1. Introduction

1.1. Purpose and Scope

The purpose of this document is to provide guidance for establishing secure operational technology (OT)[2] while addressing OT's unique performance, reliability, and safety requirements. This document gives an overview of OT systems and typical system topologies, identifies common threats and vulnerabilities for these systems, and recommends security countermeasures to mitigate the associated risks. Additionally, it presents an OT-tailored security control overlay based on NIST Special Publication (SP) 800-53, Rev. 5 [SP800-53r5] that customizes controls for the unique characteristics of the OT domain. The body of the document provides context for the overlay, but the overlay is intended to stand alone.

Because there are many types of OT with varying levels of potential risk and impact, this document provides a list of many methods and techniques for securing OT systems. The document should not be used purely as a checklist to secure a specific system. Readers are encouraged to perform a risk-based assessment on their systems and to tailor the recommended guidelines and solutions to meet their specific security, business, and operational requirements. The range of applicability of the basic concepts for securing OT systems presented in this document continues to expand.

1.2. Audience

This document covers details that are specific to OT systems. Readers of this document should be acquainted with general computer security concepts and communication protocols, such as those used in networking. The document is technical in nature. However, it provides the necessary background to understand the topics that are discussed.

The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement OT systems
- System administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure OT systems
- Security consultants who perform security assessments and penetration testing of OT systems
- Managers who are responsible for OT systems
- Senior management who need to better understand the risks to OT systems as they justify and apply an OT cybersecurity program
- Researchers and analysts who are trying to understand the unique security needs of OT systems
- Vendors who are developing products that will be deployed as part of an OT system

[2] The acronym "OT" can stand for either "operational technology" or "operational technologies." The context around the acronym, especially the use of singular or plural words, will indicate which meaning is intended.

1.3. Document Structure

The remainder of this document is divided into the following major sections:

- Section 2 gives an overview of OT, including a comparison between OT and IT systems.
- Section 3 discusses the development and deployment of an OT cybersecurity program to mitigate risk for the vulnerabilities identified in Appendix C.
- Section 4 examines OT security risk management and applying the Risk Management Framework to OT systems.
- Section 5 provides recommendations for integrating security into network architectures typically found in OT systems, with an emphasis on network segmentation and separation practices.
- Section 6 offers guidance on applying the Cybersecurity Framework to OT systems.
- The References section provides a list of references used in the development of this document.

This guide also contains several appendices with supporting material, as follows:

- Appendix A lists the acronyms and abbreviations used in this document.
- Appendix B contains a glossary of the terms used in this document.
- Appendix C discusses OT threat sources, vulnerabilities and predisposing conditions, threat events, and incidents.
- Appendix D presents lists and descriptions of OT security organizations, research, and activities.
- Appendix E discusses various OT security capabilities and tools.
- Appendix F defines the NIST SP 800-53, Rev. 5 OT overlay and lists security controls, enhancements, and supplemental guidance that apply specifically to OT systems.

2. OT Overview

Operational technology (OT)[3] encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

OT systems consist of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an objective (e.g., manufacturing, transportation of matter or energy). The part of the system primarily concerned with producing an output is referred to as the *process*. The part of the system primarily concerned with maintaining conformance with specifications is referred to as the *controller* (or *control*). The control components of the system include the specification of the desired output or performance. The system can be configured in one of three ways:

- *Open loop*: The output is controlled by established settings.
- *Closed loop*: The output affects the input in such a way as to maintain the desired control objective.
- *Manual mode*: The system is completely controlled by humans.

This section provides an overview of several types of common OT systems, including supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), building automation systems (BASs), physical access control systems (PACSs), and the Industrial Internet of Things (IIoT). Diagrams depict the network topology, connections, components, and protocols that are typically used for each system type. These examples only attempt to identify notional topology concepts. Actual implementations of these types of control systems may be hybrids that blur the lines between them. Note that the diagrams in this section do not focus on securing OT. Security architecture and security controls are discussed in Section 5 and Appendix F of this document, respectively.

2.1. Evolution of OT

Much of today's OT evolved from the insertion of IT capabilities into existing physical systems, often replacing or supplementing physical control mechanisms. For example, embedded digital controls replaced analog mechanical controls in rotating machines and engines. Improvements in cost and performance have encouraged this evolution and resulted in many of today's "smart" technologies, such as the smart electric grid, smart transportation, smart buildings, smart manufacturing, and the Internet of Things. While this increases the connectivity and criticality of these systems, it also creates a greater need for their adaptability, resilience, safety, and security.

Engineering OT continues to provide new capabilities while maintaining the typical long life cycles of these systems. The introduction of IT capabilities into physical systems presents emergent behavior with security implications. Engineering models and analysis are evolving to address these emergent properties, including safety, security, privacy, and environmental impact interdependencies.

[3] See https://csrc.nist.gov/Projects/operational-technology-security.

2.2. OT-Based Systems and Their Interdependencies

OT is used in many industries and infrastructures, including those identified by the Cybersecurity and Infrastructure Security Agency (CISA) as critical infrastructure sectors listed below. OT can be found in all critical infrastructures and is more prevalent in the sectors that are in bold.

- **Chemical Sector**
- **Commercial Facilities Sector**
- Communications Sector
- **Critical Manufacturing Sector**
- **Dams Sector**
- **Defense Industrial Base Sector**
- **Emergency Services Sector**
- **Energy Sector**
- Financial Services Sector
- **Food and Agriculture Sector**
- **Government Facilities Sector**
- **Healthcare and Public Health Sector**
- Information Technology Sector
- **Nuclear Reactors, Materials, and Waste Sector**
- **Transportation Systems Sector**
- **Water and Wastewater Systems Sector**

OT is vital to the operation of U.S. critical infrastructures, which are often highly interconnected and mutually dependent systems, both physically and through a host of information and communications technologies. It is important to note that while federal agencies operate many of the critical infrastructures mentioned above, many others are privately owned and operated. Additionally, critical infrastructures are often referred to as a "system of systems" because of the interdependencies that exist between various industrial sectors and the interconnections between business partners [Peerenboom][Rinaldi]. An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

For example, both the electrical power transmission and distribution grid industries use geographically distributed SCADA control technology to operate highly interconnected and dynamic systems that consist of thousands of public and private utilities and rural cooperatives for supplying electricity to end users. Some SCADA systems monitor and control electricity distribution by collecting data from and issuing commands to geographically remote field control stations from a centralized location. SCADA systems are also used to monitor and control water, oil, and natural gas distribution, including pipelines, ships, trucks, rail systems, and wastewater collection systems.

SCADA systems and DCS are often networked together. This is the case for electric power control centers and generation facilities. Although electric power generation facility operation is controlled by a DCS, the DCS must communicate with the SCADA system to coordinate production output with transmission and distribution demands.

Electric power is often thought to be one of the most prevalent sources of disruptions of interdependent critical infrastructures. For example, a cascading failure can be initiated by a disruption of the microwave communications network used for an electric power transmission SCADA system. The lack of monitoring and control capabilities could cause a large generating unit to be taken offline and lead to the loss of power at a transmission substation. This loss could cause a major imbalance, triggering a cascading failure across the power grid and resulting in large area blackouts that potentially affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for electric power.

2.3. OT System Operation, Architectures, and Components

As **Fig. 1** depicts, a typical OT system contains numerous control loops, human-machine interfaces, and remote diagnostics and maintenance tools. The system is built using an array of network protocols on layered network architectures. Some critical processes may also include safety systems.

A *control loop* utilizes sensors, actuators, and controllers to manipulate some controlled process. A *sensor* is a device that produces a measurement of some physical property and then sends this information as *controlled variables* to the controller. The controller interprets the measurements and generates corresponding *manipulated variables* based on a control algorithm and target set points, which it transmits to the actuators. *Actuators* – such as control valves, breakers, switches, and motors – are used to directly manipulate the controlled process based on commands from the controller.

In a typical monitoring system, there are generally no direct connections between the sensors and any actuators. Sensor values are transmitted to a monitoring station to be analyzed by a human. However, these types of systems can still be considered OT systems (albeit with a human in the loop) because the objective of the monitoring system is likely to identify and ultimately mitigate an event or condition (e.g., a door alerting that it has been forced open, resulting in security personnel being sent to investigate; an environmental sensor that detects high temperatures in a server room, resulting in control center personnel activating an auxiliary air conditioning unit).

Operators and engineers use *human-machine interfaces (HMIs)* to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information. *Diagnostics and maintenance utilities* are used to prevent, identify, and recover from abnormal operation or failures.

Sometimes, control loops are nested and/or cascading, whereby the set point for one loop is based on the process variable determined by another loop. Supervisory-level loops and lower-level loops operate continuously over the duration of a process with cycle times ranging in the order of milliseconds to minutes.

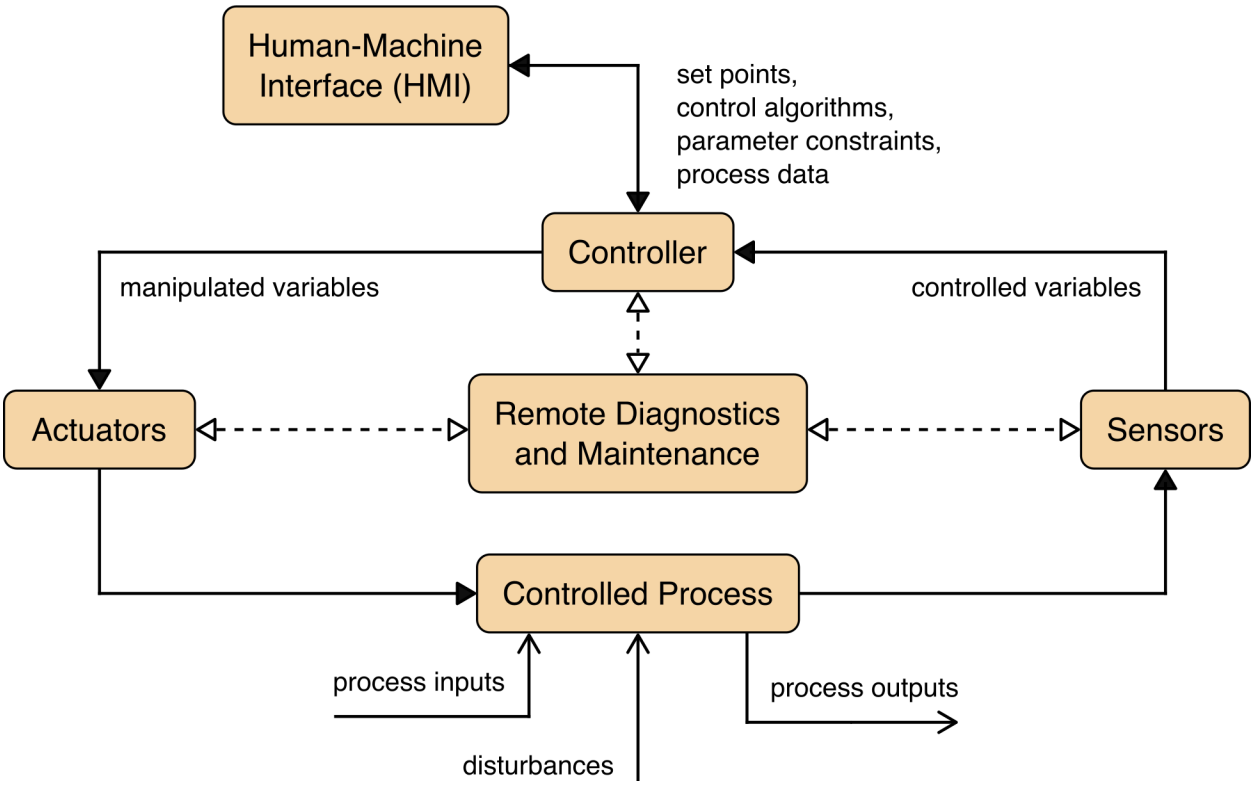

Fig. 1. Basic operation of a typical OT system

2.3.1. OT System Design Considerations

The design of an OT system depends on many factors, including whether a SCADA, DCS, or PLC-based topology is used. This section identifies key factors that drive design decisions regarding the control, communication, reliability, and redundancy properties of the OT system. Because these factors heavily influence the design of the OT system, they also help determine the system's security needs.

- **Safety.** Systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations, human oversight and control of a potentially dangerous process are essential.
- **Control timing requirements.** System processes have a wide range of time-related requirements, including very high speed, consistency, regularity, and synchronization. Humans may be unable to reliably and consistently meet these requirements, so automated controllers may be necessary. Some systems may require computation to be performed as close to sensors and actuators as possible to reduce communication latency and perform necessary control actions on time.
- **Geographic distribution.** Systems have varying degrees of distribution, ranging from a small system (e.g., local PLC-controlled process) to large, distributed systems (e.g., oil pipelines, electric power grids). Greater distribution typically implies a need for wide area networking (e.g., leased lines, circuit switching, packet switching) and mobile communication.

- **Hierarchy.** Supervisory control is used to provide a central location that can aggregate data from multiple locations to support control decisions based on the current state of the system. A hierarchical or centralized control is often used to provide human operators with a comprehensive view of the entire system.
- **Control complexity.** Simple controllers and preset algorithms can often perform control functions. However, more complex systems (e.g., air traffic control) require human operators to ensure that all control actions are appropriate for meeting the larger objectives of the system.
- **Availability.** Systems with strong availability and up-time requirements may require more redundancy or alternate implementations across all communications and controls.
- **Impact of failures.** The failure of a control function could cause substantially different impacts across domains. Systems with greater impacts often require the ability to continue operations through redundant controls or to operate in a degraded state.

2.3.2. SCADA Systems

Supervisory control and data acquisition (SCADA) systems are used to control dispersed assets for which centralized data acquisition is as important as control [Bailey][Boyer]. These systems are used in distribution systems, such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a control center, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real-time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands.

Typical hardware includes a control server placed at a control center, communications equipment (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field sites that consist of remote terminal units (RTUs) and/or PLCs that control actuators and/or monitor sensors. The control server stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process. The communications hardware allows for the transfer of information and data between the control server and the RTUs or PLCs. The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when a process variable changes outside of acceptable values. An intelligent electronic device (IED), such as a protective relay, may communicate directly to the control server, or a local RTU may poll the IEDs to collect the data and pass it to the control server. IEDs provide a direct interface to control and monitor equipment and sensors. IEDs may be directly polled and controlled by the control server and, in most cases, have local programming that allows for the IED to act without direct instructions from the control center. SCADA systems are usually designed to be fault-tolerant systems with significant redundancy built in, although redundancy may not be a sufficient countermeasure in the face of a malicious attack.

Figure 2 shows the components and general configuration of a SCADA system. The control center at the top of the diagram houses a control server and the communications routers. Other control center components include the HMI, engineering workstations, and the data historian, which are all connected by a local area network (LAN). The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based on detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting.

The field sites at the bottom of **Fig. 2** locally control actuators and monitor sensors. Field sites are often equipped with a remote access capability to allow operators to perform remote diagnostics and repairs, usually over a separate dial-up modem or wide area network (WAN) connection. Standard and proprietary communication protocols that run over serial and network communications are used to transport information between the control center and field sites using telemetry techniques, such as telephone line, cable, fiber, and radio frequencies (e.g., broadcast, microwave, satellite).

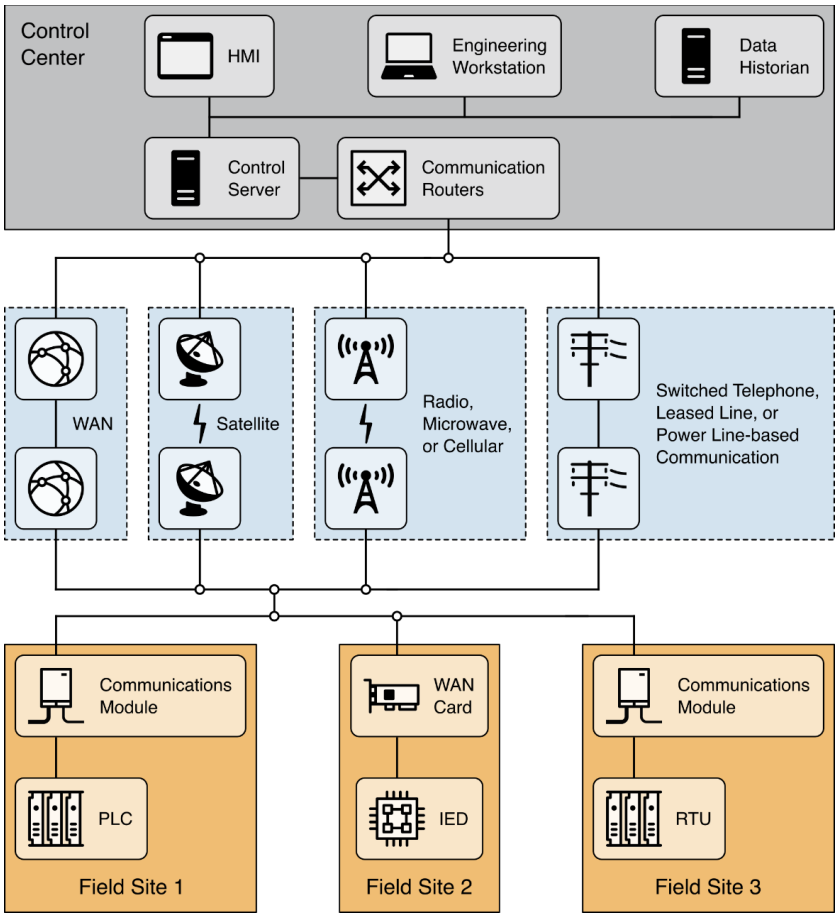

Fig. 2. A general SCADA system layout that shows control center devices, communications equipment, and field sites

SCADA communication topologies vary among implementations. The various topologies used are shown in **Fig. 3**, including point-to-point, series, series-star, and multi-drop [AGA12]. Point-to-point is functionally the simplest type, though it can be expensive because of the individual channels needed for each connection. In a series configuration, the number of channels used is reduced, though channel sharing impacts the efficiency and complexity of SCADA operations. Similarly, the series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and increased system complexity.

The four basic SCADA topologies shown in **Fig. 3** can be further augmented by using dedicated devices to manage communication exchanges and perform message switching and buffering.

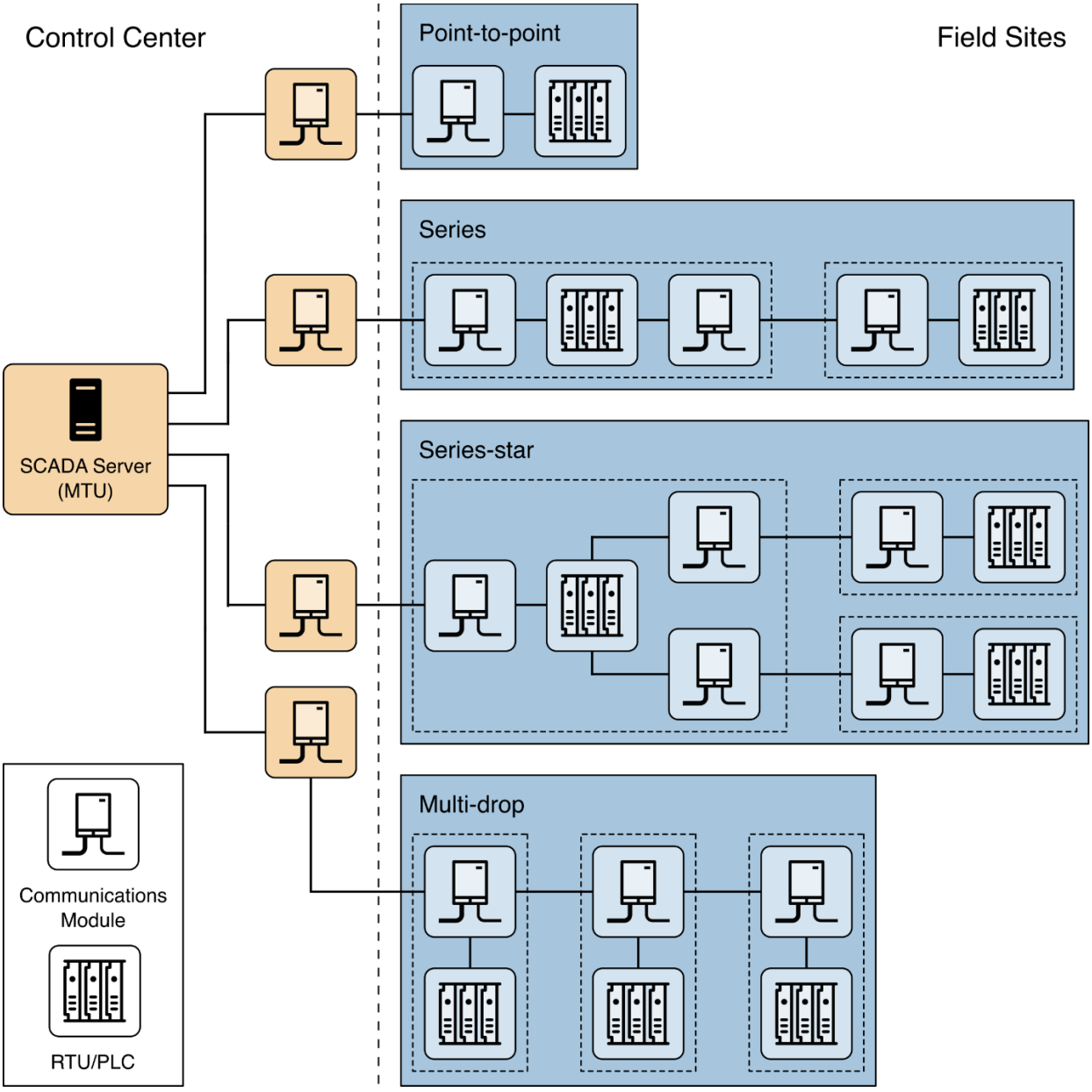

Fig. 3. Examples of point-to-point, series, series-star, and multi-drop SCADA communications topologies

Large SCADA systems that contain hundreds of RTUs often employ a sub-control server to alleviate the burden on the primary server. This type of topology is shown in **Fig. 4**.

