syslog 10.100.0.14
Security Onion 10.100.0.26
Windows WSUS 10.100.0.12
Cybersecurity LAN - 10.100.0.0/24
Plant
10.100.2.8
172.16.2.1
PCS Boundary Router 10.100.0.40 172.16.1.1 172.16.3.1
Switch
Engineering Workstation 172.16.3.10
Switch
HMI 172.16.1.4
Plant Controller 172.16.1.5
Engineering LAN – 172.16.3.0/24
VLAN 1 – 172.16.1.0/24
Local Historian 172.16.2.4
OPC Server 172.16.2.5
Supervisory PLC 172.16.2.102
DeviceNet to Field Devices
Manufacturing Process
VLAN 2 – 172.16.2.0/24

Figure 8-3 PCS Network Architecture

8.2 Discrete-based Manufacturing System

The CRS workcell, shown in Figure 8-4 contains two robotic arms that perform a material handling process called machine tending [11]. Robotic machine tending utilizes robots to interact with machinery, performing physical operations a human operator would normally perform (e.g., loading and unloading of parts in a machine, opening and closing of machine doors, activating operator control panel buttons, etc.).

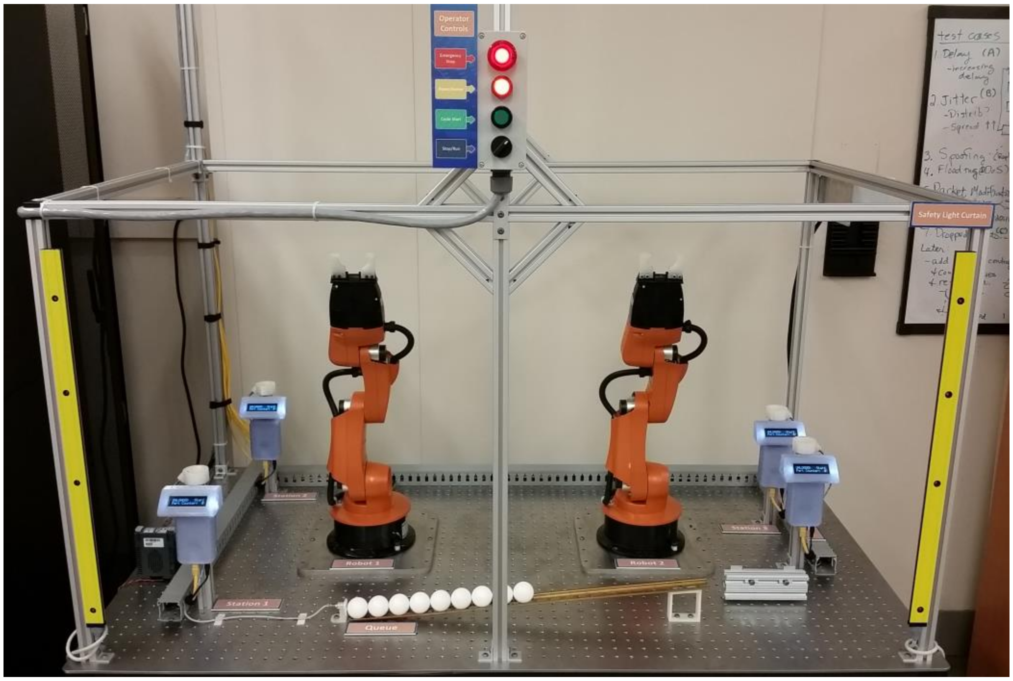

Figure 8-4 The CRS workcell in standby, waiting for the operator to initiate the manufacturing process. The operator control panel is visible at the top of the figure.

A human operator interfaces with the workcell through a human-machine interface (HMI) and a control panel external to the work area.

The workcell was designed and constructed to be reconfigurable, allowing numerous types of operational methodologies, network topologies, and industrial networking protocols to be investigated. The two robots collaborate to transport parts through the manufacturing process, as a single robot cannot physically reach all four stations. Having two robots also increases workcell efficiency.

8.2.1 Control System Operation

Parts are transported by the robot arms through four simulated machining operations, known as *stations*. Each station is comprised of: a fixture for holding the part, an infrared proximity sensor for detecting the part, a single board computer simulating the actions and communications of a typical machining center, and a liquid crystal display (LCD) for displaying the operational status of the station. The stations communicate with the Supervisory PLC over the workcell LAN. The Supervisory PLC monitors and controls all aspects of the manufacturing process.

Manufacturing data from the four machining stations are used by the PLC to determine which operations, known as *jobs*, the robots must perform to keep the parts moving through the sequential manufacturing process. The PLC also communicates with the HMI for operator visibility and control.

The workcell is supported by a shared infrastructure of networked servers, measurement tools, and other technologies. The infrastructure is used for many research functions including: testing, deployment, and hosting of cybersecurity tools; measurement and packet capture systems for network traffic; creation and manipulation of network traffic for inducing anomalous network activity; and archival storage of experiment data. A virtualized server infrastructure was installed to support the numerous cybersecurity technologies and tools required for the implementation.