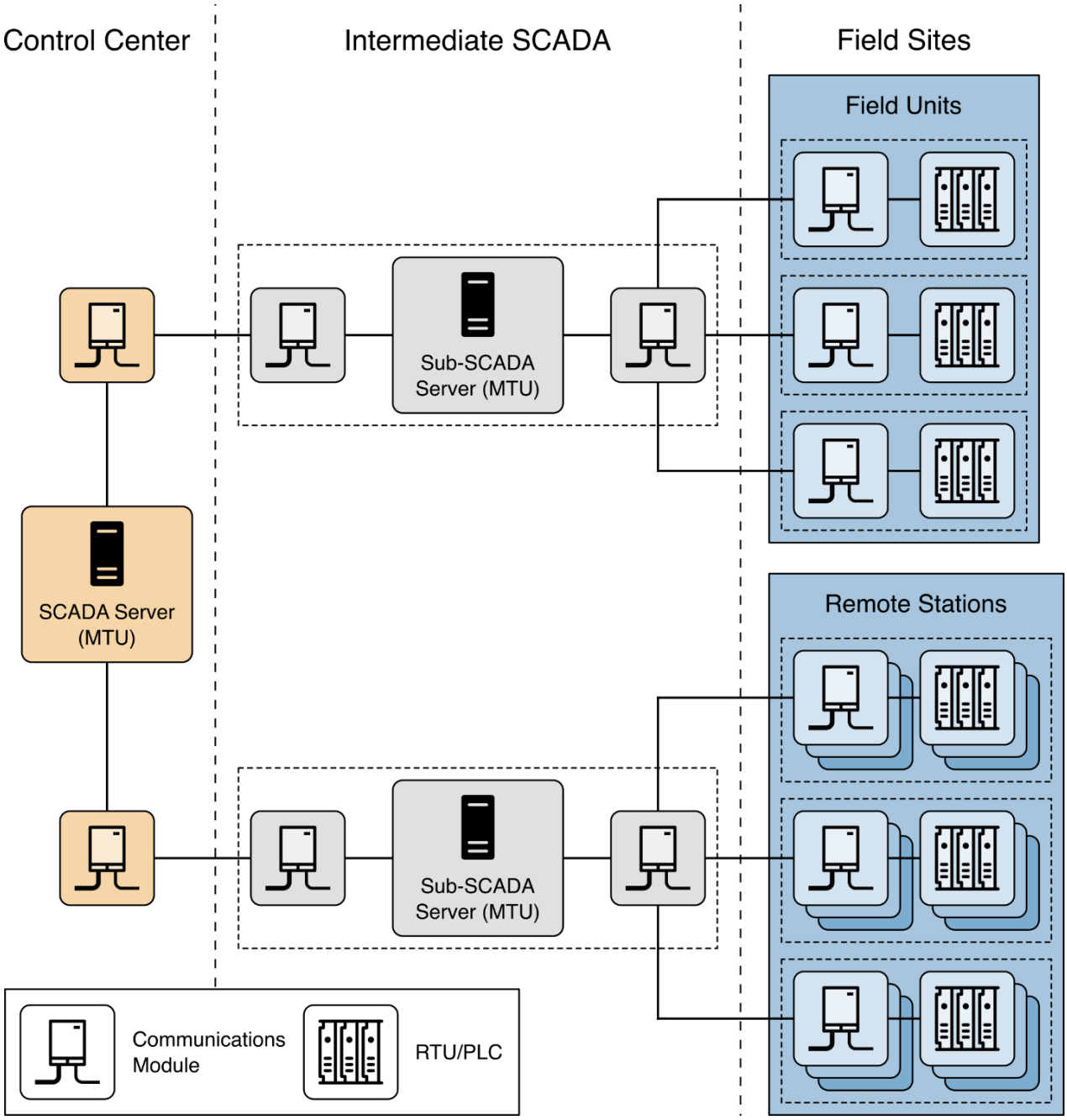

Fig. 4. An example SCADA topology that supports a large number of remote stations

Figure 5 shows an example SCADA system implementation that consists of a primary control center and three field sites. A second backup control center provides redundancy in the event of a primary control center malfunction. Point-to-point connections are used for all communications between the control center and field site, and two connections use radio telemetry. The third field site is local to the control center and uses the WAN for communications. A regional control center resides above the primary control center for a higher level of supervisory control. The corporate enterprise network has access to all control centers through the WAN, and field sites can be accessed remotely for troubleshooting and maintenance operations. The primary control center polls field devices for data at defined intervals (e.g., 5 seconds, 60 seconds) and can send new set points to field devices as required. In addition to polling and issuing high-level commands, the control server also watches for priority interrupts from field site alarm systems.

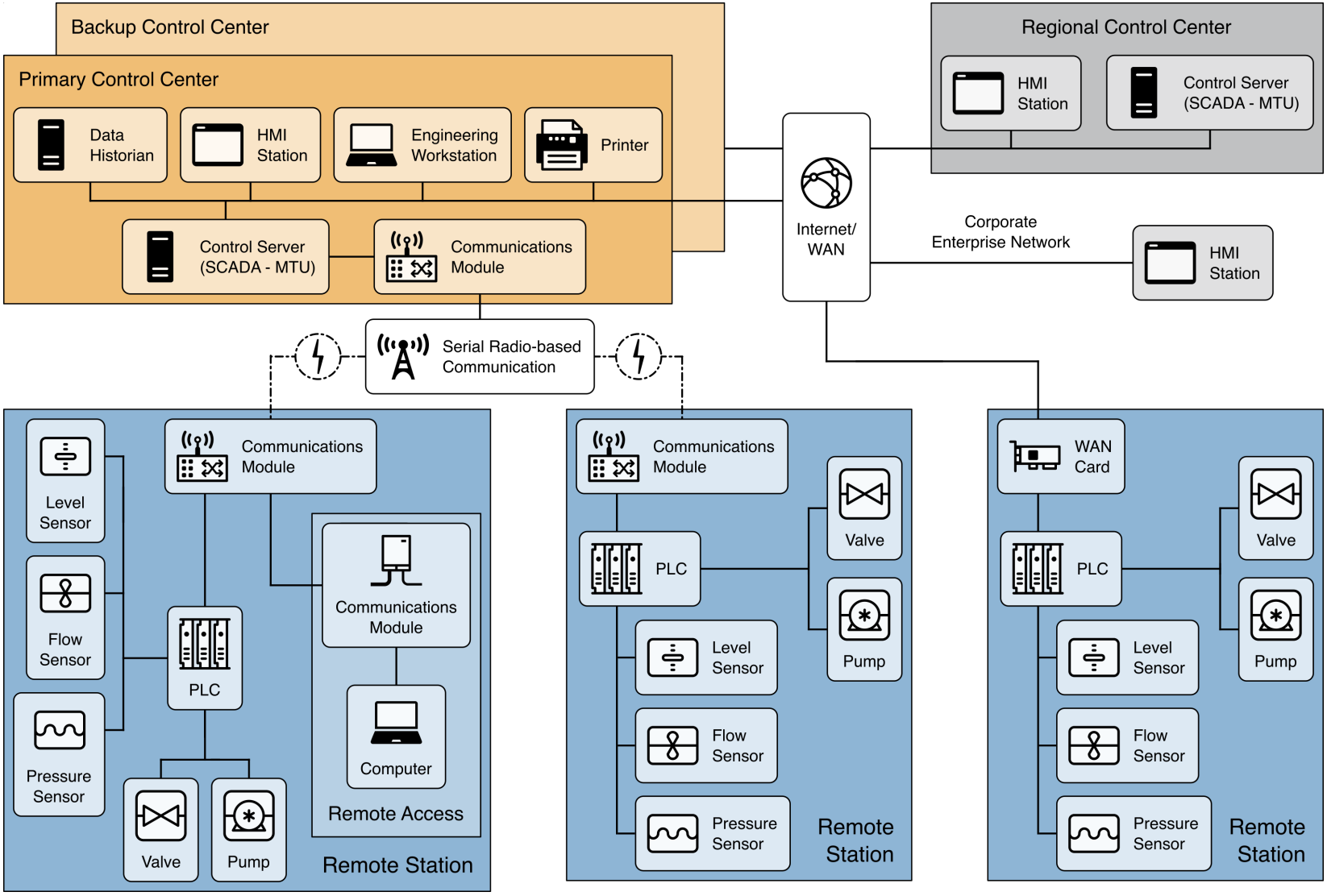

Fig. 5. A comprehensive SCADA system implementation example

Figure 6 shows an example implementation for rail monitoring and control. This example includes a rail control center that houses the SCADA system and three sections of a rail system. The SCADA system polls the rail sections for information, such as the status of the trains, signal systems, traction electrification systems, and ticket vending machines. This information is also fed to operator consoles at the HMI stations within the rail control center. The SCADA system monitors operator inputs at the rail control center and disperses high-level operator commands to the rail section components. In addition, the SCADA system monitors conditions at the individual rail sections and issues commands based on these conditions (e.g., stopping a train to prevent it from entering an area that has been flooded or is occupied by another train).

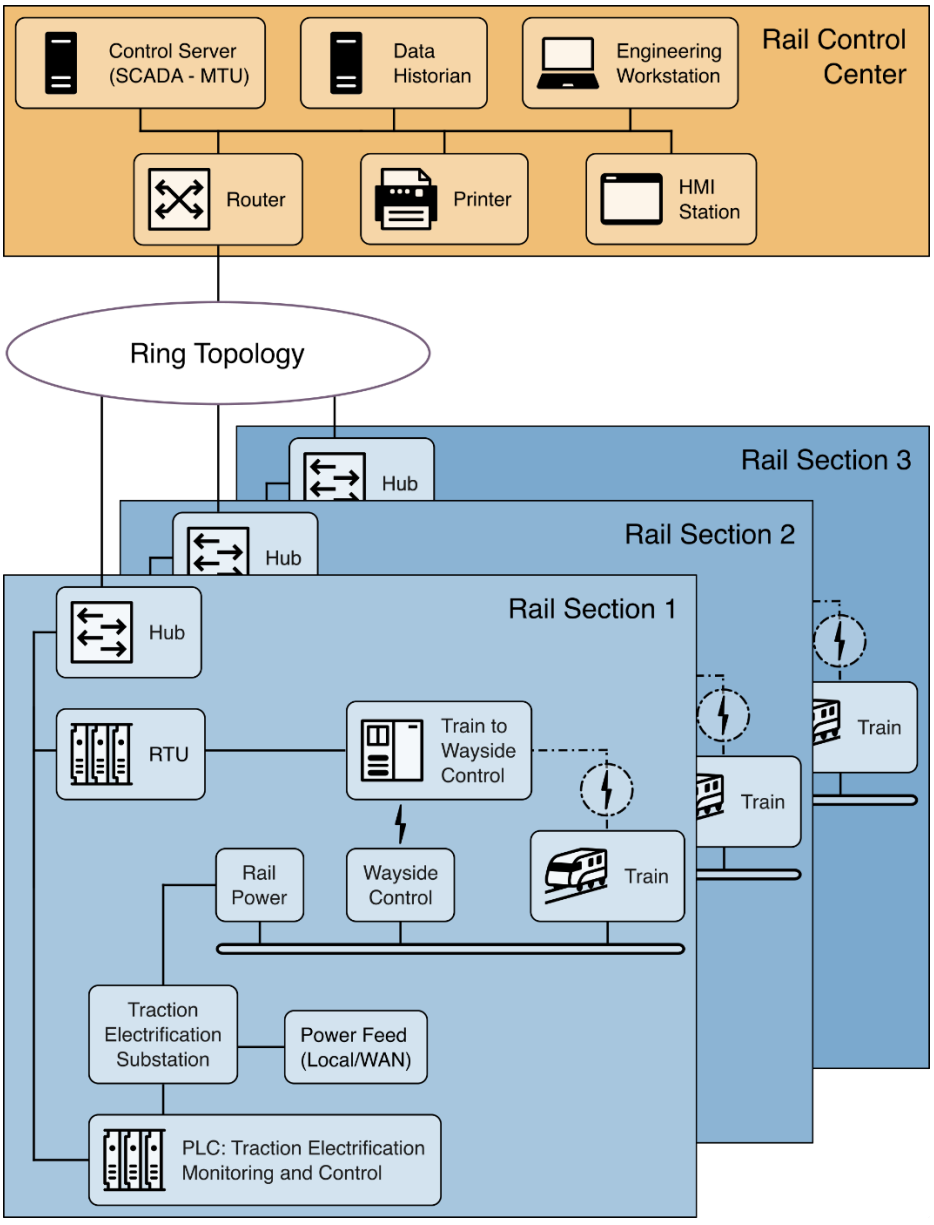

Fig. 6. An example rail monitoring and control SCADA system implementation

2.3.3. Distributed Control Systems

A distributed control system (DCS) is used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation, chemical manufacturing, automotive production, and pharmaceutical processing. These systems are usually process control or discrete part control systems.

A DCS is integrated as a control architecture that contains a supervisory level of control to oversee multiple integrated sub-systems that are responsible for controlling the details of a localized process. A DCS uses a centralized supervisory control loop to mediate a group of localized controllers that share the overall tasks of carrying out an entire production process [Erickson]. Product and process control are usually achieved by deploying feedback or feedforward control loops, whereby key product and/or process conditions are automatically maintained around a desired set point. Specific process controllers or more capable PLCs are employed in the field and tuned to provide the desired tolerance and the rate of self-correction during process upsets. By modularizing the production system, a DCS reduces the impact of a single fault on the overall system. In many modern systems, the DCS is interfaced with the corporate enterprise network to give business operations a view of production.

Figure 7 shows an example implementation of the components and general configuration of a DCS. This DCS encompasses an entire facility, from the bottom-level production processes up to the corporate enterprise layer. In this example, a supervisory controller (control server) communicates to its subordinates via a control network. The supervisor sends set points to and requests data from the distributed field controllers. The distributed controllers control their process actuators based on control server commands and sensor feedback from process sensors.

Figure 7 also gives examples of low-level controllers found on a DCS system. The field control devices shown include a machine controller, a PLC, and a process controller. The machine controller interfaces with sensors and actuators using point-to-point wiring, while the other three field devices incorporate fieldbus networks to interface with process sensors and actuators. Fieldbus networks eliminate the need for point-to-point wiring between a controller and individual field sensors and actuators. Additionally, a fieldbus allows for greater functionality beyond control, including field device diagnostics, and can accomplish control algorithms within the fieldbus, thereby avoiding signal routing back to the PLC for every control operation. Standard industrial communication protocols designed by industry groups such as Modbus and Fieldbus [Berge] are often used on control networks and fieldbus networks.

In addition to the supervisory-level and field-level control loops, intermediate levels of control may also exist. For example, in the case of a DCS controlling a discrete part manufacturing facility, there could be an intermediate level supervisor for each cell within the plant. This supervisor encompasses a manufacturing cell containing a machine controller that processes a part and a robot controller that handles raw stock and final products. There could be several of these cells that manage field-level controllers under the main DCS supervisory control loop.

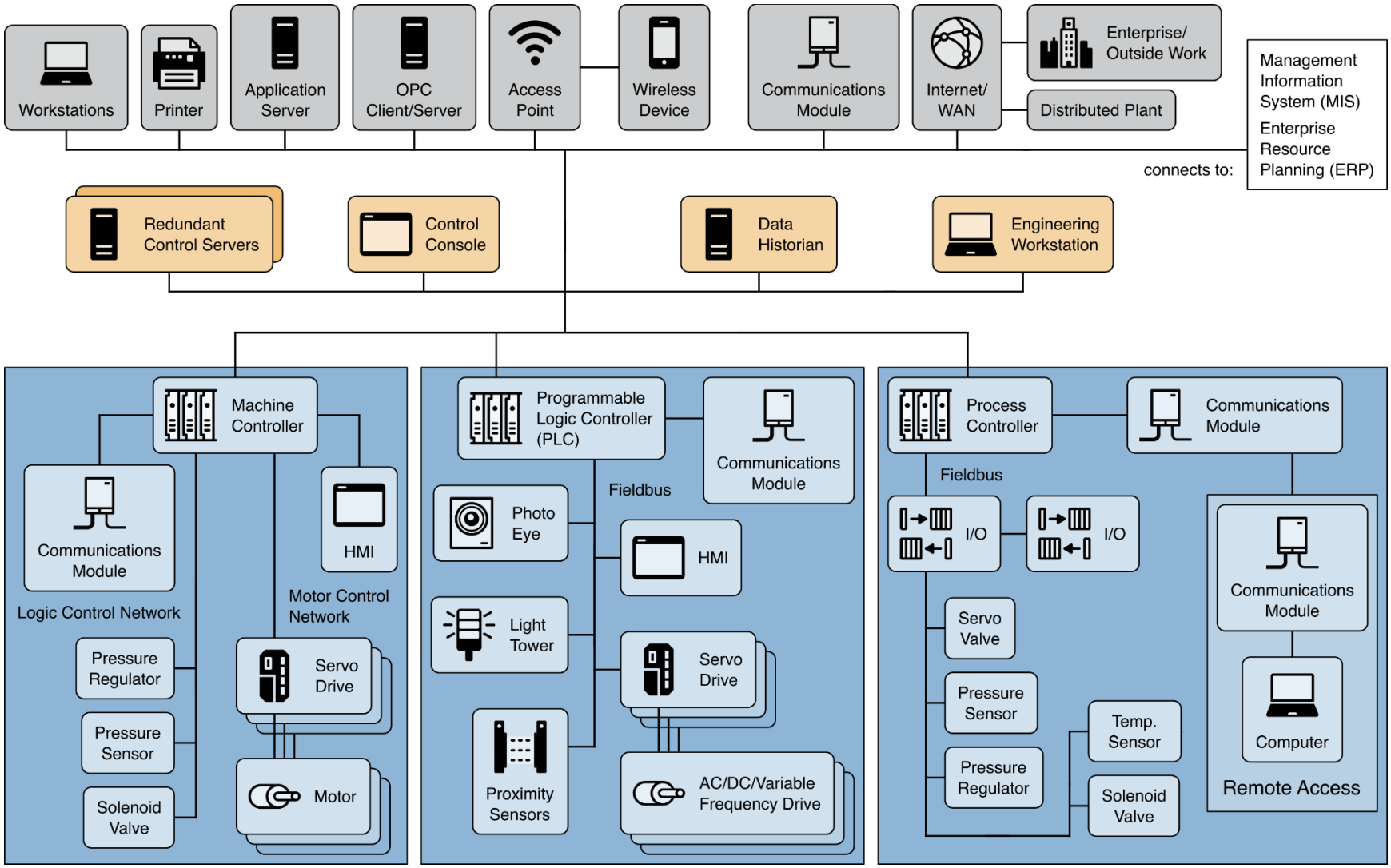

Fig. 7. A comprehensive DCS implementation example

2.3.4. Programmable Logic Controller-Based Topologies

PLCs are used in both SCADA and DCS systems as the control components of an overall hierarchical system to locally manage processes through feedback control, as described in the previous sections. In the case of SCADA systems, they may provide similar functionality to RTUs. When used in DCS systems, PLCs are implemented as local controllers within a supervisory control scheme.

PLCs can also be implemented as the primary controller in smaller OT system configurations to provide operational control of discrete processes (e.g., automobile assembly lines, process controllers). These topologies differ from SCADA and DCS in that they generally lack a central control server or HMI and, therefore, primarily provide closed-loop control with minimal human involvement. PLCs have a user-programmable memory for storing instructions for the purpose of implementing specific functions, such as I/O control, logic, timing, counting, three mode proportional-integral-derivative (PID) control, communications, arithmetic, and data and file processing.

Figure 8 shows a PLC over a fieldbus network performing the control of a manufacturing process. The PLC is accessible via a programming interface located on an engineering workstation, and data is stored in a data historian, all of which are connected on a LAN.

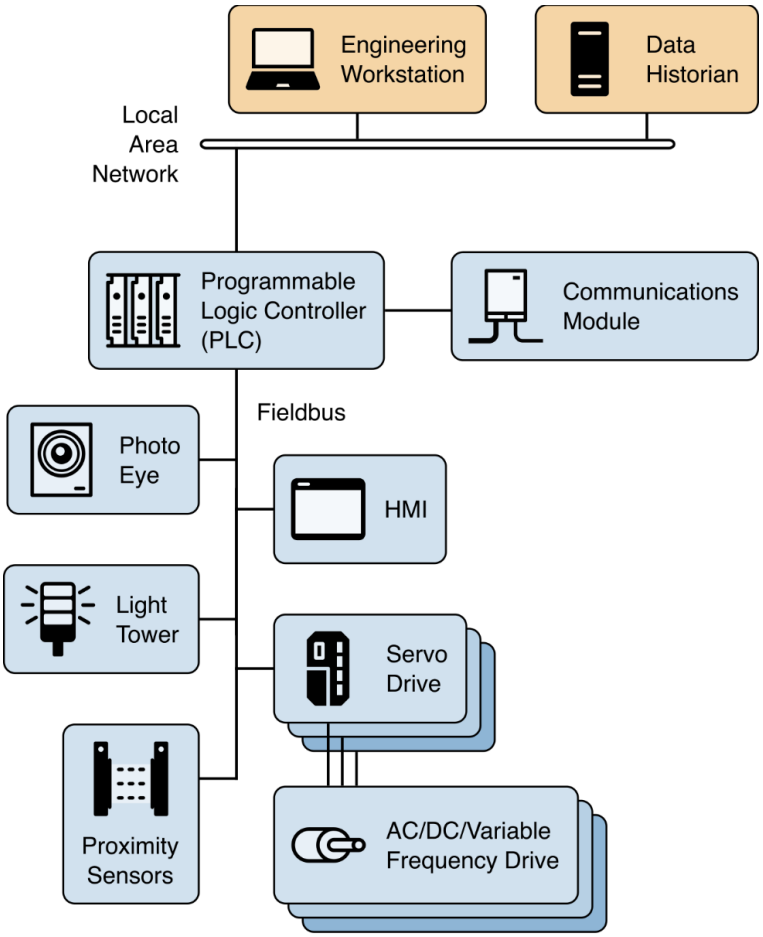

Fig. 8. A PLC control system implementation example

2.3.5. Building Automation Systems

A building automation system (BAS) is a type of OT used to control the many systems used in a building, including heating, ventilation, and air conditioning (HVAC); fire; electrical; lighting; physical access control; physical security; and other utility systems. Most modern buildings contain some form of a BAS when they are constructed. However, older buildings and equipment may have to be retrofitted to take advantage of the benefits that a BAS provides.

Some of the most common functions of a BAS include maintaining environmental conditions for occupant comfort, reducing energy consumption, reducing operating and maintenance costs, increasing security, recording historical data (e.g., temperature, humidity), and performing general equipment monitoring (e.g., provide alerts to building personnel of device failure or an alarm condition).

An example of a BAS is shown in **Fig. 9**. A BAS may communicate over wired or wireless paths to controllers or gateways. For example, environmental control sensors can provide the temperature and humidity to a building controller. If the sensor values are outside of the set points, the controller can signal a variable air volume (VAV) box to increase or decrease airflow and bring the temperature to the desired state. Similarly, a building occupant scanning their identification badge at a badge reader can result in the credentials being sent to the access control controller and application control server to determine whether access should be granted.

While this guide contains recommendations that are applicable and could be used as a reference to protect a BAS against cybersecurity threats, readers are encouraged to perform a risk-based assessment on their systems and tailor the recommended guidelines and solutions to meet their specific security, business, and operational requirements.

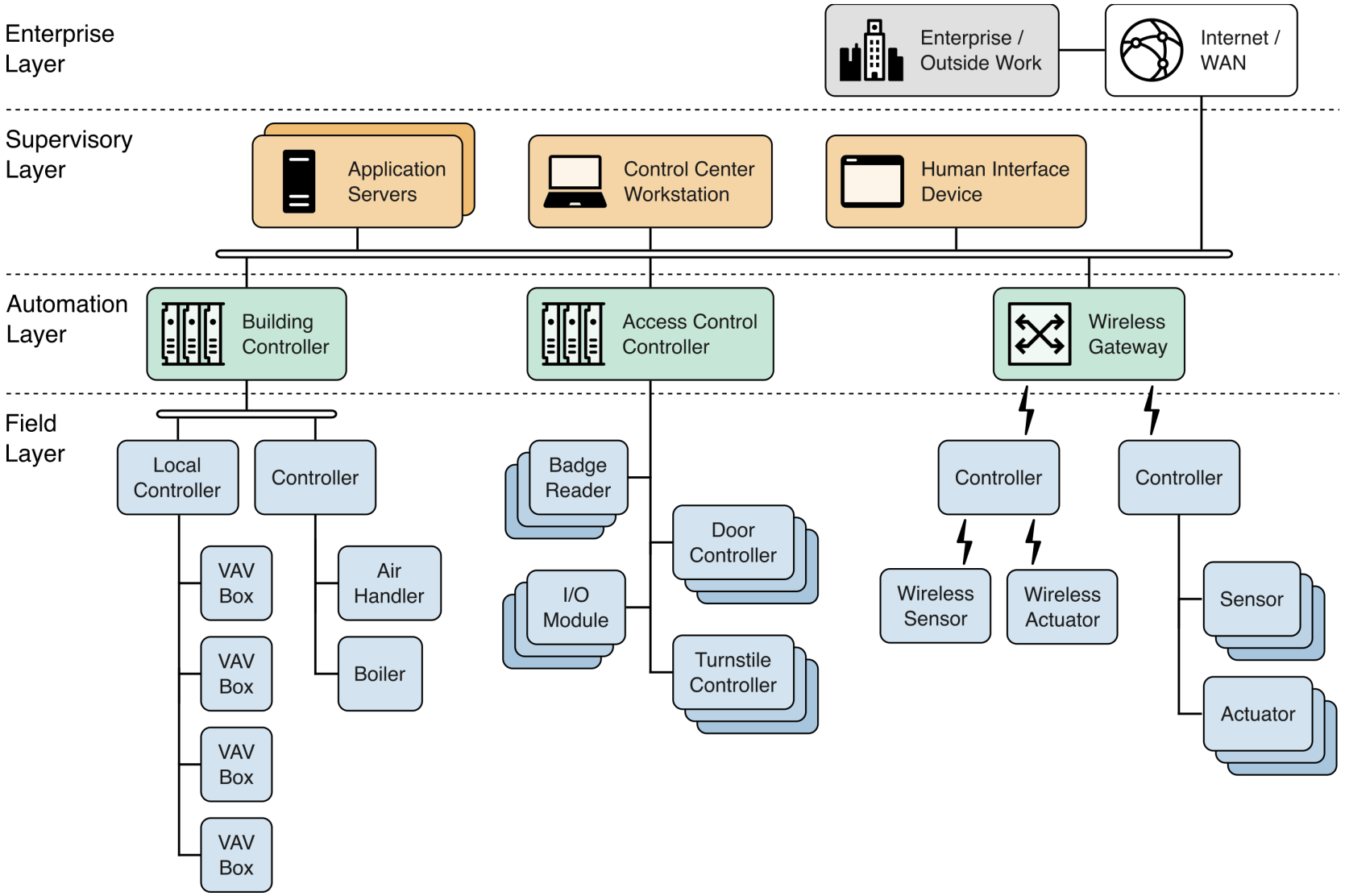

Fig. 9. A BAS implementation example

2.3.6. Physical Access Control Systems

A physical access control system (PACS) is a type of physical security system designed to control access to an area. Unlike standard physical barriers, physical access control can control who is granted access, when the access is granted, and how long the access should last.

An *access point* is the entrance or barrier where access control is required. Some common physical access control examples of access points are doors and locks, security gates, turnstiles, and vehicular gate arms. Depending on the type of facility, there can be a single access point (e.g., for high-security areas) or many (e.g., for a large office building).

An identification (ID) or personal credential is used to identify the authorized user trying to gain access to the area or facility. A PACS often requires a user to have credentials to gain entrance to a facility or access sensitive data. Examples of identification credentials include simple controls (e.g., PIN codes, passwords, key fobs, key cards) and more advanced credentials (e.g., encrypted badges, mobile credentials). Identification credentials allow the system to know who is attempting to gain access and to maintain access logs.

Readers and/or keypads are typically located at the access point. The reader reads the data and sends it to a door controller to validate the credential and determine whether access should be authorized. If a keypad or biometric reader is also required (i.e., for multi-factor authentication), the user will enter their PIN or perform the biometric scan following their credential scan. An example of a PACS is shown in **Fig. 10**.

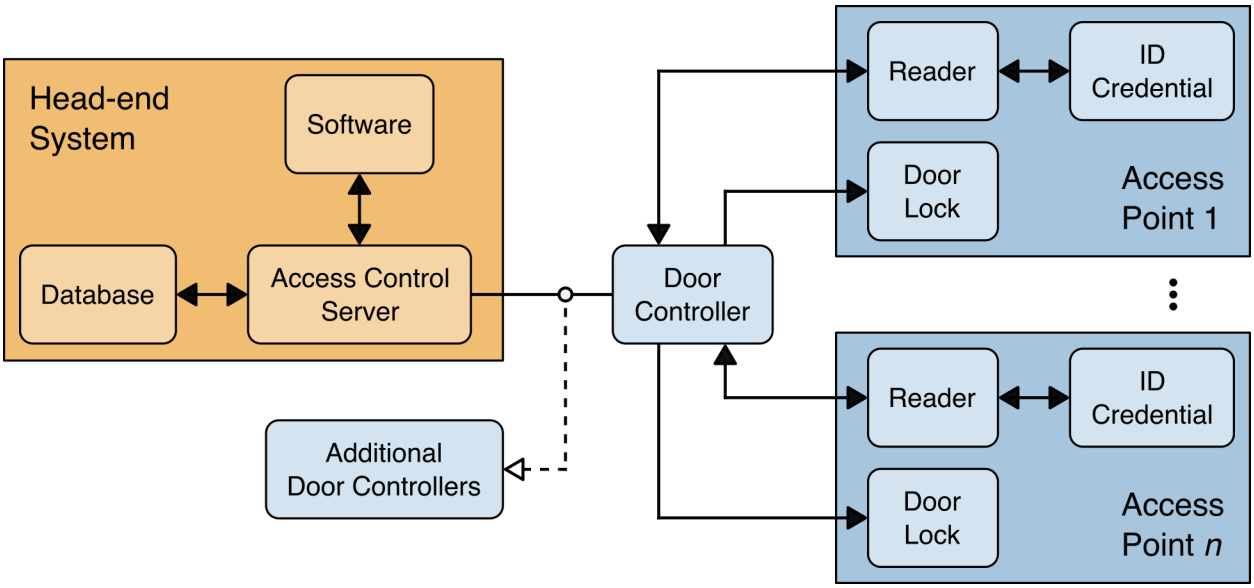

Fig. 10. A PACS implementation example

In this example, the door controller receives credential data from the reader and verifies the identification credential. If the credential is approved by the access control server, the control panel transmits the command to authorize access and unlock the door. If the credential is denied, the door will remain locked, and the user will not be able to gain entry. All access attempts are logged by the door controller(s) and, ultimately, the access control server. The access control

server is the repository for user information, access privileges, and audit logs. Depending on the system, the server might be on-premises or managed in the cloud.

While this guide contains recommendations that are applicable and could be used as a reference to protect a PACS against cybersecurity threats, readers are encouraged to perform a risk-based assessment on their systems and tailor the recommended guidelines and solutions to meet their specific security, business, and operational requirements.

2.3.7. Safety Systems

Many of the physical processes that OT systems control have the potential to create hazardous situations to human life and safety, property, and the environment. Safety systems are designed to reduce the likelihood and/or consequence of these potentially hazardous situations by bringing the system to a safe state. There are several types of safety systems related to OT environments, including emergency shut down (ESD), process safety shutdown (PSS), and fire and gas systems (FGS).

One of the more well-known types of safety system is the safety instrumented system (SIS), which is composed of one or more safety instrumented functions (SIFs). An SIF is an engineered system that is typically comprised of sensors, logic solvers, and final control elements (e.g., actuators) whose purpose is to bring a system to a safe state when predetermined thresholds are violated. An SIS is implemented as part of an overall risk reduction strategy to reduce the likelihood and/or potential consequences of a previously identified event so that it is within the organization's risk tolerance. Although numerous other terms are associated with safety systems, the SIS is specifically designed in accordance with [IEC61511]. An SIS is typically found in chemical, refinery, and nuclear processes.

An SIS is often independent from all other control systems in such a manner that a failure of the basic process control system (BPCS) will not impact SIS functionality in a deleterious manner. Historically, an SIS was designed to be stand-alone, physically and logically separated, and air-gapped from the rest of the control system. In the configuration shown in **Fig. 11**, the SIS and BPCS operate completely independent of each other with no direct communication between the systems. However, some modern SISs have been designed to allow communication with the control system. These types of SISs are called Integrated Control and Safety Systems (ICSSs). An ICSS solution may be an all-in-one device from a single vendor or incorporate multiple devices from multiple vendors. While an ICSS combines the functionality of both control and safety systems, the SIS must still comply with the requirements outlined in [IEC61511]. One of the advantages to this ICSS methodology is the ability to communicate information from the SIS to the BPCS.

While this guide contains recommendations that are applicable and could be used as a reference to protect safety systems against cybersecurity threats, readers are encouraged to perform a risk-based assessment on their systems and tailor the recommended guidelines and solutions to meet their specific security, business, and operational requirements.

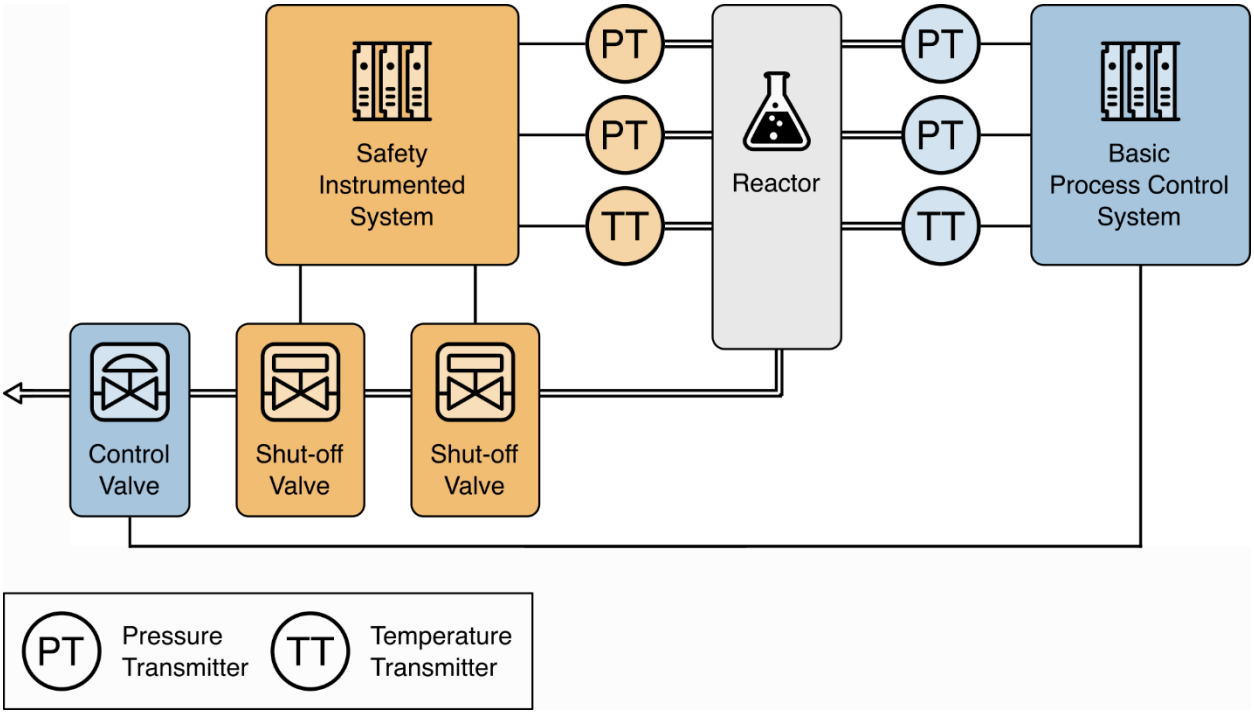

Fig. 11. An SIS implementation example

2.3.8. Industrial Internet of Things

The Industrial Internet of Things (IIoT) consists of sensors, instruments, machines, and other devices that are networked together and use internet connectivity to enhance industrial and manufacturing business processes and applications [Berge]. As IT and OT systems continue to converge and become even more interconnected, the control of physical processes remains a relatively unique and critical concept of OT.

The Industry IoT Consortium proposes a three-tier system architecture model for representing IIoT systems [IIRA19]: the edge tier, platform tier, and enterprise tier. Each tier plays a specific role in processing the data flows and control flows involved in usage activities. The tiers are connected by three networks: the proximity network, access network, and service network. An example architecture is shown in **Fig. 12**.

The enterprise tier implements domain-specific applications and decision support systems, provides interfaces to end users, receives data flows from the other tiers, and issues control commands to the other tiers.

The platform tier receives, processes, and forwards control commands from the enterprise tier to the edge tier. It consolidates processes and analyzes data flows from the other tiers, provides management functions for devices and assets, and offers non-domain-specific services, such as data query and analytics. Based on the specific implementation, these functions can be implemented on the IIoT platform that is deployed in an on-site data center, an off-site data center, or in the cloud.

The service network enables connectivity between the services in the platform tier, the enterprise tier, and the services within each tier. This connectivity may be an overlay private network over

the public internet or the internet itself, allowing enterprise-grade security between end users and services.

The edge tier collects data from the edge nodes using the proximity network. The architectural characteristics of this tier vary depending on the specific implementation (e.g., geographical distribution, physical location, governance scope). It is a logical layer rather than a true physical division. From a business perspective, the location of the edge depends on the business objectives.

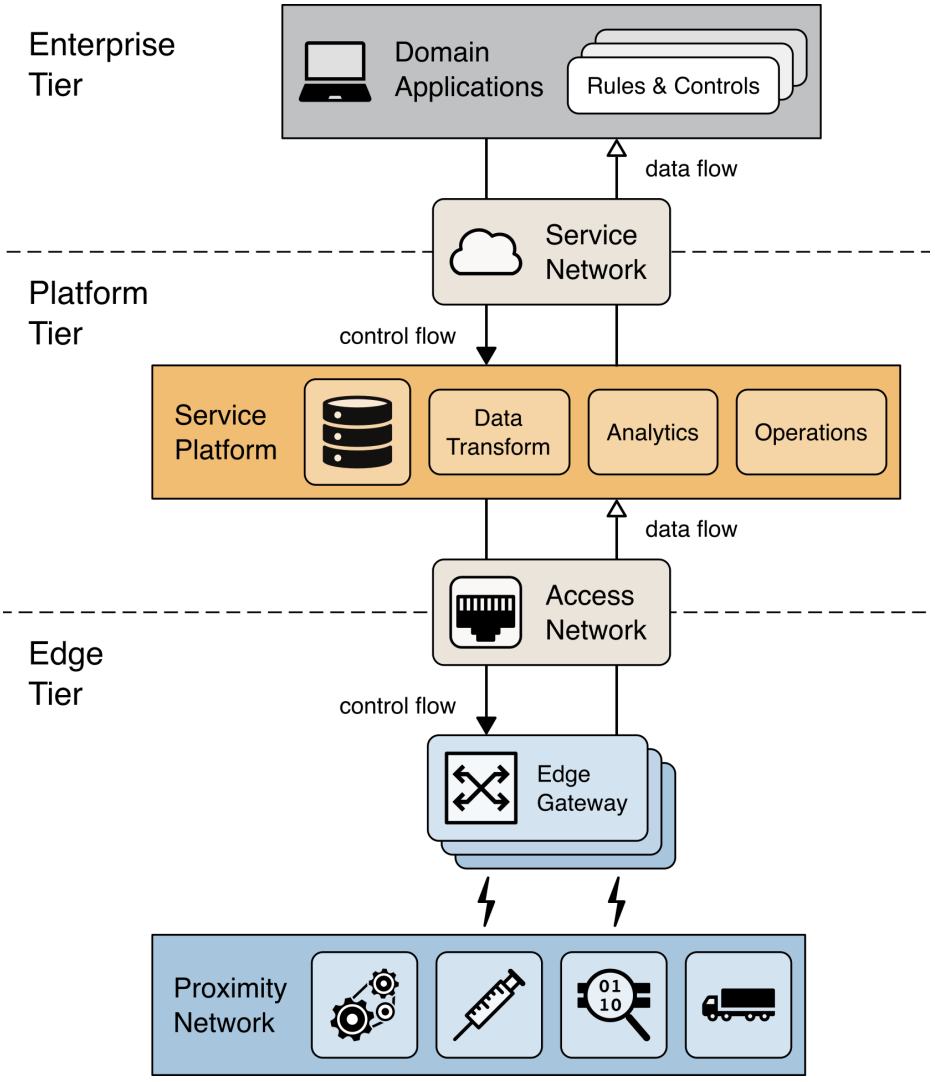

Fig. 12. A three-tiered IIoT system architecture

Edge computing is a decentralized computing infrastructure in which computing resources and application services can be distributed along the communication path between the data source and the cloud. It exists vertically within the full stack (i.e., from the device to the cloud) and horizontally across IIoT subsystems. The edge is not merely a way to collect data for transmission to the datacenter or cloud; it also processes, analyzes, and acts on data collected at the edge and is, therefore, essential for optimizing industrial data at every aspect of an operation.

The IIoT system architecture is fully distributed and can support a wide range of interactions and communication paradigms, including:

- Peer-to-peer networking (e.g., security cameras communicating about identified objects)
- Edge-device collaboration (e.g., wind turbines in remote locations)
- Distributed queries across data stored in devices, in the cloud, and anywhere in between
- Distributed data management that defines where and what data is to be stored and for how long
- Data governance, including quality, discovery, usability, privacy, and security

The proximity network connects edge nodes (e.g., sensors, actuators, devices, OT systems and assets) to the stack. It typically connects these edge nodes as one or more clusters to a gateway that bridges to other networks. The access network enables connectivity for data and control flow between the edge and platform tiers. This connection may be a corporate network or an overlay private network over the public internet or a 4G/5G network.

While this guide contains recommendations that are applicable and could be used as a reference to protect IIoT against cybersecurity threats, readers are encouraged to perform a risk-based assessment on their systems and tailor the recommended guidelines and solutions to meet their specific security, business, and operational requirements.

2.4. Comparing OT and IT System Security

OT has many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues, such as production losses. OT has different performance and reliability requirements and uses OSs and applications that may be considered unconventional in a typical IT network environment. Security protections must be implemented in a way that maintains system integrity during normal operations as well as during cyber attacks [Knapp].

Initially, OT systems had little resemblance to IT systems because they were isolated and ran proprietary control protocols using specialized hardware and software. Widely available and low-cost Ethernet, Internet Protocol (IP), and wireless devices are now replacing older proprietary technologies, which increases the likelihood of cybersecurity vulnerabilities and incidents. OT are increasingly resembling IT systems as they adopt IT technologies to promote corporate connectivity and remote access capabilities (e.g., using industry standard computers, OSs, and network protocols). This integration supports new IT capabilities but provides significantly less isolation for OT from the outside world than predecessor systems, creating a greater need to secure them. While security solutions have been designed to deal with these issues in typical IT systems, special precautions must be taken when introducing these same solutions to OT environments. In some cases, new security solutions are needed that are tailored to the OT environment.

Some special considerations when securing OT include:

- **Timeliness and performance requirements.** OT systems are generally time-critical, with the criterion for acceptable levels of delay and jitter dictated by the individual installation. Some systems require reliable, deterministic responses. High throughput is typically not essential to OT. In contrast, IT systems typically require high throughput and can withstand some level of delay and jitter. For some OT, automated response times or system responses to human interaction is critical. Many OT systems utilize real-time OSs (RTOS), where real-time refers to timeliness requirements. The units of real time are highly application-dependent and must be explicitly stated.
- **Availability requirements.** Many OT processes are continuous in nature. Unexpected outages of systems that control industrial processes are unacceptable. Outages must often be planned and scheduled days or weeks in advance. Exhaustive pre-deployment testing is essential to ensuring high availability (i.e., reliability) for the OT. OT systems often cannot be stopped and started without affecting production. In some cases, the products produced or equipment being used are more important than the information being relayed. Therefore, typical IT strategies (e.g., rebooting a component) are usually not acceptable for OT due to adverse impacts on the requirements for high availability, reliability, and maintainability. Some OT employ redundant components – often running in parallel – to provide continuity when primary components are unavailable.
- **Risk management requirements.** In a typical IT system, primary concerns include data confidentiality and integrity. For OT, primary concerns include safety, fault tolerance to prevent the loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products. The personnel responsible for operating, securing, and maintaining OT must understand the important link between safety and security. Any security measure that impairs safety is unacceptable.
- **Physical effects.** Field devices (e.g., PLCs, operator stations, DCS controllers) are directly responsible for controlling physical processes. OT can have complex interactions with physical processes and consequences in the OT domain that can manifest in physical events. Understanding these potential physical effects often requires communication between experts in OT and experts in the particular physical domain.
- **System operation.** OT OSs and control networks are often quite different from their IT counterparts and require different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers rather than IT personnel. Assuming that differences are insignificant can have disastrous consequences on system operations.
- **Resource constraints.** OT and their real-time operating systems (RTOSs) are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems often lack resources that are common on modern IT systems. Many systems may also lack desired features, including encryption capabilities, error logging, and password protection. Indiscriminate use of IT security practices in OT may cause availability and timing disruptions. There may not be computing resources available on OT components to retrofit these systems with current security capabilities. Adding resources or features may not be possible.

- **Communications.** Communication protocols and media used by OT environments for field device control and intra-processor communication are typically different from IT environments and may be proprietary.
- **Change management.** Change management is paramount to maintaining the integrity of both IT and OT systems. Unpatched software represents one of the greatest vulnerabilities to a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policies and procedures. In addition, these procedures are often automated using server-based tools. Software updates on OT cannot always be implemented on a timely basis. These updates need to be thoroughly tested by both the vendor and the end user of the industrial control application before being implemented. Additionally, the OT owner must plan and schedule OT outages days or weeks in advance. The OT may also require revalidation as part of the update process. Another issue is that many OT utilize older versions of OSs that are no longer supported by the vendor through patches. Change management is also applicable to hardware and firmware. The change management process requires careful assessment by OT experts (e.g., control engineers) working in conjunction with security and IT personnel.
- **Managed support.** Typical IT systems allow for diversified support styles, perhaps supporting disparate but interconnected technology architectures. For OT, service support is sometimes only available from a single vendor. In some instances, third-party security solutions are not allowed due to OT vendor licensing and service agreements, and service support can be lost if third-party applications are installed without vendor acknowledgement or approval.
- **Component lifetime.** Typical IT components have a lifetime on the order of three to five years due to the quick evolution of technology. For OT, where technology has been developed in many cases for specific uses and implementations, the lifetime of the deployed technology is often in the order of 10 to 15 years and sometimes longer.
- **Component location.** Most IT components and some OT components are located in business and commercial facilities that are physically accessible by local transportation. Remote locations may be utilized for backup facilities. Distributed OT components may be isolated, remote, and require extensive transportation effort to reach. The component location also needs to consider necessary physical and environmental security measures.