8.2.2 Network Architecture

The CRS network, shown in Figure 8-5, is hierarchically architected, separating the devices performing supervisory functions from the devices controlling the manufacturing process. The workcell top-level router is a Siemens RUGGEDCOM RX1510, and provides firewall capabilities for rule-based allowance and restriction of network traffic. The router is connected to the Laboratory LAN (identified in Figure 8-5 as the Testbed LAN) using network address translation (NAT). Layer 2 network traffic for the Supervisory LAN is handled by a Netgear GS724T managed Ethernet switch, and network traffic for the Control LAN is handled by a Siemens i800 managed Ethernet switch.

The router and network switches are configured to mirror all incoming network traffic to a packet capture server located in the measurement rack. In-line (i.e., bump-in-the-wire) network probes are located at the PLC, HMI, and Station 1 to provide dedicated forwarding of all incoming and outgoing network traffic to the packet capture server.

All manufacturing process-based network communications utilize the Modbus TCP industrial network protocol, and all network traffic between the robot controllers and robot drivers utilize the Robot Operating System’s (ROS) native transport protocols TCPROS and UDPROS.

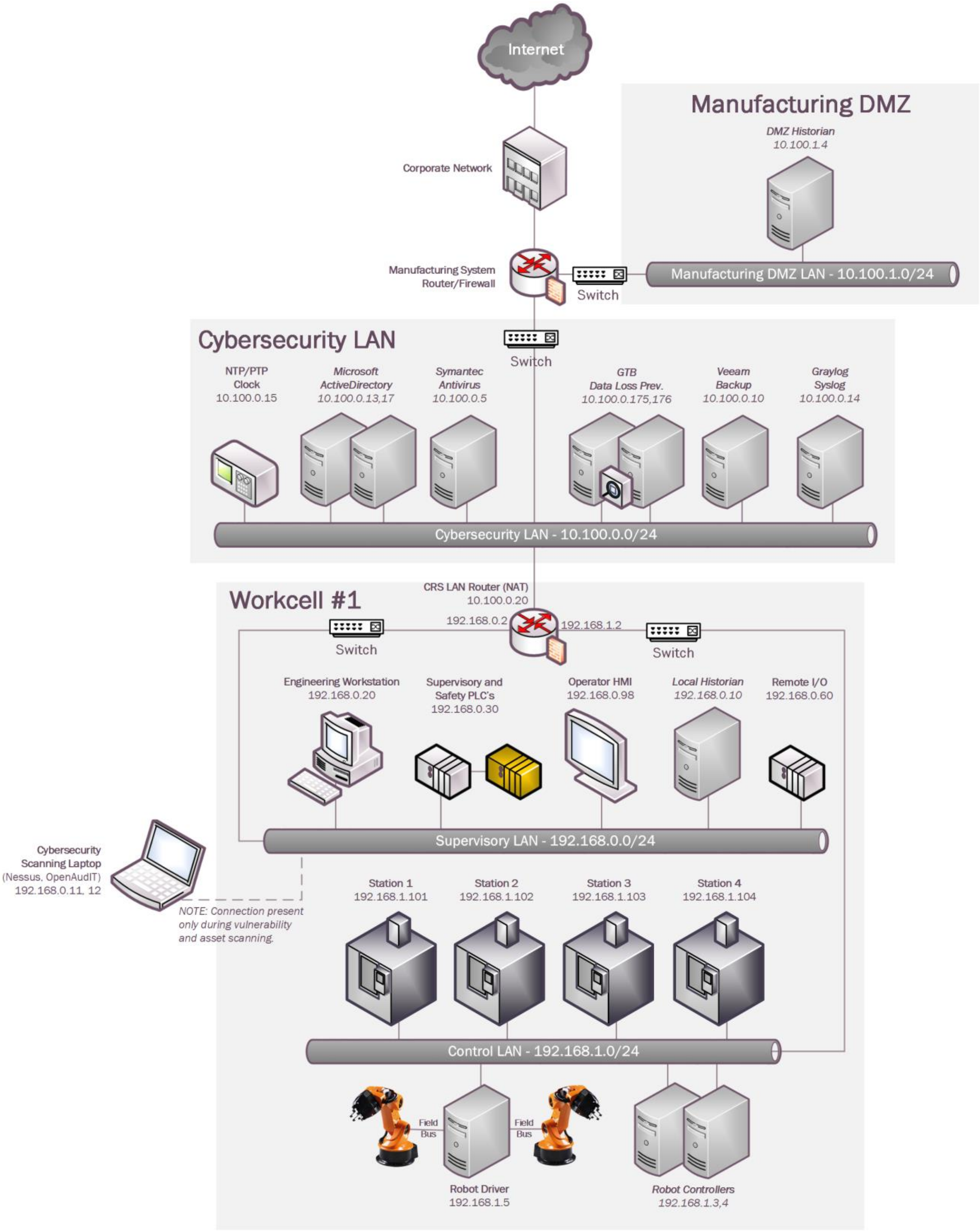

Figure 8-5 Robotic Assembly CRS Network

Appendix A - Acronyms and Abbreviations

Selected acronyms and abbreviations used in in this document are defined below.