Table 1 summarizes some of the typical differences between IT and OT systems.

Table 1. Summary of typical differences between IT and OT systems

Category	Information Technology	Operational Technology
Performance Requirements	Non-real time Response must be consistent. High throughput is demanded. High delay and jitter may be acceptable. Emergency interaction is less critical. Tightly restricted access control can be implemented to the degree necessary for security.	Real-time Response is time-critical. Modest throughput is acceptable. High delay and/or jitter is unacceptable. Response to human and other emergency interaction is critical. Access to OT should be strictly controlled but should not hamper or interfere with human-machine interaction.

Category	Information Technology	Operational Technology
Availability (Reliability) Requirements	Responses such as rebooting are acceptable. Availability deficiencies can often be tolerated, depending on the system's operational requirements.	Responses such as rebooting may not be acceptable because of process availability requirements. Availability requirements may necessitate redundant systems. Outages must be planned and scheduled days or weeks in advance. High availability requires exhaustive pre-deployment testing.
Risk Management Requirements	Manage data Data confidentiality and integrity is paramount. Fault tolerance is less important; momentary downtime is not a major risk. The major risk impact is a delay of business operations.	Control physical world Human safety is paramount, followed by protection of the process. Fault tolerance is essential; even momentary downtime may be unacceptable. The major risk impacts are regulatory non-compliance, environmental impacts, and the loss of life, equipment, or production.
System Operation	Systems are designed for use with typical OSs. Upgrades are straightforward with the availability of automated deployment tools.	Systems often use different and possibly proprietary OSs, sometimes without security capabilities built in. Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and potentially modified hardware and software involved.
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications, such as security solutions.	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities.
Communications	Standard IT communications protocols are used. Primarily wired networks with some localized wireless capabilities. Typical IT networking practices are employed.	Many proprietary and standard communication protocols are used. Several types of communications media are used, including dedicated wired and wireless (e.g., radio and satellite). Complex networks exist that sometimes require the expertise of control engineers.
Change Management	Software changes are applied in a timely fashion in the presence of good security policies and procedures, and the procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the OT system is maintained. OT outages must often be planned and scheduled days or weeks in advance. OT may use OSs that are no longer supported. OT systems often have custom applications.
Managed Support	Allow for diversified support styles	Service support is usually provided through a single vendor.
Component Lifetime	Lifetime on the order of three to five years	Lifetime on the order of 10 to 15 years
Components Location	Components are usually local and easy to access.	Components can be isolated, remote, and require extensive physical effort to gain access to them.

In summary, the operational and risk differences between IT and OT systems create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators, and IT security professionals must work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with OT need to understand the reliability impacts of information security technologies before deployment. Moreover, some of the OSs and applications that run on OT may not operate correctly with commercial-off-the-shelf (COTS) IT cybersecurity solutions because of their unique requirements.

3. OT Cybersecurity Program Development

To mitigate cybersecurity risks to their OT systems, organizations need to develop and deploy an OT cybersecurity program. It should be consistent and integrated with existing IT cybersecurity programs and practices but also account for the specific requirements and characteristics of OT systems and environments. Organizations should regularly review and update their OT cybersecurity plans and programs to reflect changes in technologies, operations, standards, regulations, and the security needs of specific facilities.

Effective integration of cybersecurity into the operation of OT requires defining and executing a comprehensive program that addresses all aspects of cybersecurity. This includes defining the objectives and scope of the program; establishing a cross-functional team that understands OT and cybersecurity; establishing policies and procedures; identifying cyber risk management capabilities that include people, processes, and technologies; and identifying day-to-day operations of event monitoring and auditing for compliance and improvement.

When a new system is being designed and installed, it is imperative to take the time to address security throughout the life cycle, including architecture, procurement, installation, maintenance, and decommissioning. Deploying systems to the field based on the assumption that these systems will be secured later introduces significant risks to the systems and the organization. If there are not enough time and resources to properly secure the system before deployment, it is unlikely that security will be addressed at a later time. Since new OT systems are designed and deployed less frequently than IT systems, it is much more common to improve, expand, or update an existing OT system than to design a new one.

This section introduces the basic process for developing an OT cybersecurity program and applies to new and deployed OT systems. Additional guidance for developing the specific elements of an OT cybersecurity program can be found in Section 3.3.10.

3.1. Establish a Charter for the OT Cybersecurity Program

Senior management must demonstrate a clear commitment to cybersecurity and communicate its importance throughout the organization. Cybersecurity is a business responsibility shared by all members of the organization, especially by its leaders and IT and OT teams. Commitment to cybersecurity can be demonstrated by establishing a charter for a cybersecurity program with adequate funding, visibility, governance, and support from senior leaders. A cybersecurity program that has commitment from senior management is more likely to achieve the mission and business goals of the organization.

A charter for a cybersecurity program is a plain-language high-level description that establishes clear ownership and accountability for protecting OT resources and provides a mandate for the most senior person responsible to establish and maintain the cybersecurity program (e.g., CISO). This section focuses on an OT-specific program, which should be integrated with the organization's overall cybersecurity program.

A cybersecurity program charter should include program objectives, scope, and responsibilities. Senior management establishes the OT cybersecurity program charter and identifies an OT cybersecurity manager with appropriate authority to lead the OT cybersecurity program. The OT cybersecurity manager should define the roles and responsibilities of system owners, mission and business process managers, and users. The OT cybersecurity manager should also document the

objectives and scope of the OT security program, including the business organizations affected, the systems and networks involved, the budget and resources required, and the division of responsibilities.

The organization may already have an information security program in place or have developed one for its IT systems. The OT cybersecurity manager should identify which existing practices to leverage and which practices are specific to the OT system. Ultimately, it will be more effective for the team to share resources with others in the organization that have similar objectives.

3.2. Business Case for the OT Cybersecurity Program

The cybersecurity of OT systems is a critical component in the overall security of the organization. Cybersecurity events could potentially impact the organization's mission and objectives, the environment, regulatory compliance, and even human safety. OT systems can also be used as an entry point to organizational IT systems and other enterprise systems. As OT systems are increasingly being connected to IT networks, relying on traditional measures (e.g., air gaps) is not enough to protect such systems from cyber attacks. Therefore, security measures tailored to the OT system are required to protect the organization. An OT cybersecurity program considers the characteristics of OT systems that require special consideration in order to mitigate these risks.

3.2.1. Benefits of Cybersecurity Investments

OT cybersecurity supports the mission and business functions of the organization and provides additional benefits, including:

- Improving OT system safety, reliability, and availability
- Improving OT system efficiency
- Reducing community concerns
- Reducing legal liabilities
- Meeting regulatory requirements
- Helping with insurance coverage and costs

A strong OT cybersecurity program is fundamental to a sustainable business operation and can potentially enhance system reliability and availability. This includes minimizing unintentional OT system information security impacts from inappropriate testing, policies, and misconfigured systems. Cyber attacks can also have other significant impacts, such as:

- **Physical impacts.** Physical impacts encompass the set of direct consequences of OT failure, particularly personal injury and the loss of life. Other effects include the loss of property (including data) and potential damage to the environment.
- **Economic impacts.** Economic impacts are a second-order effect of physical impacts that ensue from an OT incident, which in turn inflict a greater economic loss on the facility, organization, or others who are dependent on the OT systems. The unavailability of critical infrastructure (e.g., electrical power, transportation) can have economic impacts

far beyond the systems that sustain direct and physical damage. These effects could negatively impact the local, regional, national, or possibly global economy.

- **Social impacts**. Another second-order effect is the loss of national or public confidence in an organization.

Additional examples of the potential consequences of an OT incident are listed below. Note that items in this list are not independent. For example, the release of hazardous material could lead to injury or death.

- Impact on national security (e.g., facilitate an act of terrorism)
- Reduction or loss of production at one site or multiple sites simultaneously
- Injury or death of employees
- Injury or death of persons in the community
- Damage to equipment
- Release, diversion, or theft of hazardous materials
- Environmental damage
- Violation of regulatory requirements
- Product contamination
- Criminal or civil legal liabilities
- Loss of proprietary or confidential information
- Loss of brand image or customer confidence

Safety and security incidents can have negative impacts that last longer than other types of incidents on all stakeholders, including employees, shareholders, customers, and the communities in which an organization operates. Senior management should identify and evaluate the highest priority items to estimate the annual business impact (e.g., in financial terms).

3.2.2. Building an OT Cybersecurity Business Case

A well-defined business case for an OT cybersecurity program is essential for management buy-in to ensure the long-term commitment of the organization and the allocation of resources needed for the development, implementation, and maintenance of the program. The first step in developing an OT security program is to identify the organization's business objectives and missions, as well as how the cybersecurity program can lower risk and protect the organization's ability to perform those objectives and missions. The business case should capture the business concerns of senior management and provide the business impact and financial justification for creating an integrated organizational cybersecurity program. It should include detailed information about the following:

- Benefits of creating an integrated security program
- Potential costs and failure scenarios if an OT cybersecurity program is not implemented

- High-level overview of the process required to implement, operate, monitor, review, maintain, and improve the information security program

The costs and resources required to develop, implement, and maintain the security program should be considered. The economic benefits of the cybersecurity program may be evaluated in the same way that worker health and safety programs are. However, an attack on the OT system could have significant consequences that far exceed monetary costs.

3.2.3. Resources for Building a Business Case

Helpful resources can be found through information sharing exchanges, trade and standards organizations, consulting firms, and internal risk management programs or engineering and operations. External organizations can also provide useful tips as to what factors most strongly influenced management to support their efforts and what resources within their organizations proved most helpful. While these factors may vary across industries, there may be similarities in the roles that other risk management specialists can play. Appendix D lists some current activities in OT security.

Internal resources in related risk management efforts (e.g., information security, health, safety and environmental risk, physical security, business continuity) can provide tremendous assistance in prioritizing threats and estimating business impacts. These resources can also provide insight into which managers are focused on dealing with which risks and who may be the most appropriate or receptive to serving as a champion.

3.2.4. Presenting the OT Cybersecurity Business Case to Leadership

In order to be successful, the OT cybersecurity program must have active participation from senior management. Organization-level management in both IT and OT operations has the perspective to understand the risks as well as the authority to assume responsibility for them.

Senior management will be responsible for approving and driving information security policies, assigning security roles and responsibilities, and implementing the information security program across the organization. Funding for the entire program can usually be done in phases. While some funding may be required to start the program, additional funding can be obtained later as the security vulnerabilities and needs of the program are better understood and additional strategies are developed. Additionally, costs should be considered for retrofitting the OT for security versus addressing security to begin with.

Often, a good approach to obtaining management buy-in is to base the business case on a successful example of another organization that had a similar problem and how they solved it. This will often prompt management to ask how that solution might be applicable to their organization.

When presenting the business case to leadership, it may also be helpful to mention the specific challenges in securing the OT systems:

- OT systems operate under different environments and requirements than IT systems. For example, OT systems tend to prioritize availability and safety over other factors like confidentiality.

- IT programs or tools may not be suitable or effective for OT systems.
- Compensatory measures may be an effective solution to securing an OT system without affecting system performance.
- Protecting OT systems is critical, and a cybersecurity incident on an OT system may have catastrophic consequences that affect human life and the environment.

3.3. OT Cybersecurity Program Content

This section provides recommendations for establishing, implementing, maintaining, and continually improving an OT cybersecurity program. These recommendations are independent, which allows the organization to select the approaches and technologies that are most suitable to its needs.

An OT cybersecurity program is typically tailored to a specific OT environment. An organization may have multiple sites, each with multiple specific OT environments. In such situations, an organizational-level OT security program should be defined with recommendations that cascade down and adapt to the needs of individual sites and OT environments.

The effectiveness of an OT cybersecurity program is often enhanced through coordination or integration with the organization's processes and information security program. However, information security programs typically focus on the confidentiality, integrity, and availability – in that order – of information for the entire organization. Information security programs do not necessarily address all of the specific security and operational needs of an OT environment, which instead prioritizes safety, followed by availability, integrity, and confidentiality. This difference in focus and priorities between IT and OT security programs should be kept in mind. NIST SP 800-100, *Information Security Handbook: A Guide for Managers* [SP800-100], provides a broad overview of information security program elements to assist in establishing and implementing an information security program in an organization.

The lifespan of an OT system can exceed 20 years. As a result, many legacy systems may contain hardware and software that are no longer supported by vendors and cannot be patched or updated to protect against new vulnerabilities. In that case, the security program should be tailored to the unique characteristics of the legacy system to determine whether the controls are applicable. When security controls are not supported by the legacy OT system, compensating controls should be considered. For example, anti-malware software may not be available for systems such as PLCs and DCS, which means that malware protection requirements cannot be applied to these endpoints. In this case, a compensating control should be considered, such as using a firewall with a deep packet inspection capability that can monitor and block advanced threats like malware.

The primary purpose of investing in a cybersecurity program is risk management. Risk to operations exists because of the potential of threat actors exploiting the vulnerabilities in the applications and infrastructures. Therefore, the most appropriate decision regarding what to include in the scope of a cybersecurity program can be made if investments are viewed through the lens of corporate risk management. To help design and drive a cybersecurity program with a risk management perspective, NIST SP 800-37, Rev. 2 [SP800-37r2] describes the Risk Management Framework, which defines the core tasks and processes for implementing a

cybersecurity program. This is briefly summarized in Section 3.3.6 and further elaborated in Section 4.

The OT cybersecurity program should also address policy exceptions and deviations. In a demanding OT environment, situations may arise that require a temporary deviation from the security policy in order to maintain the mission or goal of the OT system. Such deviations or exceptions must be handled with great care and receive approval from management and the cross-functional team. The security program can establish a policy and procedure for handling these policy exceptions. All of these guidance documents recognize that one size does not fit all. Rather, domain knowledge combined with site-specific constraints should be applied in adapting this guidance to a specific organization.

3.3.1. Establish OT Cybersecurity Governance

OT governance should include the policies, procedures, and processes for managing the organization's regulatory, legal, risk, environmental, and operational requirements. The governance should ensure that the policies, procedures, and processes are well understood by staff and inform the management of OT cybersecurity risk. To establish an effective OT cybersecurity governance capability, develop a process and assign responsibilities and accountability to appropriate roles in the corporate risk management function. Typically, a cybersecurity governance process should include the following:

- Ensure that the OT cybersecurity policy is established and communicated.
- Ensure that OT cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
- Ensure that legal and regulatory requirements regarding OT cybersecurity, including privacy, are understood and managed.
- Ensure that cybersecurity risks are integrated into corporate risk management processes.

Further guidance for establishing OT cybersecurity guidance can be found in Section 6. Additional information with specific examples for establishing a cybersecurity governance capability are also provided in NIST Internal or Interagency Report (NIST IR) 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.2. Build and Train a Cross-Functional Team to Implement the OT Cybersecurity Program

It is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experience to evaluate and manage risk in OT. The OT cybersecurity team should consist of representatives from the following departments: IT staff, control engineer, control system operator, security subject-matter expert, and enterprise risk management. For completeness, the information security team should also include any cybersecurity service providers.

From a safety perspective, major accident hazards and the loss of containment due to equipment failure or operator mistakes can have serious consequences. Cybersecurity is another threat to the safety and reliability of industrial processes, so including safety experts as part of the

cybersecurity team will be beneficial in identifying potential impact areas due to cyber vulnerabilities. Their insight into OT design and safety considerations will also help in formulating cyber mitigations.

While the control engineers will play a large role in securing OT, they will not be able to do so without collaboration and support from both the IT department and management. IT often has years of cybersecurity experience, much of which is applicable to OT. As the cultures of control engineering and IT are often significantly different, their integration will be essential for the development of a collaborative security design and operation.

Organizations come in various sizes, structures, geographical spreads, and complexities. These factors and the strategies related to resources and budget constraints may drive organizations to hire OT cybersecurity resources as employees or contractors or outsource the OT security operation function as a managed security service. Irrespective of the security operation and resource model used, the responsibility for OT cybersecurity management should be integrated with IT cybersecurity and the corporate risk management function.

The responsibility and accountability for implementing and managing cybersecurity functions typically falls under the IT and OT infrastructure organization, whereas cybersecurity operational metrics and risks are reported to the risk management office. These two lines of reporting structure need to collaborate in terms of funding and expectations of what can be achieved given a funding and resource level. The risk executive function works with executive management to decide the risk tolerance and residual risk.

As part of building a cybersecurity team, the following tasks should be included:

- Establish and maintain cybersecurity roles and responsibilities for building, operating, and improving an OT cybersecurity program.
- Establish cybersecurity roles and responsibilities for third-party providers, which can include service providers, contractors, and other organizations that provide OT system development and services and security operation and management.

Further guidance for establishing a cross-functional team can be found in Section 4 and Appendix D. Additional information with specific examples for establishing a cross-functional team are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.3. Define the OT Cybersecurity Strategy

An organization-wide risk management strategy is foundational to developing an OT cybersecurity strategy.[4] The OT cybersecurity strategy leverages the organization-wide risk management strategy – including organization-defined risk tolerance, threats, assumptions, constraints, priorities, and trade-offs – to further tailor the strategy to apply to the OT cybersecurity program.

[4] For additional information on developing an organization-wide risk management strategy, refer to NIST SP 800-37, Rev. 2 [SP800-37r2], Prepare Step, Task P-2, Risk Management Strategy. Section 3 provides additional information on organization-level and system-level tasks to prepare for implementing the NIST Risk Management Framework.

The OT cybersecurity strategy:

- Refines and supplements guidance from the organization-wide risk management strategy to address OT-specific constraints and requirements
- Identifies the OT cybersecurity team and personnel
- Addresses the OT cybersecurity operation model (e.g., insource, outsource, and/or use managed security services)
- Outlines the appropriate cybersecurity architecture for the various OT sites within the OT program
- Defines OT-specific cybersecurity training and awareness

The OT cybersecurity strategy should help refine the organizational risk tolerance for the OT operation, which in turn drives the priorities for the OT cybersecurity operation. The program should also address both IT and OT concerns and requirements. For example, IT may consider data loss or system availability as a higher priority, but OT may value system safety, production efficiency, and environmental damage as higher priorities.

Further guidance for developing an OT cybersecurity strategy can be found in Section 5, Section 6, Appendix C, and Appendix D. Additional information and specific examples for establishing an OT cybersecurity strategy are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.4. Define OT-Specific Policies and Procedures

Policies and procedures are essential to the success of any cybersecurity program. Where possible, OT-specific security policies and procedures should be derived from existing IT cybersecurity and plant operational policies and procedures for consistency throughout the organization.

As discussed earlier, organizational management is responsible for developing and communicating the risk tolerance level of the organization (i.e., the level of risk that the organization is willing to accept), which allows the OT cybersecurity manager to determine the risk management strategy. The development of cybersecurity policies should be based on a risk assessment that will set the security priorities and goals for the organization. Procedures that support the policies need to be developed so that the policies are implemented fully and properly for OT. Cybersecurity procedures should be documented, tested, and updated periodically in response to policy, technology, and threat changes.

Further guidance for developing OT-specific policies and procedures can be found in Section 6. Additional information with examples for establishing OT-specific policies and procedures are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.5. Establish a Cybersecurity Awareness Training Program for the OT Environment

Organizations should ensure that all personnel who interact with OT systems – including employees, contractors, consultants, and vendors – receive cybersecurity training that is relevant to the OT environment in addition to general IT cybersecurity awareness training. This training is used to inform personnel of basic cybersecurity principles, teach them about their potential impacts on security and safety, and outline the steps that they need to follow when interacting with OT systems. Cybersecurity awareness training should be required for new employees at the time of hire and at regular intervals, as dictated by regulatory requirements and organizational policies.

Further guidance for OT cybersecurity awareness training can be found in Section 6 and Appendix D. Additional information with specific examples for OT cybersecurity awareness training are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.6. Implement a Risk Management Framework for OT

OT system risk is another risk confronting an organization (e.g., financial, safety, environmental, IT). In each case, managers responsible for the mission or business function establish and operate a risk management program in coordination with senior management. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [SP800-39], provides a framework for an enterprise-level risk management program, which is also detailed in Section 4 of this document. OT personnel should be involved in developing the OT cybersecurity risk management program and communicating with senior management.

NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP800-37r2], provides a structured process for managing security and privacy risk. This includes preparing for organization-wide risk management; system categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

Applying the Risk Management Framework (RMF) to OT systems is detailed in Section 4.

3.3.7. Develop a Maintenance Tracking Capability

Establish processes and implement tools to ensure that routine and preventative maintenance and repairs (both local and remote) of OT assets are performed consistent with OT organizational policies and procedures. The tools used for maintenance logging and tracking should be controlled and managed. Ensure that the processes and tools allow for scheduling, authorizing, tracking, monitoring, and auditing maintenance and repair activities for OT assets. If the ability for remote maintenance is required, ensure that the remote access tool supports the authentication of maintenance personnel, connection establishment at the beginning of maintenance activities, and immediate teardown once the maintenance activities are performed. Also ensure that the tool can log the remote maintenance activities that are performed.

Further guidance for OT maintenance tracking can be found in Section 6. Additional information with specific examples for OT maintenance tracking are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.8. Develop an Incident Response Capability

Organizations should establish an OT cybersecurity incident response (IR) function that should include planning, detection, analysis, containment, and reporting activities in the case of a cybersecurity incident. The IR function requires the establishment of several cybersecurity capabilities, including incident management, forensic analysis, vulnerability management, and response communication. As part of building the IR function, the OT cybersecurity department should create an incident response plan. The purpose of the incident response capability is to determine the scope and risk of cybersecurity incidents, respond appropriately to the incident, communicate the incident to all stakeholders, and reduce the future impact. This plan applies to all OT personnel, networks, systems, and data. The IR plan guides the activities of the cybersecurity team to respond, communicate, and coordinate in the event of a cybersecurity incident. Without such a plan, the organization will find it extremely difficult to respond when a cybersecurity incident occurs. The plan includes the roles and responsibilities of personnel, the incident response workflow, incident type and severity classification, contacts of critical personnel who should be involved, contacts of external entities that may be useful in assisting with IR, information sharing policy, and internal and external communication.

Further guidance for OT incident response can be found in Section 6.2.4.5 and Appendix C. Additional information with specific examples for OT incident response are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.9. Develop a Recovery and Restoration Capability

The organization should establish the capability to recover from cybersecurity incidents and to restore the assets and services that were impaired by the cybersecurity incident to a pre-cyber-incident state. This capability typically includes the following tasks:

- Define recovery objectives when recovering from disruptions. For example, the recovery capability shall prioritize human safety and environmental safety prior to restarting the OT operation that was impaired by the cybersecurity event.
- Develop a site disaster recovery plan (DRP) and business continuity plan (BCP) to prepare the OT organization to respond appropriately to significant disruptions in their operations due to the cybersecurity incident.
- Establish backup systems and processes to back up the relevant OT systems' state, data, configuration files, and programs at regular intervals to support recovery to a stable state.
- Establish processes for restoring relevant OT systems' state, data, configuration files, and programs from backups in a timely manner.

- Establish recovery processes and procedures that will be executed to restore the OT assets and services affected by cybersecurity incidents.
- Establish communication plans to coordinate restoration activities with internal and external stakeholders and the executive management team.
- Establish communication plans to manage public relations.
- Establish a task for lessons learned as part of the recovery process for continuous improvement of the cybersecurity capabilities (e.g., vulnerability management, cybersecurity operation, incident response handling, and recovery handling).
- Test these plans at reasonable intervals that are appropriate for the organization.

Further guidance for OT recovery and restoration can be found in Section 6. Additional information with specific examples for OT recovery and restoration are also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.3.10. Summary of OT Cybersecurity Program Content

This section presented the elements of a cybersecurity program and the various considerations for establishing such a program. Further guidance can be found in the document sections listed in **Table 2**.

Table 2. Sections with additional guidance for establishing a cybersecurity program

Cybersecurity Program Element	Section Number for Additional Guidance
Establish OT cybersecurity governance	Section 6
Build and train a cross-functional team to implement an OT cybersecurity program	Section 4, Appendix D
Define the OT cybersecurity strategy	Sections 5 and 6, Appendices 169 and 186
Define OT-specific policies and procedures	Section 6
Establish a cybersecurity awareness training program for an OT organization	Section 6, Appendix 186
Implement a Risk Management Framework for OT	Section 4 and 6, Appendices 169 and 186
Develop a maintenance tracking capability	Section 6
Develop an incident response capability	Section 6, Appendix 169
Develop a recovery and restoration capability	Section 6

4. Risk Management for OT Systems

Organizations manage risks every day when meeting their business objectives, including financial losses, equipment failure, and personnel safety. Organizations develop processes to evaluate the risks associated with their business and to decide how to manage those risks based on organizational priorities, risk tolerance, and internal and external constraints. This risk management is an interactive ongoing process that is part of normal operations. Organizations that use OT systems have historically managed risk through good practices in safety and engineering. Safety assessments are well established in most sectors and often incorporated into regulatory requirements. Information security risk management is an added dimension that can be complementary. The risk management process and framework outlined in this section can be applied to managing safety, information security, and cyber supply chain risk. Privacy is also a risk consideration for some OT systems. For additional guidance on privacy risk management, refer to the NIST Risk Management Framework [SP800-37r2] and the Privacy Framework [PF].

A risk management process is deployed throughout an organization using a three-level approach to address risk at the (i) organization level, (ii) mission and business process level, and (iii) system level (i.e., IT and OT). The risk management process is carried out seamlessly across the three levels with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders with a shared interest in the success of the organization.

This section focuses primarily on OT system considerations at the system level, though the risk management activities, information, and artifacts at each level impact and inform the other levels. Section 6 applies the Cybersecurity Framework to OT systems, while Appendix F provides OT-specific recommendations to augment the NIST SP 800-53, Rev. 5 [SP800-53r5] control families. This section also discusses OT system considerations and the impact that these considerations have on the risk management process.

For more information on multi-tiered risk management and the risk management process, refer to NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [SP800-39]. NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP800-37r2], provides guidelines for applying the Risk Management Framework to federal information systems, including conducting the activities of security categorization,[5] security control selection and implementation, security control assessment, information system authorization,[6] and security control monitoring. NIST SP 800-30, *Guide for Conducting Risk Assessments* [SP800-30r1], provides a step-by-step process for organizations on how to (i) prepare for risk assessments, (ii) conduct risk assessments, (iii) communicate risk assessment results to key organizational personnel, and (iv) maintain the risk assessments over time.

[5] Federal Information Processing Standard (FIPS) 199 [FIPS199] provides security categorization guidance for non-national security systems. Committee on National Security Systems (CNSS) Instruction 1253 provides similar guidance for national security systems.
[6] Security authorization is the official management decision given by a senior organizational official to authorize the operation of an information system and explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

4.1. Managing OT Security Risk

While the risk management process presented in NIST SP 800-39 [SP800-39] applies to all types of systems, there are some unique aspects to consider when it comes to managing OT system security risk. As shown in **Fig. 13**, the risk management process has four components: *framing risk* (i.e., establishing the context for risk-based decisions), *assessing risk*, *responding to risk*, and *monitoring risk*. These activities are interdependent and often occur simultaneously within an organization. For example, the results of the monitoring component will feed into the framing component. Because the environment in which organizations operate is always changing, risk management must be a continuous process in which all components have ongoing activities. It is important to remember that these components apply to the management of any type of risk, including cybersecurity, physical security, safety, and financial. Sections 4.1.1 through 4.1.4 discuss the four components of the risk management process in further detail and provide OT-specific implementation guidance.

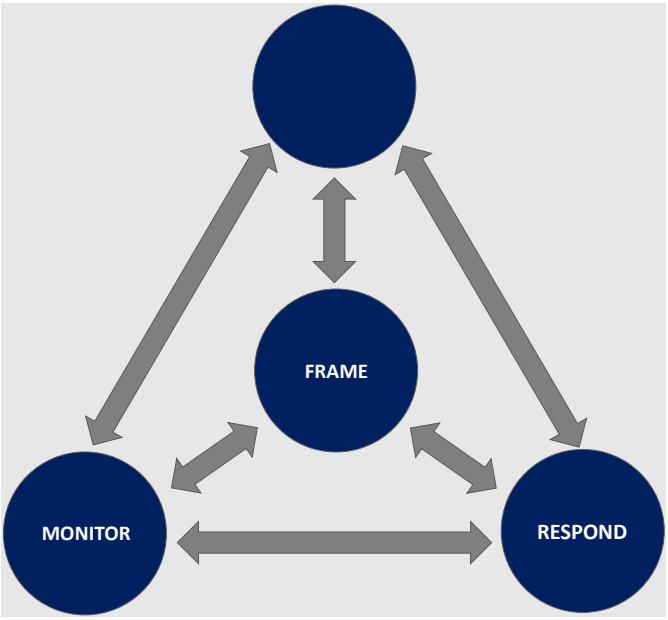

Fig. 13. Risk management process: Frame, assess, respond, and monitor

Organization-wide risk management is applied at three levels, as **Fig. 14** depicts. Level 1 addresses risk management from the organizational perspective and implements risk framing by providing context for all risk management activities within the organization. Level 2 addresses risk from a mission and business process perspective and is informed by the Level 1 risk context, decisions, and activities. Level 3 addresses risk at the system level and is informed by the Level 1 and 2 activities and outputs.

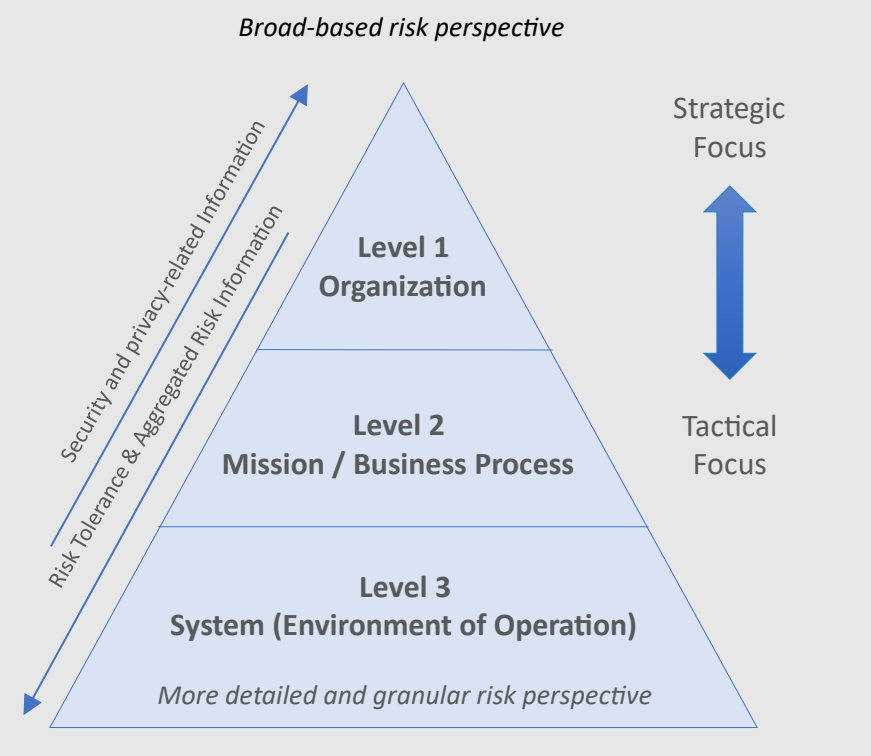

Fig. 14. Risk management levels: Organization, mission and business process, and system

Together, each of the risk management components (i.e., frame, assess, respond, and monitor) are applied across the risk management levels, resulting in organization-wide risk awareness and the traceability and transparency of risk-based decisions.

4.1.1. Framing OT Risk

The framing component consists of the processes for establishing the required assumptions, constraints, risk tolerances, and risk management strategies for organizations to make consistent risk management decisions. Specifically, risk framing supports the overall risk management strategy by incorporating elements from the organizational governance structure, legal/regulatory environment, and other factors to establish how the organization intends to assess, respond to, and monitor risk to all IT and OT systems.

OT-Specific Recommendations and Guidance

For OT system operators, safety directly affects decisions on how systems are engineered and operated. Safety can be defined as "freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."[7] Based on this, human safety impacts are typically evaluated based on the degree of injury, disease, or death that could result from the OT system malfunctioning after a cyber incident, taking into consideration any previously performed safety impact assessments

[7] See https://csrc.nist.gov/glossary/term/safety.

regarding the employees and the public. The importance of safety and developing a safety culture plays a critical role in determining risk tolerance.

Organizations should consider incorporating an analysis of cybersecurity effects on OT systems that impact personnel safety and the environment, as well as mitigating controls. More specifically, organizations may want to consider employing a comprehensive process to systematically predict or identify the operational behavior of each safety-critical failure condition, fault condition, or human error that could lead to a hazard or potential human harm.

Organizations may also want to consider the impact of legacy systems and components on their environment. Specifically, legacy systems may be unable to adequately support cybersecurity to prevent risks from exceeding organizational tolerance levels.

Another major concern for OT system operators is the availability of services provided by the OT system. The OT system may be part of critical infrastructure (e.g., water or power systems), where there is a significant need for continuous and reliable operations. As a result, OT systems may have strict requirements for availability or recovery. Organizations should understand and plan for the levels of redundancy required to achieve the desired resilience for their operating environments and incorporate these requirements into their risk framing. This will help organizations make risk decisions that avoid unintended consequences on those who depend on the services provided. More specifically, organizations should consider identifying interdependent OT systems that pose cybersecurity risks that threaten system availability.

Additionally, organizations should consider how an incident could propagate to a connected system and system components. An OT may be interconnected with other systems, such that failures in one system or process can easily cascade to other systems either within or outside of the organization. Impact propagation could occur due to both physical and logical dependencies. Properly communicating the results of risk assessments to the operators of connected or interdependent systems and processes is one way to manage such impacts.

Logical damage to an interconnected OT could occur if the cyber incident propagates to connected OT systems. For example, a virus or worm may propagate to a connected OT and impact that system. Physical damage could also propagate to other interconnected OT or related physical domains. For example, the impact could result in a physical hazard that degrades nearby physical environments or common shared dependencies (e.g., power supply) or result in a shortage of material that will be needed for a later stage in an industrial process.

CISA promotes a cohesive effort between government and industry to improve their ability to anticipate, prioritize, and manage national-level OT risk. CISA assists OT system vendors and asset owners, operators, and other vendors across all critical infrastructure sectors to identify security vulnerabilities and develop sound, proactive mitigation strategies that strengthen their OT systems' cybersecurity posture.

OT-Specific Recommendations and Guidance

Organizations may want to consider incorporating resources such as the NIST National Vulnerability Database (NVD) and the MITRE ATT&CK for Industrial Control Systems (ICS) framework [ATTACK-ICS] into their processes for assessing risks to the mission and OT systems. Additionally, the nature of OT systems requires organizations to consider additional factors that may not exist when conducting risk assessment for a traditional IT system. For example, OT will have different threat sources, vulnerabilities, and compensating controls than IT. The impact of a cyber incident in an OT environment may include both physical and digital effects that risk assessments need to incorporate, including:

- Impacts on safety and the use of safety assessments
- Physical impacts of a cyber incident on an OT, including the larger physical environment, and the effect on the process controlled
- The consequences for risk assessments of non-digital control components within an OT

During risk framing, organizations should select appropriate risk assessment methodologies that include OT. When evaluating the potential physical damage from a cyber incident, organizations with OT systems may consider i) how a cyber incident could manipulate the operation to impact the physical environment, ii) what design features exist in the OT system to prevent or mitigate an impact, and iii) how a physical incident could emerge based on these conditions.

OT-Specific Recommendations and Guidance

When framing risks within an OT environment, organizations may discover that cybersecurity threats are not always as well understood or predictable as OT hazards. Organizations may consider incorporating cyber attack and IT failure scenarios into their process hazard analysis (PHA) or failure mode and effects analysis (FMEA) processes. By including risks due to cyber attacks and cyber risk management measures in these processes, organizations may gain a better understanding of the cyber risks to the OT operational environment.

As part of risk framing, organizations may also need to consider:

- Assumptions about how risk is assessed, responded to, and monitored across the organization
- The risk tolerance for the organization, the level of risk that can be accepted as part of achieving strategic goals and objectives,

and the priorities and trade-offs considered as part of managing risk

In the context of OT, the potential for damage to equipment, human safety, the natural environment, and other critical infrastructures is part of these considerations. Organizations may need to consider evaluating the potential physical impacts for all parts of an OT system. Organizations may also need to determine how OT systems interact or depend on IT to support risk framing. These processes may require organizations to identify a common framework for evaluating impacts that incorporate OT considerations. One approach is based on NIST FIPS 199 [FIPS199], which specifies that systems are categorized as low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability. Another approach that is based on ISA 62443-3-2 [ISA62443] provides example definitions for determining a system categorization utilizing OT impacts.

Table 3 provides possible example categories and impact levels that organizations may customize to meet their specific industry or business requirements. For example, some organizations may see an outage lasting up to one day as a having a high impact instead of moderate, as shown in the table.

Table 3. Possible definitions for OT impact levels based on the product produced, the industry, and security concerns

Category	High Impact	Moderate Impact	Low Impact
Outage at multiple Sites	Significant disruption to operations at multiple sites with restoration expected to require one or more days	Operational disruptions at multiple sites with restoration expected to require more than one hour	Partially disrupted operations at multiple sites with restoration to full capability requiring less than one hour
National infrastructure and services	Impacts multiple sectors or disrupts community services in a major way	Potential to impact sector at a level beyond the company	Little to no impact to sectors beyond the individual company and little to no impact on community
Cost (% of revenue)	> 25 %	> 5 %	< 5 %
Legal	Felony criminal offense or compliance violation that affects the license to operate	Misdemeanor criminal offense or compliance violation that results in fines	None
Public confidence	Loss of brand image	Loss of customer confidence	None
People on-site	Fatality	Loss of workday or major injury	First aid or recordable injury
People off-site	Fatality or major community incident	Complaints or local community impact	No complaints
Environment	Citation by regional agency or long-term significant damage over large area	Citation by local agency	Small, contained release below reportable limits

To support the risk assessment process, organizations should also define how the likelihood of occurrence for cybersecurity events will be determined to maintain consistency when assessing risks. NIST SP 800-30, Rev. 1 [SP800-30r1] provides guidance for organizations to develop likelihood weighted risk factors. Organizations should consider weighting risk factors based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities), that the threat event will be initiated, and that the threat event will result in adverse impacts.

For adversarial threats, an assessment of likelihood of occurrence is typically based on adversary intent, capability, and targeting. For other-than-adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, and other factors. If organizations find that there is minimal organizational historical data, they may want to consider extending their analysis to consider industry-specific data describes cybersecurity events reported for similar organizations.

The likelihood of threat occurrence can also be based on the state of the organization (e.g., its core mission and business processes, enterprise architecture, information security architecture, information systems, and the environments in which those systems operate) and consider predisposing conditions and the presence and effectiveness of deployed security controls to protect against unauthorized or undesirable behavior, detect and limit damage, and/or other resiliency factors for the OT capabilities.

OT-Specific Recommendations and Guidance

Organizations that establish definitions for event likelihood may want to review Appendix G of NIST SP 800-30, Rev. 1 for more detailed guidance and suggestions. Based on this guidance, organizations should consider defining five levels of likelihood from Very Low to Very High based on both adversarial (i.e., intentional threat actors) and non-adversarial (e.g., errors, accidents, acts of nature, etc.) events. Additionally, organizations may want to establish definitions for the likelihood that an event may result in an adverse impact. Using these two factors, organizations can establish a heat map like the one depicted in **Table 4** to determine the likelihood factor for supporting the risk analysis.

Table 4. Event Likelihood Evaluation

Likelihood of Threat Event Initiation or Occurrence	Likelihood That Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

4.1.2. Assessing Risk in an OT Environment

Risk assessments leverage the outputs of framing risk (e.g., acceptable risk assessment methodologies, risk management strategy, and risk tolerance) and facilitate efforts to identify, estimate, and prioritize risks to operations, assets, individuals, and other organizations. Risk assessments occur at all risk management levels (i.e., organization, mission and business function, and system) and can be used to inform risk assessments at other levels. Regardless of which risk management level the risk assessment is conducted at, assessing risk requires identifying threats and vulnerabilities, the harm that such threats and vulnerabilities may cause, and the likelihood that adverse events may arise from those threats and vulnerabilities.

When the organization conducts a risk assessment that includes OT systems, there may be additional considerations that do not exist when assessing the risks of traditional IT systems. For example, the impact of a cyber incident on an OT may include both physical and digital effects.

OT-Specific Recommendations and Guidance

Risk assessments are typically point-in-time reports. As a result, organizations should ensure that they are updated to remain current and that the security level remains adequate.

Organizations may want to review the information provided by CISA's Alerts and Advisories, NIST's NVD, and MITRE ATT&CK for ICS to identify common vulnerability areas for OT environments, such as:

- Poor coding practices, network designs, or device configurations
- Vulnerable network services and protocols
- Weak authentication
- Excessive privileges
- Information disclosure

OT systems often have specific environmental requirements (e.g., a manufacturing process may require a precise temperature), or they may be tied to their physical environment for operations. Organizations may want to consider incorporating these requirements and constraints into the framing component so that associated risks are identified. Additionally, organizations may want to consider:

- Identifying the physical assets and security controls that directly relate to safety, human life, and maintaining continuity of operations of the OT system
- Identifying the cybersecurity risks associated with physical assets that could threaten OT system functionality
- Ensuring that physical security personnel understand the relative risks and physical security countermeasures associated with the OT system environments that they protect

- Ensuring that physical security personnel are aware of areas in an OT system production environment that house data acquisition and operate in sensitive spaces
- Mitigating business continuity risks by specifying immediate response plans if physical safety is jeopardized

Risk assessments also require reviewing the digital and non-digital mechanisms that are implemented to minimize adverse event impacts. OT systems often incorporate non-digital mechanisms to provide fault tolerance and prevent the OT from acting outside of acceptable parameters. These non-digital mechanisms may help reduce the negative impacts that a digital incident on the OT might have and should be incorporated into the risk assessment process. For example, OT often have non-digital control mechanisms that can prevent it from operating outside of a safe boundary and thereby limit the impact of an attack (e.g., a mechanical relief pressure valve). Analog mechanisms (e.g., meters, alarms) can also be used to observe the physical system state and provide operators with reliable data if digital readings are unavailable or corrupted. **Table 5** categorizes non-digital control mechanisms that could reduce the impact of an OT incident.

Table 5. Categories of non-digital OT control components

Control Type	Description
Analog displays or alarms	Non-digital mechanisms measure and display the state of the physical system (e.g., temperature, pressure, voltage, current) and can provide the operator with accurate information when digital displays are unavailable or corrupted. The information may be provided to the operator on some non-digital display (e.g., thermometers, pressure gauges) and through audible alarms.
Manual control mechanisms	Manual control mechanisms (e.g., manual valve controls, physical breaker switches) allow operators to manually control an actuator without relying on the digital OT system. This ensures that an actuator can be controlled even if the OT system is unavailable or compromised.
Analog control systems	Analog control systems use non-digital sensors and actuators to monitor and control a physical process. These may prevent the physical process from entering an undesired state when the digital OT system is unavailable or corrupted. Analog controls include devices such as regulators, governors, and electromechanical relays. An example is a device that is designed to open during emergency or abnormal conditions to prevent the rise of internal fluid pressure in excess of a specified value, thus bringing the process to a safer state. The device may also be designed to prevent an excessive internal vacuum, such as a pressure relief valve, a non-reclosing pressure relief device (e.g., rupture disc), or a vacuum relief valve.

OT-Specific Recommendations and Guidance

Organizations should analyze all digital and non-digital control mechanisms and the extent to which they can mitigate potential negative impacts to the OT. For example, non-digital control mechanisms may require additional time and human involvement, such as operators travelling to a remote site to perform certain control functions. Such mechanisms may also depend on human response times, which may be slower than automated controls.

Additionally, organizations may need to consider privacy with their risk assessment, which sometimes require a different approach. The NIST Privacy Risk Assessment Methodology (PRAM) is a tool that applies the risk model from NIST IR 8062 [IR8062] and helps organizations analyze, assess, and prioritize privacy risks to determine how to respond and select appropriate solutions.

4.1.3. Responding to Risk in an OT Environment

The risk response component provides an organization-wide response to risk in accordance with the risk framing component by identifying possible courses of actions to address risk, evaluating those possibilities while considering the organization's risk tolerance and other issues identified during framing, and choosing the best alternative for the organization. The response component includes the implementation of the chosen course of action to address the identified risk: *acceptance*, *avoidance*, *mitigation*, *sharing*, *transfer*, or any combination of these options.[8]

OT-Specific Recommendations and Guidance

For an OT system, available risk responses may be constrained by system requirements, potential adverse impacts on operations, or even regulatory compliance regimes. An example of risk sharing is when utilities enter into agreements to "loan" line workers in an emergency, which reduces the duration of an incident's effect to acceptable levels.

4.1.4. Monitoring Risk in an OT Environment

Monitoring risk is the fourth component of risk management activities. Organizations monitor risk on an ongoing basis, including the implementation of chosen risk management strategies, changes in the environment that may affect the risk calculation, and the effectiveness and efficiency of risk reduction activities. The activities in the monitoring component impact all of the other components.