CAN	Controller Area Network
CERT	Computer Emergency Response Team
COTS	Commercial Off-The-Shelf
CRS	Collaborative Robotics System
CSF	Cybersecurity Framework
DA	Data Access
DCS	Distributed Control System
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
FIPS	Federal Information Processing Standards
GBPS	Gigabits Per Second
GMT	Greenwich Mean Time
HMI	Human Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICSJWG	Security Industrial Control System Joint Working Group
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISA	The International Society of Automation
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
LCD	Liquid Crystal Display
LVL	Level
MBPS	Megabits Per Second
MFG	Manufacturing
NAT	Network Address Translation
NCCIC	National Cybersecurity & Communications Integration Center
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NISTIR	NIST Internal Report
OEM	Original Equipment Manufacturer
OPC	Open Process Control
OSPF	Open Shortest Path First
OT	Operational Technology
PCS	Process Control System

PLC	Programmable Logic Controller
RAM	Random Access Memory
ROS	Robot Operating System
SCADA	Supervisory Control and Data Acquisition
SEC	Security
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TCPROS	TCP-based Robot Operating System protocol
UDP	User Datagram Protocol
UDPROS	UDP-based Robot Operating System protocol
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
UTC	Coordinated Universal Time
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network

Appendix B - Glossary

Selected terms used in in this document are defined below.

Actuator - A device for moving or controlling a mechanism or system. It is operated by a source of energy, typically electric current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion. An actuator is the mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or other agent. [800-82]

Business/Mission Objectives - Broad expression of business goals. Specified target outcome for business operations.

Category - The subdivision of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

Critical Infrastructure - Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. [DHS]

Criticality Reviews - A determination of the ranking and priority of manufacturing system components, services, processes, and inputs in order to establish operational thresholds and recovery objectives.

Critical Services - The subset of mission essential services required to conduct manufacturing operations. Function or capability that is required to maintain health, safety, the environment and availability for the equipment under control. [62443]

Cyber Risk - Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

Cybersecurity - The process of protecting information by preventing, detecting, and responding to attacks. [CSF]

Event - Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). [CSF]

Firmware - Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. [Techterms.com]

Framework - The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

Function - Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CSF]

Informative References - Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory in the Cybersecurity Framework.

Manufacturing Operations - Activities concerning the facility operation, system processes, materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to the manufacturing enterprise.

Network Access - any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Operational technology - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner.com]

Programmable Logic Controller - A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. [800-82]

Profile - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. [CSF]

- Target Profile - the desired outcome or ‘to be’ state of cybersecurity implementation
- Current Profile – the ‘as is’ state of system cybersecurity

Protocol - A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [800-82]

Remote Access - Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). [800-53]

Resilience Requirements - The business-driven availability and reliability characteristics for the manufacturing system that specify recovery tolerances from disruptions and major incidents.

Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [800-82]

Risk Tolerance - The level of risk that the Manufacturer is willing to accept in pursuit of strategic goals and objectives. [800-53]

Router - A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. [800-82]

Security Control - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. [800-82]

Subcategory - The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.” [CSF]

Supporting Services - Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. [800-53]

Switch - A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. [Whatis.com]

System Categorization - The characterization of a manufacturing system, its components, and operations, based on an assessment of the potential impact that a loss of availability, integrity, or confidentiality would have on organizational operations, organizational assets, or individuals. [FIPS 199]

Third-Party Relationships - relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties. [DHS]

Third-party Providers - Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system.

Thresholds - Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.

Appendix C - References

1. Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915

2. National Institute of Standards and Technology (2014) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), February 12, 2014. https://doi.org/10.6028/NIST.CSWP.02122014

3. Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

4. Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

5. The International Society of Automation (2019) *ISA99, Industrial Automation and Control Systems Security*. Available at https://www.isa.org/isa99/.

6. National Cybersecurity & Communications Integration Center (NCCIC) - https://www.dhs.gov/national-cybersecurity-and-communications-integration-center.

7. U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) (2019) *Cybersecurity and Infrastructure Security Agency -- Industrial Control Systems*. Available at https://ics-cert.us-cert.gov/.

8. Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, McCarthy J (2019) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8183, Includes updates as of May 20, 2019. https://doi.org/10.6028/NIST.IR.8183

9. J. J. Downs and E. F. Vogel, A Plant-Wide Industrial Process Control Problem, Computers and Chemical Engineering, vol. 17, no. 3, pp. 245-255, 1993.

10. L. Ricker, Decentralized control of the Tennessee Eastman Challenge Process, Journal of Process Control, vol. 6, no. 4, pp. 205-221, 1996.

11. Zimmerman T (2017) Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8177, Includes updates as of May 21, 2019. https://doi.org/10.6028/NIST.IR.8177

12. Tang CY (2017) Key Performance Indicators for Process Control System Cybersecurity Performance Analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8188, 2017. https://doi.org/10.6028/NIST.IR.8188