OT-Specific Recommendations and Guidance

Many OT system monitoring capabilities leverage passive monitoring techniques to detect system changes. However, this may not always capture all modifications to the system. Modern monitoring platforms that leverage native protocol communications to access more system information may improve awareness, but the limitations of these OT systems must be understood. Often OT systems are implemented with an undefined frequency for monitoring cyber activities. Users should set a frequency in accordance with the respective risk profile.

Threat information as it relates to the OT environment is evolving, and the availability and accuracy of this threat information is early in its development. By their nature, threats may be difficult to accurately predict, even with historical data. Organizations should categorize threats based on the likelihood of occurrence and their potential consequences.

[8] For additional information on these options, refer to NIST SP 800-39 [SP800-39].

For example, the threat of an internet-connected system being scanned would have a high likelihood and a low severity consequence, but the threat of a nation-state actor disrupting a supply chain may have low likelihood and high severity consequences.

Since security countermeasures are typically developed for IT environments, organizations should consider how deploying security technologies into OT environments may negatively impact operations or safety.

4.2. Special Areas for Consideration

Supply chain risk management and risk management for safety are critical aspects of OT cybersecurity risk management.

4.2.1. Supply Chain Risk Management

Cybersecurity risks can arise from the products or services acquired to support OT needs. These risks can be introduced anywhere in the supply chain and at any stage in the life cycle. Whether they are malicious, natural, or unintentional, these risks have the potential to compromise the availability and integrity of critical OT systems and components, as well as the availability, integrity, and confidentiality of the data utilized by the OT, thereby causing harms that range from minor disruptions to impacts on life and safety.

With few exceptions, organizations that are responsible for OT rely upon suppliers, other third-party providers, and their extended supply chains for a range of needs. These supply-side organizations perform critical roles and functions, including manufacturing and provisioning technology products, providing software upgrades and patches, performing integration services, or otherwise supporting the day-to-day operations and maintenance of OT systems, components, and operational environments. For this reason, OT organizations should seek to understand and mitigate the supply chain-related risks that can be inherited from these supply-side organizations and the products and services that they provide.

Identifying, assessing, and effectively responding to cybersecurity risks in supply chains is best accomplished by incorporating cybersecurity supply chain risk management (C-SCRM) considerations into organizational policies, plans, and practices. This includes extending cybersecurity expectations and requirements to vendors and gaining better understanding, visibility, and control over the supply chains that are associated with acquired products and services. Organizations should vet suppliers and service providers to ascertain their capabilities, trustworthiness, the adequacy of their internal security practices, the effectiveness of safeguards, their supply chain relationships, and any risks that may be associated with those relationships and dependencies. The requirements for and evaluation of products and discrete components should extend beyond an assessment of whether functional and technical requirements are satisfied and address applicable C-SCRM factors, such as a product's provenance, pedigree, and composition and whether the product is taint-free and authentic. Additionally, special consideration should be given to how difficult it may be to attain original replacement parts or updates over the life of the product and how diverse the sources of supply are and may be in the future.

OT organizations should familiarize themselves with NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [SP800-161], and begin or continue to implement the key practices, C-SCRM security controls, and C-SCRM risk management process activities described in that publication. There is extensive guidance about how to establish a C-SCRM program using a phased approach that begins with putting the foundational elements in place and expanding upon that foundation over time to ensure sustained effectiveness and the ability to enhance program capabilities. There is also guidance about conducting supply chain risk assessments, incorporating C-SCRM into procurement requirements, the importance of an integrated and inter-disciplinary risk management approach, supplemental C-SCRM security control guidance, and templates that organizations can leverage.

4.2.2. Safety Systems

The culture of safety and safety assessments is well established within much of the OT user community. Information security risk assessments should complement such assessments, though they may use different approaches and cover different areas. Safety assessments are primarily concerned with the physical world, while information security risk assessments consider the digital world. However, in an OT environment, the physical and the digital are intertwined, and significant overlap may occur.

Organizations should, therefore, consider all aspects of risk management for safety (e.g., risk framing, risk tolerances) and the safety assessment results when carrying out risk assessments for information security. The personnel responsible for the information security risk assessment must be able to identify and communicate identified risks that could have safety implications. Conversely, the personnel charged with safety assessments must be familiar with the potential physical impacts and their likelihood.

Safety systems may reduce the impact of a cyber incident on the OT and are often deployed to perform specific monitoring and control functions to ensure the safety of people, the environment, processes, and assets. While these systems are traditionally implemented to be fully redundant and independent from the primary OT, some architectures combine control and safety functions, components, or networks. Combining control and safety could allow a sophisticated attacker access to both control and safety systems if the OT were compromised. Organizations should ensure the adequate separation of components consistent with the risk of compromise and evaluate the impact of the implemented security controls on the safety system to determine whether they negatively impact the system.

4.3. Applying the Risk Management Framework to OT Systems

The NIST Risk Management Framework (RMF) applies the risk management process and concepts (i.e., framing risk, assessing risk, responding to risk, and monitoring risk) to systems and organizations. The following subsections describe the process of applying the RMF to OT and include a brief description of each step and task, the intended outcome of each task, task mappings to other standards and guidelines applicable to OT (e.g., the Cybersecurity Framework and IEC 62443), and OT-specific implementation guidance. Some tasks are optional, and not all tasks include OT-specific considerations or guidance.

The RMF steps in **Fig. 15**, while shown sequentially, can be implemented in a different order to be consistent with established management and system development life cycle processes.

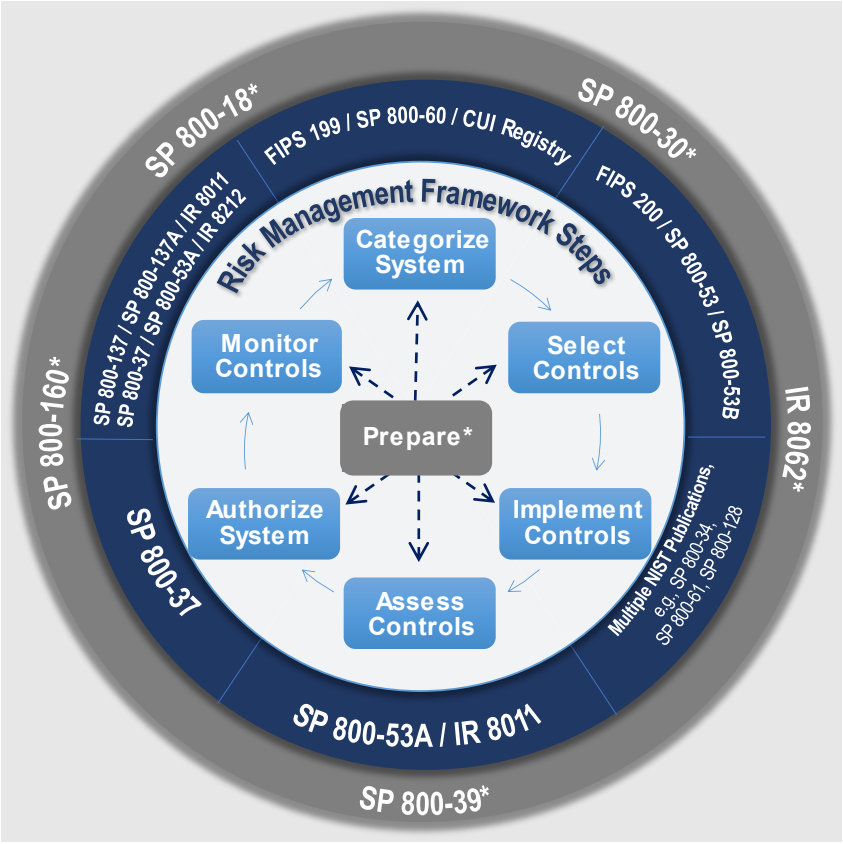

Fig. 15. Risk Management Framework steps

4.3.1. Prepare

The purpose of the Prepare step is to carry out essential activities at the organizational, mission and business process, and system levels to help the organization manage its security and privacy risks using the RMF. The Prepare step leverages activities that are already being conducted within cybersecurity programs to emphasize the importance of having organization-wide governance and resources in place to support risk management. **Table 6** provides details on applying the Prepare step to OT.

Table 6. Applying the RMF Prepare step to OT

Tasks	Outcomes	OT-Specific Guidance
Organizational and Mission and Business Process Levels		
TASK P-1 RISK MANAGEMENT ROLES	Individuals are identified and assigned key roles for executing the RMF. [*Cybersecurity Framework*: **ID.AM-6**; **ID.GV-2**] [IEC 62443-2-1: **ORG 1.3**]	Establish and maintain personnel cybersecurity roles and responsibilities for both IT and OT systems. Include cybersecurity roles and responsibilities for third-party providers. Examples of OT

Tasks	Outcomes	OT-Specific Guidance
		personnel include the Process/Plant Manager, Process Control Engineer, Operator, Functional Safety Engineer, Maintenance Personnel, and Process Safety Manager.
TASK P-2 RISK MANAGEMENT STRATEGY	A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **ID.RM; ID.SC**] [IEC 62443-2-1: **ORG 2.1**]	The risk management strategy encompasses the whole organization. Consider the unique regulatory requirements as it relates to organizations with OT systems.
TASK P-3 RISK ASSESSMENT—ORGANIZATION	An organization-wide risk assessment is completed, or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**] [IEC 62443-2-1: **Event1.9; ORG 1.3; 2.1**]	
TASK P-4 ORGANIZATIONALLY TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	Organizationally tailored control baselines and/or Cybersecurity Framework profiles are established and made available. [*Cybersecurity Framework*: **Profile**]	An organizationally tailored control baseline for OT systems can be developed to address mission and business needs, unique operating environments, and/or other requirements.
TASK P-5 COMMON CONTROL IDENTIFICATION	Common controls that are available for inheritance by organizational systems are identified, documented, and published.	Common controls available for inheritance may adversely impact OT system operation. Consider whether common controls can be applied to OT systems effectively, safely, and without adverse impacts on OT system operation.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-5**] [IEC 62443-2-1: **DATA 1.1**]	Criteria such as safety or critical service delivery can be used in the impact-level prioritization.
TASK P-7 CONTINUOUS MONITORING STRATEGY – ORGANIZATION	An organization-wide strategy for monitoring control effectiveness is developed and implemented. [*Cybersecurity Framework*: **DE.CM; ID.SC-4**] [IEC 62443-2-1: **EVENT 1.1; COMP 2.2 USER 1.06; EVENT 1.1.; ORG2.2**	
System-Level		
TASK P-8 MISSION OR BUSINESS FOCUS	Missions, business functions, and mission and business processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **ID.BE**] [IEC 62443-2-1: **ORG1.6; AVAIL 1.2; AVAIL 1.1**]	When mapping OT and IT processes, the information flows and protocols should also be documented.
TASK P-9 SYSTEM STAKEHOLDERS	The stakeholders with an interest in the system are identified.	Example OT personnel include the Process/Plant Manager,

Tasks	Outcomes	OT-Specific Guidance
	[*Cybersecurity Framework*: **ID.AM**; **ID.BE**]	Process Control Engineer, Operator, Functional Safety Engineer, and Process Safety Manager.
TASK P-10 ASSET IDENTIFICATION	Stakeholder assets are identified and prioritized. [*Cybersecurity Framework*: **ID.AM**]	OT system components can include PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.
TASK P-11 AUTHORIZATION BOUNDARY	The authorization boundary (i.e., system) is determined.	
TASK P-12 INFORMATION TYPES	The types of information processed, stored, and transmitted by the system are identified. [*Cybersecurity Framework*: **ID.AM-5**]	
TASK P-13 INFORMATION LIFE CYCLE	All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system. [*Cybersecurity Framework*: **ID.AM-3**; **ID.AM-4**]	
TASK P-14 RISK ASSESSMENT – SYSTEM	A system-level risk assessment is completed, or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; ID.SC-2**]	Risk assessments, including performance/load testing and penetration testing, are conducted on the OT systems with care to ensure that OT operations are not adversely impacted by the testing process.
TASK P-15 REQUIREMENTS DEFINITION	Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **ID.GV; PR.IP**]	
TASK P-16 ENTERPRISE ARCHITECTURE	The placement of the system within the enterprise architecture is determined.	Group OT components by function or sensitivity level to optimize cybersecurity control implementation.
TASK P-17 REQUIREMENTS ALLOCATION	Security and privacy requirements are allocated to the system and the environment in which the system operates. [*Cybersecurity Framework*: **ID.GV**]	As security and privacy requirements are allocated to the OT system, considerations such as impact on performance and safety are considered.
TASK P-18 SYSTEM REGISTRATION	The system is registered for purposes of management, accountability, coordination, and oversight. [*Cybersecurity Framework*: **ID.GV**]	

4.3.2. Categorize

In the Categorize step, the potential adverse impacts of the loss of confidentiality, integrity, and availability of the information and system are determined. For each information type and system under consideration, the three security objectives – confidentiality, integrity, and availability – are associated with one of three levels of potential impacts of a security breach. Of the three security objectives, availability is generally the greatest concern for an OT. The standards and guidance for this categorization process can be found in FIPS 199 [FIPS199] and NIST SP 800-60 [SP800-60v1r1][SP800-60v2r1], respectively.

The following OT example is taken from FIPS 199:

OT-Specific Recommendations and Guidance

A power plant contains a SCADA system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)}, and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)}

representing the high-water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate, reflecting a more realistic view of the potential impact on the system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}

Table 7 provides details on applying the RMF Categorize step to OT.

Table 7. Applying the RMF Categorize step to OT

Tasks	Outcomes	OT-Specific Guidance
TASK C-1 SYSTEM DESCRIPTION	The characteristics of the system are described and documented. [*Cybersecurity Framework*: **Profile**]	
TASK C-2 SECURITY CATEGORIZATION	A security categorization of the system, including the information processed by the system represented by the organization-identified information types, is completed. [*Cybersecurity Framework*: **ID.AM-1**; **ID.AM-2**; **ID.AM-3**; **ID.AM-4**; **ID.AM-5**] Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission and business processes. [*Cybersecurity Framework*: **Profile**] Security categorization results reflect the organization's risk management strategy.	OT and IT systems may have different categorization criteria. System information and the system process (e.g., chemical production) should be considered during the security categorization.
TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	The security categorization results are reviewed, and the categorization decision is approved by senior leaders in the organization.	

4.3.3. Select

The purpose of the Select step is to select the initial controls to protect the system commensurate with risk. The control baselines are the starting point for the control selection process and are chosen based on the security category and associated impact level of the systems identified in the Categorize step. NIST SP 800-53B [SP800-53B] identifies the recommended control baselines for federal systems and information. To address the need for developing community-wide and specialized sets of controls for systems and organizations, the concept of overlays is introduced. An *overlay* is a fully specified set of controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance to security control baselines described in NIST SP 800-53B, Appendix C.

In general, overlays are intended to reduce the need for ad hoc tailoring of baselines by organizations through the selection of a set of controls and control enhancements that more closely correspond to common circumstances, situations, and/or conditions. Appendix F of this publication includes an OT-specific overlay of applicable NIST SP 800-53 controls that provides tailored baselines for low-impact, moderate-impact, and high-impact OT. These tailored baselines are starting specifications and recommendations that can be applied to specific OT by responsible personnel.

OT owners can tailor the overlay from Appendix F when it is not possible or feasible to implement specific controls. The use of overlays does not in any way preclude organizations from performing further tailoring (i.e., overlays can also be subject to tailoring) to reflect organization-specific needs, assumptions, or constraints. However, all tailoring activities should primarily focus on meeting the intent of the original controls whenever possible or feasible. For example, when the OT cannot support or the organization determines that it is not advisable to implement particular controls or control enhancements in an OT (e.g., performance, safety, or reliability are adversely impacted), the organization should provide a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the OT and why the related baseline controls could not be employed. If the OT cannot support the use of automated mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance in Section 3.3 of NIST SP 800-53. Compensating controls are not exceptions or waivers to the baseline controls. Rather, they are alternative safeguards and countermeasures employed within the OT that accomplish the intent of the original controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan for the OT.

Table 8 provides additional details on applying the RMF Select step to OT.

Table 8. Applying the RMF Select step to OT

Tasks	Outcomes	OT-Specific Guidance
TASK S-1 CONTROL SELECTION	Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**]	OT systems can leverage the OT control baselines identified in Appendix F as a starting point or an organization-defined control selection approach.
TASK S-2 CONTROL TAILORING	Controls are tailored to produce specific control baselines. [*Cybersecurity Framework*: **Profile**]	Due to operational or technical constraints, it may not be feasible to implement certain controls. Organizations should consider the use of compensating controls to manage risk to an acceptable level.
TASK S-3 CONTROL ALLOCATION	Controls are assigned as system-specific, hybrid, or common controls. Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [*Cybersecurity Framework*: **Profile**; **PR.IP**]	
TASK S-4 DOCUMENTATION OF PLANNED CONTROL IMPLEMENTATIONS	Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents. [*Cybersecurity Framework*: **Profile**]	
TASK S-5 CONTINUOUS MONITORING STRATEGY – SYSTEM	A continuous monitoring strategy for the system that reflects the organizational risk management strategy is developed. [*Cybersecurity Framework*: **ID.GV**; **DE.CM**]	An OT-specific continuous monitoring strategy to measure control effectiveness may be necessary due to unique operational, environmental, and/or availability constraints.

Tasks	Outcomes	OT-Specific Guidance
TASK S-6 PLAN REVIEW AND APPROVAL	Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorizing official.	Review any potential impact to the OT system's operational effectiveness and safety.

4.3.4. Implement

The Implement step involves the implementation of controls in new or legacy systems. The control selection process described in this section can be applied to OT from two perspectives: new development and legacy.

For new development systems, the control selection process is applied from a requirements definition perspective since the systems do not yet exist and organizations are conducting initial security categorizations. The controls included in the security plans for the systems serve as security specifications and are expected to be incorporated into the systems during the development and implementation phases of the system development life cycle.

In contrast, the security control selection process for legacy systems is applied from a gap analysis perspective when organizations anticipate significant changes to the systems (e.g., during major upgrades, modifications, or outsourcing). Since the systems already exist, organizations have likely completed the security categorization and security control selection processes, resulting in the establishment of previously agreed-upon controls in the respective security plans and the implementation of those controls within the systems.

Table 9 provides additional details on applying the RMF Implement step to OT.

Table 9. Applying the RMF Implement step to OT

Tasks	Outcomes	OT-Specific Guidance
TASK I-1 CONTROL IMPLEMENTATION	Controls specified in the security and privacy plans are implemented. [*Cybersecurity Framework*: **PR.IP-1**] Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework: **PR.IP-2***]	For existing (operational) OT systems, schedule control implementation during the OT system maintenance window. A complete verification is recommended to ensure that the controls are not affecting or degrading the performance and safety of the OT system. In some cases, it may not be feasible to immediately mitigate the risk due to scheduling issues. However, interim compensating controls can be leveraged.
TASK I-2 UPDATE CONTROL IMPLEMENTATION INFORMATION	Changes to the planned implementation of controls are documented. [*Cybersecurity Framework: **PR.IP-1***] The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework*: **Profile**]	

4.3.5. Assess

The Assess step of the RMF determines the extent to which the controls in the system are effective in their application and producing the desired results. NIST SP 800-53A [SP800-53Ar5] provides guidance for assessing selected controls from NIST SP 800-53 to ensure that they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

Table 10 provides additional details on applying the Assess step to OT.

Table 10. Applying the RMF Assess step to OT

Tasks	Outcomes	OT-Specific Guidance
TASK A-1 ASSESSOR SELECTION	An assessor or assessment team is selected to conduct the control assessments. The appropriate level of independence is achieved for the assessor or assessment team selected.	Include OT system personnel and operator in the assessment team.
TASK A-2 ASSESSMENT PLAN	Documentation needed to conduct the assessments is provided to the assessor or assessment team. Security and privacy assessment plans are developed and documented. Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.	
TASK A-3 CONTROL ASSESSMENTS	Control assessments are conducted in accordance with the security and privacy assessment plans. Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered. Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.	Consider the use of tabletop exercises or simulations to reduce the impact to production OT. Use automated tools to conduct assessments with care to ensure that the OT system is not adversely impacted by the testing process.
TASK A-4 ASSESSMENT REPORTS	Security and privacy assessment reports that provide findings and recommendations are completed. [*Cybersecurity Framework*: **ID.RA-1 and ID.RA-3**]	
TASK A-5 REMEDIATION ACTIONS	Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. Security and privacy plans are updated to reflect the control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]	Ensure that remediation actions do not negatively impact the efficiency and safe operations of OT. Consider the use of compensating controls as one of the remediation actions.
TASK A-6 PLAN OF ACTION AND MILESTONES	A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-6**]	Consider the unique time constraints of the OT system in the plan of action and milestones, and take into account planned schedule maintenance or shutdowns of the OT system.

4.3.6. Authorize

The Authorize step involves a management decision to authorize the operation of a system and explicitly accept the risks to operations, assets, and individuals based on the implementation of an agreed-upon set of controls. A new system is not placed into production or operation until the system is authorized.

Table 11 provides additional details on applying the Authorize step to OT.

Table 11. Applying the RMF Authorize step to OT

Tasks	Outcomes	OT-Specific Guidance
TASK R-1 AUTHORIZATION PACKAGE	An authorization package is developed for submission to the authorizing official.	
TASK R-2 RISK ANALYSIS AND DETERMINATION	A risk determination by the authorizing official that reflects the risk management strategy, including risk tolerance, is rendered.	
TASK R-3 RISK RESPONSE	Risk responses for determined risks are provided. [*Cybersecurity Framework*: **ID.RA-6**]	Develop and implement a comprehensive strategy to manage risk to the OT system that includes the identification and prioritization of risk responses.
TASK R-4 AUTHORIZATION DECISION	The authorization for the system or the common controls is approved or denied.	Organizations may need to determine remediation strategies when system risks drift out of the acceptable range while considering OT-specific dependencies, such as the inability to take a system or component offline until remediated.
TASK R-5 AUTHORIZATION REPORTING	Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.	Ensure that decisions, vulnerabilities, and risks are reported to OT and operations personnel.

4.3.7. Monitor

The Monitor step continuously tracks changes to the system that may affect controls and assesses control effectiveness. NIST SP 800-37, Rev. 2 provides guidance on cybersecurity continuous monitoring [SP800-37r2].

Table 12 provides additional details on applying the Monitor step to OT.

Table 12. Applying the RMF Monitor step to OT

Tasks	Outcomes	OT-Specific Guidance
TASK M-1 SYSTEM AND ENVIRONMENT CHANGES	The system and environment of operation are monitored in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **DE.CM**; **ID.GV**]	Leverage the OT-specific continuous monitoring strategy that considers performance impacts and safety systems to be critical.
TASK M-2 ONGOING ASSESSMENTS	Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **ID.SC-4**]	Conduct ongoing assessments that consider system performance and safety impacts.
TASK M-3 ONGOING RISK RESPONSE	The output of continuous monitoring activities is analyzed and responded to appropriately. [Cybersecurity Framework: RS.AN]	Correlate detected event information with risk assessment outcomes to achieve perspective on incident impact on the OT system.
TASK M-4 AUTHORIZATION PACKAGE UPDATES	Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **RS.IM**]	
TASK M-5 SECURITY AND PRIVACY REPORTING	A process is in place to report the security and privacy posture to the authorizing official and other senior leaders and executives.	
TASK M-6 ONGOING AUTHORIZATION	Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.	
TASK M-7 SYSTEM DISPOSAL	A system disposal strategy is developed and implemented, as needed.	Planned obsolescence found in IT components may not extend to OT components. Consider the maintenance and repair of OT components that are required to be sustained beyond IT component availability.

5. OT Cybersecurity Architecture

When designing a security architecture for an OT environment, it is generally recommended to separate the OT network(s) from the corporate network. The nature of network traffic on these two network types is different. For example, internet access, email, and remote access are typically permitted on the corporate network but not allowed on OT networks. There may also be differences in the degree of rigor associated with corporate and OT environment change control procedures. Additionally, using the corporate network for OT communication protocols could expose the OT components to cyber attacks (e.g., DoS, adversary-in-the-middle or other network-based attacks). Utilizing separate networks allows for greater flexibility to address security and performance requirements between the two environments.

Practical considerations – such as digital transformation, the cost of OT installation, or maintaining a homogenous network infrastructure – often mean that a connection is required between OT and corporate or other IT networks. This connection represents additional risk, and organizations may want to minimize these connections and consider additional security controls for them. This section outlines security strategies for organizations to consider when engineering their OT environments to support cybersecurity objectives.

5.1. Cybersecurity Strategy

The adoption of a cybersecurity strategy can result in a more systematic implementation of risk decisions into system development and operation. A comprehensive and accepted cybersecurity strategy can assist an organization with consistently maintaining acceptable risk management throughout the life cycle of an OT system.

System security is optimized by engineering design that is based on a proactive loss prevention strategy. Such a strategy includes planned measures that are engineered to address what *can* happen rather than what is *likely* to happen in order to proactively identify and rid the system of weaknesses and defects that lead to security vulnerabilities, understand the certainty and uncertainty of adversarial and non-adversarial threats, and put in place the means and methods to protect against adverse consequences. Proactive systems security engineering also includes planning for failure regardless of whether the failure results from adversarial or non-adversarial events and ensuring that the system is resilient to such events.

OT-Specific Recommendations and Guidance

When planning a security strategy, organizations may need to consider critical infrastructure standards and regulatory requirements. Based on guidance from CISA, organizations may find that both IT and OT environments fall within the critical infrastructure sectors. These standards and requirements are typically designed to protect critical cyber assets to support reliability and may carry additional legal obligations for the organization.

5.1.1. Impacts of Choosing a Cybersecurity Strategy

By consciously choosing to develop and implement a cybersecurity strategy, an organization establishes a disciplined approach that considers all aspects of the system life cycle – from procurement to decommissioning – with cybersecurity in mind. As a result, the organization can ensure that cybersecurity goals are realized in its systems.

Decisions on cybersecurity strategy should flow from a high-level understanding of the operations, objectives, and cybersecurity goals of the organization. For example, the organization may want its systems to display certain characteristics, such as resiliency or trustworthiness. The strategy provides a framework for incorporating those characteristics into the final systems. The strategy can also include additional considerations, such as the flexibility to adopt new technologies (e.g., crypto agility, artificial intelligence [AI] and machine learning [ML] technologies, digital twins). Finally, the strategy can state the need for sound cybersecurity practices, such as patching or monitoring.

The cybersecurity strategy should directly impact the architectural decisions made for systems. The existence of an architecture informed by a cybersecurity strategy increases the likelihood that high-level cybersecurity goals will be reflected in the cybersecurity of individual systems. The strategy provides a document and reminder of those goals when decisions are being made at the system level.

OT-Specific Recommendations and Guidance

OT assets often have long life cycles and reflect massive investments in operational, reliability, and safety testing. It is sometimes neither economically nor technically feasible to replace existing equipment and applications wholesale with newer alternatives in the short- or medium-term. Such equipment is at greater risk of attacks than equipment with the latest versions of security features and security updates. The adoption of a cybersecurity strategy can assist an organization in understanding the life cycle of its OT systems and adjusting its approaches to maintaining security.

5.1.2. Defense-in-Depth Strategy

Defense in depth is a multifaceted strategy that integrates people, technology, and operational capabilities to establish variable barriers across multiple layers and dimensions of the organization. Many cybersecurity architectures incorporate the principles of defense in depth. It is considered best practice and integrates into numerous standards and regulatory frameworks.

The basic concepts are to prevent single points of failure in cybersecurity defenses and to assume no single origin of threats. From this position, cybersecurity controls are organized to provide layers of protection around the critical system and system components.

OT-Specific Recommendations and Guidance

A defense-in-depth strategy is particularly useful in OT environments because it can focus attention and defensive mechanisms on critical functions. Additionally, the principles of defense in depth are flexible

and can be applied to a wide range of OT environments, including ICS, SCADA, Internet of Things (IoT), IIoT, and hybrid environments.

Defense in depth requires an integration of people, processes, and technology to be effective. Additionally, cybersecurity defenses are not static and require changes and updates as risks change for the environment. To help establish and support an effective defense-in-depth architecture, organizations should consider:

- Training people to support the security environment and reduce risky behaviors
- Implementing appropriate and sustainable cybersecurity technology
- Implementing procedures to monitor, respond, and adapt cybersecurity defenses to changing conditions

5.1.3. Other Cybersecurity Strategy Considerations

Traditional OT systems were designed to operate industrial processes safely and reliably without connections to external networks. However, due to the need for business agility and cost reduction for OT infrastructures, OT systems and networks are becoming more integrated into business networks and cloud infrastructures. Additionally, the introduction of IIoT systems into OT environments may have unintended cybersecurity consequences.

Similarly, cloud computing capabilities (e.g., infrastructure as a service, platform as a service, software as a service, and security as a service) are increasingly being utilized by organizations. While the use of these capabilities to support IT services is relatively well understood, the ability to utilize these services to support OT environments may have additional availability challenges resulting from increased sensitivity to system performance levels or connection issues. As a result, the adoption of a security architecture strategy may be impacted by the current state of existing OT environments. For example, based on the architectural strategy, procurement decisions might be adjusted to include migrating specific components to support the new strategy. Organizations may also find that existing systems already support some or most of the security architecture strategy, so building on these existing capabilities could accelerate the strategy implementation. Additionally, new OT environments provide an opportunity to evaluate cyber risk early on and build cybersecurity into the design.

OT-Specific Recommendations and Guidance

Organizations should ensure that their security architecture strategy provides the required flexibility to evolve their environment while also carefully considering the impacts to operations and cybersecurity.

5.2. Defense-in-Depth Architecture Capabilities

Many organizations are embracing digital transformation initiatives that require altering their OT environments and developing strategies that provide a multi-tiered information architecture by supporting organization objectives, such as:

- Maintenance of field devices, telemetry collection, or industrial-level process systems
- Enhanced data collection and dissemination
- Remote access

Overall, integration between IT and OT is increasing as organizations adapt to changing local and global needs and requirements. Utilizing the principles of a defense-in-depth architecture to systematically layer security controls – including people, processes, and technology – can help organizations strengthen their overall cybersecurity defenses. As a result, adversaries may find it increasingly difficult to penetrate the environment without detection. The following sections discuss specific defense-in-depth layers, including topics and ideas for organizations to consider when developing and implementing their defense-in-depth cybersecurity architecture. The layers are:

- Layer 1 – Security Management
- Layer 2 – Physical Security
- Layer 3 – Network Security
- Layer 4 – Hardware Security
- Layer 5 – Software Security

5.2.1. Layer 1 – Security Management

Security management or governance is the overarching cybersecurity program that supports the OT environment. Sections 3 and 4 discuss the program and risk management considerations for organizations to establish their cybersecurity programs. These programmatic and organizational decisions will guide and impact the decisions made for the other defense-in-depth layers. As a result, organizations should complete this layer before attempting to implement the other layers.

5.2.2. Layer 2 – Physical Security

Physical security measures are designed to reduce the risk of accidental or deliberate loss or damage to assets and the surrounding environment. Safeguarded assets may include control systems, tools, equipment, the environment, the surrounding community, and intellectual property, including proprietary data (e.g., process settings and customer information). Organizations may also need to consider additional environmental, safety, regulatory, legal, and other requirements when implementing physical security.

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

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

OT-Specific Recommendations and Guidance

Organizations should consider whether the physical security of remote assets is implemented at differing levels and whether those differences could create cyber risks. For example, one remote location may utilize only a padlock with minimal electronic surveillance to secure access to network equipment that, if bypassed, could allow a malicious actor to gain access to an OT network segment from the remote location.

Organizations should also consider whether secondary services, such as the communications and power that support physical security devices (e.g., cameras, sensors, etc.), require additional redundancy, isolation, protection, and monitoring.

5.2.3. Layer 3 – Network Security

Building from physical security, organizations should investigate network communications and how to protect the data and devices used to support their OT environment. This section focuses on several foundational elements to assist organizations with planning and implementing their network security capabilities. These include applying the network architecture principles of segmentation and isolation, centralizing logging, network monitoring, and malicious code protection. Additionally, this section discusses zero trust architecture (ZTA) and considerations for applying these architecture enhancements to an OT environment.

5.2.3.1. Network Architecture

A good practice for network architectures is to characterize, segment, and isolate IT and OT devices. For example, devices may be segmented based on management authority, level of trust, functional criticality, data flow, location, or other logical combinations. Organizations may also consider using an industry-recognized model to organize their OT network segmentation, such as the Purdue model [Williams], ISA-95 levels [IEC62264], the three-tier IIoT system architecture [IIRA19], or a combination of these models.

Additional, organizations may consider incorporating a DMZ as an enforcement boundary between network segments, as depicted in **Fig. 16**. Implementing network segmentation utilizing levels, tiers, or zones allows organizations to control access to sensitive information and components while also considering operational performance and safety.

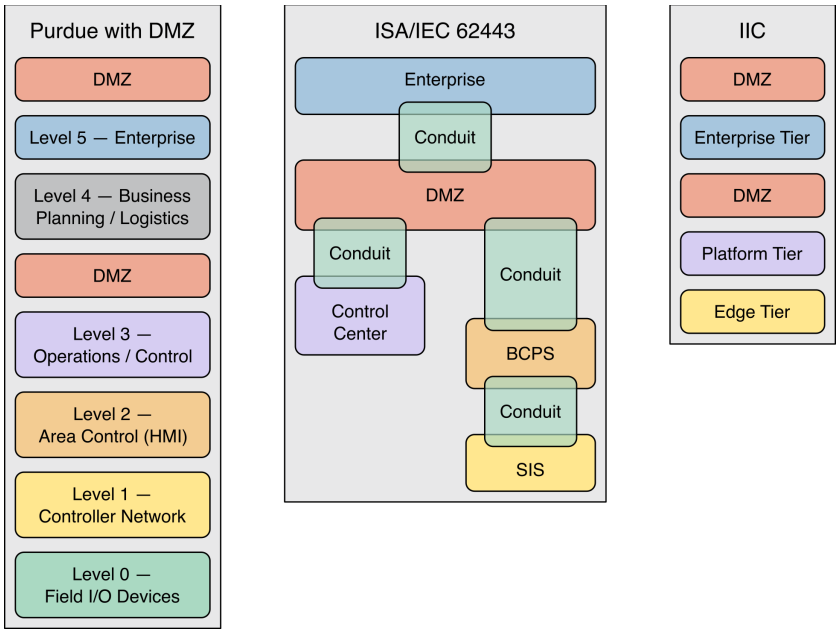

Fig. 16. High-level example of the Purdue model and IIoT model for network segmentation with DMZ segments

OT-Specific Recommendations and Guidance

Whether using a risk-based approach, functional model, or other organizing principle, grouping components into levels, tiers, or zones is a precursor activity before organizations can consider applying isolation devices to protect and monitor communications between levels, tiers, or zones. When organizing assets, organizations should consider how the zone and isolation configuration impact their day-to-day operations, safety, and response capabilities.

When properly configured, network architectures support segmentation and isolation by enforcing security policies and controlling network communications. Organizations typically utilize their mapped data flows to identify required communications. These requirements are then incorporated into the network architecture and configured into the policy engines of the network devices to support monitoring communication between segments and permitting only authorized communications. Network devices that support traffic enforcement capabilities (e.g., switches, routers, firewalls, and unidirectional gateways or data-diodes) can be used to implement network segmentation and isolation.

Firewalls are commonly used to support network isolation and employed as boundary protection devices to control connections and information flows between network segments. Firewalls may be deployed as network devices or directly run on some hosts. Firewalls are very flexible isolation devices and typically constitute the primary mechanism for protecting OT devices.

OT-Specific Recommendations and Guidance

Appropriate firewall configuration is essential to properly securing the network segments. Firewall rulesets should be established to only permit connections between adjacent levels, tiers, or zones. For example, organizations that utilize a Purdue model architecture should implement firewall rules and connection paths that prevent Level 4 devices from directly communicating with Level 2, 1, or 0 devices. A similar concept would be applied to ISA/IEC 62443 and IIC architectures.

One area of considerable variation in practice associated with firewall rules is the control of outbound traffic from the control network. Allowing outbound connections from lower levels, tiers, or zones could represent a significant risk if unmanaged. Organizations should consider making outbound rules as stringent as inbound rules to reduce these risks.

An alternative to firewalls is a unidirectional gateway or data diode that permits authorized communication in only one direction. The use of unidirectional gateways may provide additional protections associated with system compromises at higher levels or tiers within the environment. For example, a unidirectional gateway deployed between Layers 2 and 3 may protect Layer 0, 1, and 2 devices from a cybersecurity event that occurs at Layers 3, 4, or 5.

5.2.3.2. Centralized Logging

Network and computing devices (e.g., routers, gateways, switches, firewalls, servers, and workstations) should be configured to log events to support monitoring, alerting, and incident response analysis. Logging capabilities are typically available for recording events in applications, OSs, and network communications. A centralized log management platform can assist organizations with supporting log retention, monitoring, and analysis efforts.

OT-Specific Recommendations and Guidance

Organizations should review their available logging capabilities and configure them to record the operational and cybersecurity events that are appropriate for their environment.

Organizations should establish how long event logs should be retained and ensure that adequate storage is available to support log retention requirements.

5.2.3.3. Network Monitoring

Network monitoring involves reviewing alerts and logs and analyzing them for signs of possible cybersecurity incidents. Tools and capabilities that support behavior anomaly detection (BAD), security information and event management (SIEM), intrusion detection systems (IDS), and intrusion prevention systems (IPS) can assist organizations with monitoring traffic throughout the network and generate alerts when they identify anomalous or suspicious traffic. Some other capabilities to consider for network monitoring include:

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

Organizations may also want to consider incorporating additional services and capabilities, such as threat intelligence monitoring, to assist with establishing and maintaining an effective network monitoring capability.

OT-Specific Recommendations and Guidance

OT system traffic is typically more deterministic (i.e., repeatable, predictable, and designed) than IT network traffic, which can leveraged to support network monitoring for anomaly and error detection.

Organizations should understand the normal state of the OT network as a prerequisite for implementing network security monitoring to help distinguish attacks from transient conditions or normal operations within the environment. Implementing network monitoring in a passive (e.g., listen or learning) mode and analyzing the information to differentiate between known and unknown communication may be a necessary first step in implementing network security monitoring.

Organizations should consider the effects of encrypted network communications on their network monitoring capabilities and deployment strategies. For example, a BAD system or IDS may be unable to determine whether encrypted network communication is malicious and could generate false positive or negative alerts for the traffic. Changing the data collection point to capture network traffic before or after encryption (e.g., using host-based network monitoring tools) could help improve monitoring capabilities when encrypted communication is expected.

IDS and IPS products are effective at detecting and preventing well-known internet attacks, and some IDS and IPS vendors have incorporated attack signatures for various OT protocols, such as Modbus, Distributed Network Protocol 3 (DNP3), and Inter-Control Center Communications Protocol (ICCP). An effective IDS/IPS deployment typically involves both host-based and network-based capabilities.

Organizations should consider the impact that automated responses associated with IPS may have on the OT environment before deploying. In some cases, organizations may consider placing IPS units at higher levels in the environment (e.g., the DMZ interfaces) to minimize potential issues with automated responses impacting OT.

In OT environments, network-based monitoring capabilities are typically deployed on boundary protection devices using switched port analyzer (SPAN) ports or passive network taps. Organizations should also consider deploying host-based monitoring capabilities on compatible OT devices – such as HMIs, SCADA servers, and engineering workstations – to improve monitoring capabilities, provided that the addition of the tools does not adversely impact operational performance or safety.

5.2.3.4. Zero Trust Architecture (ZTA)

A ZTA is a cybersecurity paradigm that focuses on protecting resources (e.g., information services, data) based on the premise that authorization decisions are made closer to the resource being requested and are continuously evaluated rather than implicitly granted [SP800-207]. Conventional network security focuses on segmentation and perimeter defenses. Once inside the network perimeter, users are typically considered "trusted" and often given broad access to accessible resources. As a result, boundary protection devices between zones do not mitigate lateral movement risks within a zone. Additionally, with the growing prevalence of distributed computing, wireless and cellular communications, and cloud and hybrid-cloud environments, traditional network perimeters and boundaries are becoming less defined. For these situations, organizations might consider incorporating the principles of zero trust into their security architecture.

Some challenges to implementing a ZTA include:

- Organizations may not find a suitable single solution for a ZTA and may instead need to integrate several technologies with varying maturity levels to support their environment.
- Implementing zero trust principles into an existing environment may require more investments in time, resources, and technical ability.

OT-Specific Recommendations and Guidance

Some OT components (e.g., PLCs, controllers, HMI) may not support the technologies or protocols required to fully integrate with a ZTA implementation. As a result, a ZTA implementation might not be practical for some OT devices. Instead, organizations should consider applying a ZTA to compatible devices, such as those typically found at the functionally higher levels of the OT architecture (e.g., Purdue model Levels 3, 4, 5, and the OT DMZ).

Organizations may also want to consider whether any adverse impacts might occur, such as if the ZTA solution increases the latency to respond to resource requests or if one or more ZTA components become unavailable. Based on this analysis, organizations should consider

adjusting the ZTA implementations to minimize latency and ensure adequate redundancy to minimize risks to OT and safety operations.

Another important aspect of ZTA implementations is the identity of person and non-person entities accessing resources. Within OT environments, shared credentials may be utilized, which could impact the ability to fully implement a ZTA solution.

5.2.4. Layer 4 – Hardware Security

Hardware security protection mechanisms provide the foundation for supporting security and trust for the devices within an environment. Once device trust is established, the state must be maintained and tracked in accordance with the system model and policy. To support these capabilities, some vendors provide embedded technology, such as the Trusted Platform Module (TPM), or hardware implementation for the Advanced Encryption Standard (AES) and the Secure Hash Algorithm (SHA). Overall, hardware security capabilities enhance endpoints to provide specific function and security requirements, including:

- Monitoring and analysis
- Secure configuration and management
- Endpoint hardening
- Integrity protection
- Access control
- Device identity
- Root of trust
- Physical security

OT-Specific Recommendations and Guidance

Organizations should review available hardware security and automated capabilities to determine how they can support OT environments without impacting operational performance, safety, or capabilities.

5.2.5. Layer 5 – Software Security

Software security protection mechanisms provide organizations with capabilities to ensure that applications and services supporting OT are used and maintained properly. Overall, software security capabilities can enhance endpoint security when organizations incorporate:

- Application allowlisting
- Patching
- Secure code development
- Configuration management, including application hardening

5.2.5.1. Application Allowlisting

Application allowlisting technologies provide an additional protection mechanism on hosts by restricting which applications are allowed to execute. When properly configured, non-authorized applications will not execute on the host environment.

OT-Specific Recommendations and Guidance

The relatively static nature of OT environments presents an opportunity for organizations to include application allowlisting as part of their defense-in-depth strategy and is a recommended best practice by DHS. When considering application allowlisting within an OT environment, organizations should coordinate with their vendors and review available implementation guidance, such as NIST SP 800-167, *Guide to Application Whitelisting* [SP800-167]; Guidelines for Application Whitelisting in Industrial Control Systems; or relevant guidance for their industry. The configurations and policies should be thoroughly tested before being deployed to ensure that the rules and settings properly support organizational security objectives.

5.2.5.2. Patching

Patches have two main purposes: to address vulnerabilities and to enhance functionality. In the context of defense-in-depth software security, patching is associated with reducing vulnerabilities. As a result, patch management is a defense-in-depth capability that supports vulnerability management as part of an organizational risk management strategy.

Deploying patches to OT environments requires additional considerations for organizations, including testing and validation to ensure that the patches do not impact operational capabilities or safety. OT operational requirements can also impact the frequency with which patches are applied. For example, some OT environments must run nearly continuously for extended periods of time or have small maintenance windows for applying approved updates. Additionally, patching older OT components that run on unsupported OSs may not be an option. In these cases, organizations may want to consider updating their OSs or investing in additional controls that can protect the environment from attempts to exploit known vulnerabilities. Some tools, such as web application firewalls (WAF) and IPS, could be configured to provide additional protection to detect or prevent attacks against unpatched vulnerabilities while the organization waits for an opportunity to apply the updates. Other tools, such as bump-in-the-wire security devices, can be installed in line with devices that cannot be updated or are using obsolete operating systems.

OT-Specific Recommendations and Guidance

Whenever possible, patches should be tested on a sandbox system (i.e., test environment) to ensure that they do not cause problems before being deployed into a production system. Organizations should plan patches and updates during scheduled maintenance windows for the environment and have a recovery plan for the OT component or system being patched.

Organizations should also consider that different levels, tiers, and zones may have different availability requirements and, as such, may have different abilities to support patching. Whenever possible, organizations should prioritize patching components within DMZ environments and when vulnerabilities exist that impact availability and integrity or would allow unauthorized remote access to the OT environment.

5.2.5.3. Secure Code Development

Organizations that develop in-house systems and components should incorporate policies and procedures that support and validate secure code development practices into the cybersecurity program. The software development life cycle (SDLC) should include security during each phase of software development. This should include security reviews and coding techniques for each of the following processes:

- Using or developing tools to audit and automate secure code techniques
- Testing and reviewing code to comply with secure coding practices
- Testing the software for security errors in programming

For organizations that procure components or services from third parties, reviewing these same practices should be considered prior to executing contracts with vendors. Organizations can help industries move toward more secure products by requesting these practices in their service-level agreements and procurement actions.

5.2.5.4. Configuration Management

Applying configuration management practices that support secure configurations and application hardening is important to meet organizational and regulatory security requirements. These settings may include setting access controls to restrict access or enabling encryption to protect data at rest or in transit. Application hardening procedures may include disabling or blocking specific network communication ports, application features, or unnecessary services that run on the system.

Encrypting data that flows over networks (i.e., in transit) or data stored in memory and local storage (i.e., at rest) can also be used in defending OT. Encryption prevents an attacker from viewing or modifying cleartext data streams. Because encryption and the subsequent decryption process use algorithms to create ciphers, encryption adds latency and may not be suitable for all OT devices. Knowing the advantages and disadvantages of encryption can help organizations make an informed decision on where to include encryption in the defense-in-depth strategy.

OT-Specific Recommendations and Guidance

Organizations should consider using encryption to support secure connections or conduits for OT environments when the connections must pass over non-OT network segments, such as the corporate network or the internet. Virtual private network (VPN) connections should also use encryption protocols, such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec), to secure the data.

Encryption can also be used on hard local storage to protect information at rest. Full disk encryption is recommended for portable laptops and devices. Organizations may also want to consider encrypting folders that contain sensitive files.

Organizations must also consider that encryption can negatively impact other defense tools, such as network monitoring. For example, an IDS might not be able to determine whether an encrypted packet is malicious, resulting in either false-positive or false-negative alerts.

Organizations should also create procedures to manage changes to control logic to protect against the risk that improperly tested or malicious changes to logic could disrupt the system.

5.3. Additional Cybersecurity Architecture Considerations

Organizations should include considerations for supporting cyber-related safety, availability, geographically distributed systems, environmental considerations, and regulatory requirements into the security architecture designs and implementations for OT and IIoT environments. The following subsections discuss these considerations in more detail.

5.3.1. Cyber-Related Safety Considerations

OT systems are generally designed with specific safety goals, depending on both the business environment and regulatory requirements. Organizations should consider whether the additional communication and cybersecurity requirements of safety systems (e.g., segmentation and the isolation of safety systems from other OT systems) is required. Additionally, safety requirements can influence the selection of security mechanisms. For example, safety considerations may require that an organization use physical separation as opposed to logical separation.

OT systems typically employ fail-to-a-known-state design (i.e., fail-safe design) in the event of an unexpected situation or a component failure. Fail-safe design considers placing the equipment or process in a safe state that prevents injury to individuals or the destruction of property and avoids cascading events or secondary hazards. Cyber-related events, such as the loss of network communications, could trigger these fail-safe events. To minimize false positives, organizations should define the thresholds at which OT components can operate with reduced or disrupted capabilities, such as lost network communications.

5.3.2. Availability Considerations

Operational continuity management requires managing availability at multiple levels, including data, applications, IT infrastructure, power, and other supporting utilities (e.g., HVAC, water, steam, compressed air, etc.). The failure of these systems can have a cascading effect on OT systems and can adversely impact the OT operation. Different availability considerations are presented below.

5.3.2.1. Data, Applications, and Infrastructure

Architecture requirements and design should support the redundancy needs of OT systems. Availability can be enhanced using redundancy at the communication, system, or component level such that a single failure is less likely to result in a capability or information outage. Cybersecurity architecture should consider any redundant communication and protect it to the same security level as the primary.

Additionally, a data backup and restoration process will facilitate the speedy recovery of systems if data is lost due to cyber attacks or other reasons. Examples of important data and files are operational data, program files, configuration files, system images, firewall rules, and access control lists (ACLs). A "backup-in-depth" approach with multiple layers of backups (e.g., local, facility, disaster) that are time-sequenced such that rapid recent local backups are available for immediate use and secure backups are available to recover from a massive security incident (e.g., ransomware attack) can help improve OT system availability. Periodically testing data backup and restore capabilities will ensure their availability when the need arises.

5.3.2.2. Primary and Alternate Power Sources

Architectural considerations should include the impact of power outages on OT systems. For example, if the OT systems need a graceful degradation or orderly shutdown, then an alternate backup power may be considered. In addition, if the organization's business continuity plan requires that the OT systems continue operating in the event of an extended loss of the primary power source, a long-term alternate power supply for the OT systems that is self-contained and not reliant on external power generation can be implemented. The monitoring and controls systems for the power system are vulnerable to cyber attacks, so appropriate cybersecurity practices should be implemented.

5.3.2.3. Other Utilities

Industrial facilities typically have monitoring and controls systems that manage uninterruptable power supplies (UPSs), generators, HVAC, fire alarm systems, boilers, cooling water plant, steam, compressed air, and other critical functions. These monitoring and controls systems are also vulnerable to cyber attacks and can affect the OT systems, so appropriate cybersecurity practices should be implemented to protect them.

OT-Specific Recommendations and Guidance

Disaster recovery planning is another important activity for OT systems, especially when there are safety concerns. Organizations should establish and maintain a disaster recovery plan (DRP) that details the actions to take before, during, and after a natural, environmental, or human-caused (intentionally or unintentionally) disaster. The DRP should also include instructions for restoring and restarting failed components and integrating them back into operation. Organizations should consider testing the DRP to ensure that the necessary architecture capabilities can be operationalized in an actual disaster recovery scenario. Tabletop exercises can also be used to simulate a disaster recovery event to support testing.

5.3.3. Geographically Distributed Systems

Many critical infrastructure industries have sites that are geographically distributed. Organizations should consider whether differences in physical security at remote locations create risks to the OT operational capabilities or safety. The necessary cybersecurity and communication infrastructure should be provided at the remote sites to protect them from cyber threats and to communicate cybersecurity monitoring information.

OT-Specific Recommendations and Guidance

The communication between sites should be encrypted and authenticated end to end, whether the connection is via point-to-point link, satellite, or internet. Organizations should also ensure that adequate bandwidth is provisioned for collecting cyber monitoring data in addition to the operational data from remote locations.

If the organization has several geographically dispersed sites, it should consider whether security operation will be managed from a central security operations center (SOC) or regionally distributed SOCs. The availability of qualified personnel can impact these decisions.

5.3.4. Regulatory Requirements

Regulated industries must consider cyber-related regulatory requirements when designing their cybersecurity architecture. For example, NERC Standard CIP-005 (see Appendix D.1.9) provides cybersecurity architecture requirements for bulk electric systems. Similar requirements and guidance exist for other regulated industries.

5.3.5. Environmental Considerations

Organizations should conduct a hazard analysis to determine whether any of their processes or equipment pose environmental hazards. If potential environmental hazards due to cybersecurity failure have been identified, organizations should consider architectural measures to prevent them.

5.3.6. Field I/O (Purdue Level 0) Security Considerations

Many of the devices and the communication protocols at the Field I/O level (Purdue Level 0) (e.g., sensors, actuators) cannot be authenticated. Without authentication, there is the potential to replay, modify, or spoof data. Organizations should make a risk-based decision to decide where within the OT system (e.g., the most critical process) the use of mitigating security controls (e.g., digital twins, separate Field I/O monitoring network) should be implemented to detect incorrect data.

5.3.7. Additional Security Considerations for IIoT

The introduction of IIoT to OT environments can increase connectivity and information exchanges with enterprise systems and cloud-based systems, which may require additional considerations for the security architecture. For example, the introduction of IIoT devices in OT environments may require altering boundaries or exposing more interfaces and services. Additionally, the security capabilities of IIoT devices may need to be considered when developing the security architecture.

OT-Specific Recommendations and Guidance

Organizations may need to consider the impacts of supporting IIoT on policy management, enforcement, and governance. Additionally, the integration of IIoT into OT environments may require a tighter collaboration between IT and OT security teams to manage the security operations. For example, real-time situational awareness should be shared between IT and OT security teams.

5.3.7.1. Application and Infrastructure

Organizations should consider the IIoT data flow use cases, including those that share data externally, to determine whether additional access control mechanisms are necessary. Organizations should also consider that the attack vectors for IIoT may be different from those managed for OT environments (e.g., due to increased communications requirements or the use of additional services, such as cloud systems, to support operational requirements).

OT-Specific Recommendations and Guidance

Organizations should consider the following endpoint security capabilities of the IIoT devices being deployed:

- Endpoint tamper resistance capabilities
- Endpoint root of trust
- Endpoint identity
- Endpoint access control
- Endpoint integrity protection
- Endpoint data protection
- Endpoint monitoring and analysis
- Endpoint configuration and management
- Cryptographic techniques
- Capability to harden endpoints

5.3.7.2. Cybersecurity Capability Considerations

Compute resources – including processing, memory, and storage – vary among IIoT devices. Some IIoT devices may have constrained resources, while others may have unused capabilities, both of which have implications for cybersecurity. Organizations should consider how the resources and capabilities available in the IIoT devices will integrate into the security architecture to achieve their cybersecurity objectives. Additionally, organizations should consider whether the operational and safety impacts for IIoT differ from the operational and safety impacts for other OT devices. For example, IIoT devices may support a separate data monitoring (i.e., read-only capability) for the environment and have minimal impact on operational controls or safety, which may allow organizations to implement security operations differently than those established for OT devices.

5.4. Cybersecurity Architecture Models

Building on the concepts and guidance from Sections 5.1, 5.2, and 5.3, the following subsections expand on the general OT and IIoT environments described in Section 2 and provide examples for how the environments might be adapted to support defense-in-depth security architectures.

5.4.1. Distributed Control System (DCS)-Based OT Systems

As described in Section 2, a distributed control system (DCS) is used to control production systems within the same geographic location for industries. **Figure 17** shows an example DCS system implementation. **Figure 18** shows an example defense-in-depth architecture applied to the DCS system.

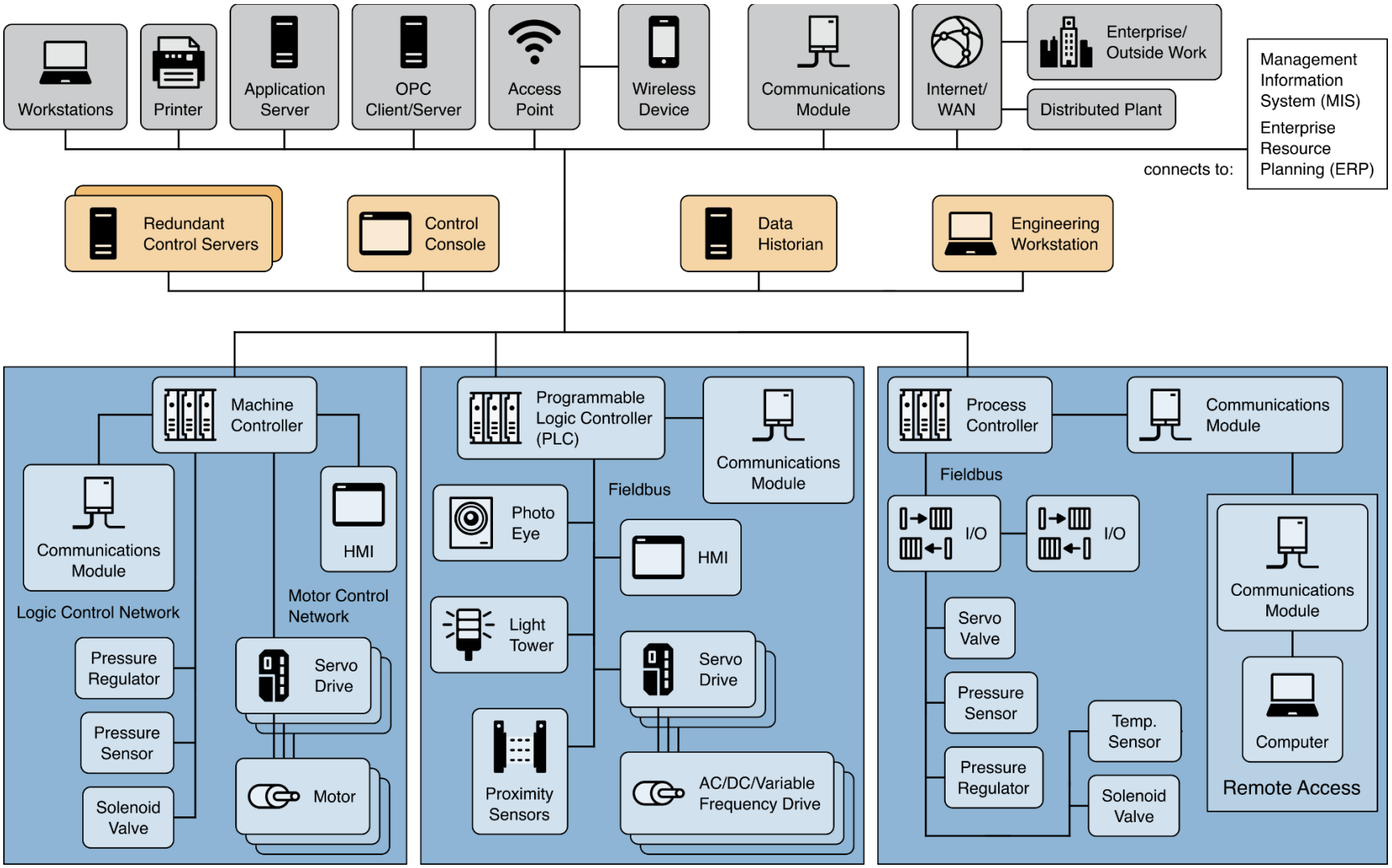

Fig. 17. A DCS implementation example

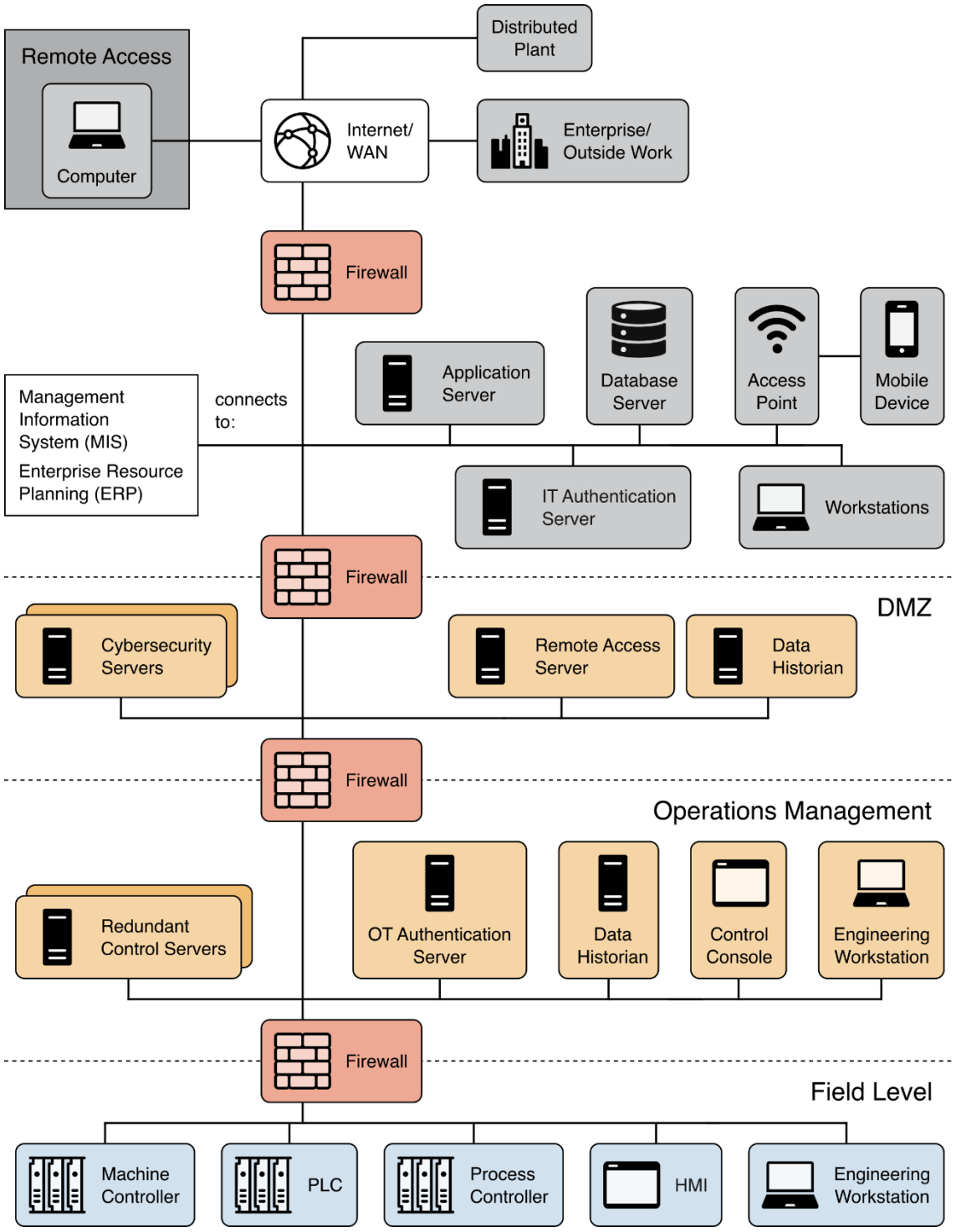

Fig. 18. A defense-in-depth security architecture example for a DCS system

In **Fig. 18**, the assumption is that the organization has already addressed Layer 1 and Layer 2. For Layer 3, the organization should consider incorporating the following capabilities into the security architecture:

- Separate networks into different levels or zones. In this example, the devices are split into different levels based on function. The field level includes devices that are typically found in the Purdue model levels 0, 1, and 2. The operations management level includes devices for monitoring and managing the field level devices and the Purdue level 3 components. The DMZ includes devices that support bridging the operations management and enterprise tiers. Organizations should also consider whether additional network segments are required for safety or security systems (e.g., physical monitoring and access controls, doors, gates, cameras, Voice over Internet Protocol [VoIP], access card readers). Network segmentation is an important step in applying a defense-in-depth strategy.
- Boundary devices (e.g., firewalls) are added to control and monitor communications between different levels. Industrial-class firewalls are sometimes used between the field and operations management levels to provide additional support for OT-specific protocols or to allow devices to operate in harsh environments. Rules for both inbound and outbound communication should be defined so that only authorized communication passes between adjacent levels.
- Implement a DMZ to separate the OT environment from the enterprise network. Any communications between the enterprise level and the operations management level are required to go through services within the DMZ. Since the DMZ connects to outside environments, the services within the DMZ must be monitored and protected to avoid compromises that allow attackers to pivot to the OT environment without detection.
- The security architecture diagram shows an IT authentication server in the enterprise network to authenticate users and a separate OT authentication server in the operations management network for OT users. Organizations may want to consider this approach if it supports their risk-based security objectives.

For Layer 4 and Layer 5, organizations should consider applying the principle of least functionality on all field, operations management, and DMZ devices to support application and device hardening. Organizations should identify and disable any non-essential capability, software, or ports on the devices. For example, a web server or SSH server may be available in some newer PLCs or HMIs. If these services are not used, they should be disabled, and the associated TCP/UDP ports should be disabled as well. Only enable the functionality when required.

5.4.2. DCS- and PLC-Based OT with IIoT

Building on the guidance for DCS- and PLC-based OT environments in Section 5.4.1, **Fig. 19** shows a simplified example security architecture implementation for the DCS system with additional IIoT devices configured to utilize a local IIoT platform for providing computing capabilities. Due to the different communication and architectural components that support IIoT, the example shows separate network segments for supporting the additional IIoT components. Communication from the IIoT platform tier is routed through the DMZ border firewall to allow

organizations to consider data transmission to servers in the DMZ or to the enterprise/internet as required to support IIoT operational requirements. Additionally, this also permits the cybersecurity services located in the DMZ to monitor the IIoT platform tier.

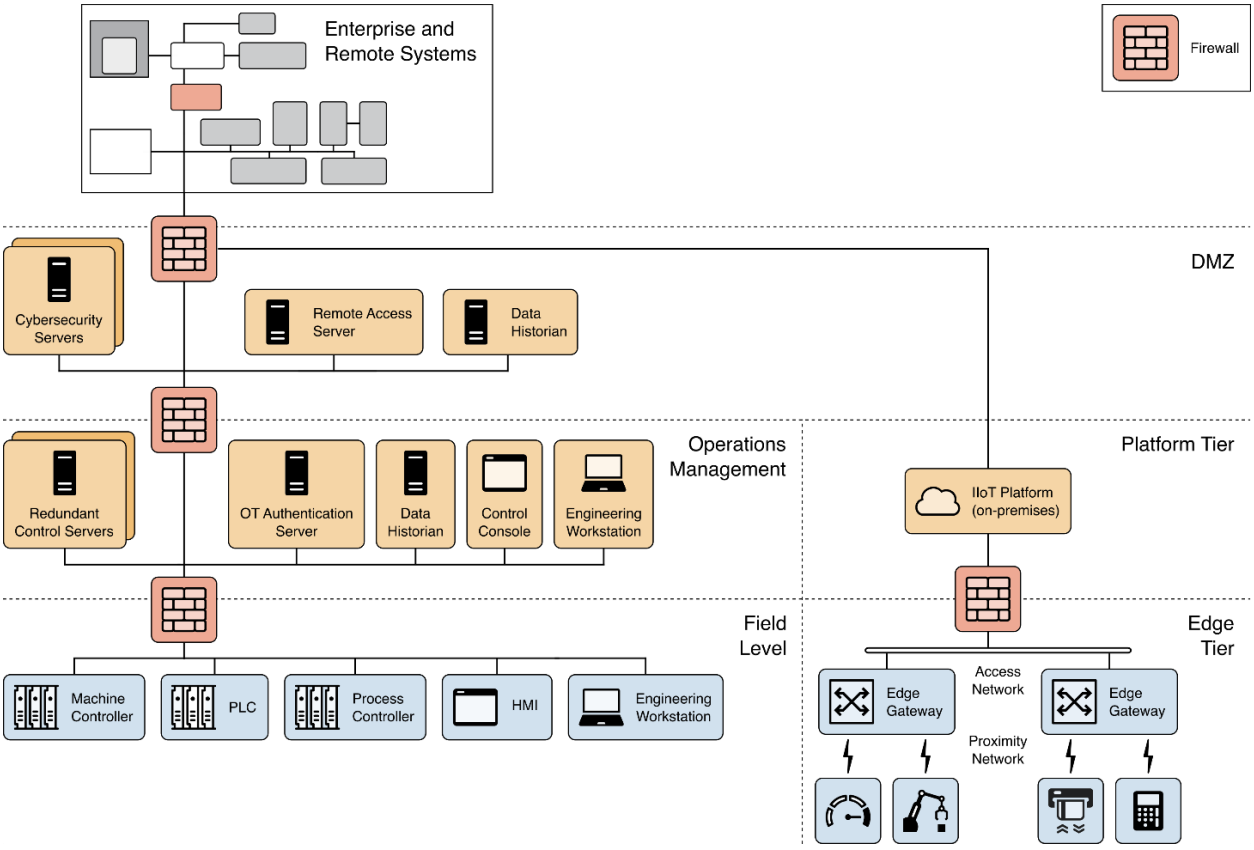

Fig. 19. A security architecture example for DCS system with IIoT devices

5.4.3. SCADA-Based OT Environments

Figure 20 shows an example implementation of the components and general configuration of a SCADA system. Typically, primary and backup control centers support one or more remote stations based on geographic locations, and regional control centers are geographically located to support one or more primary or backup control centers. Due to the distributed nature of the remote stations and control centers, communication between locations typically passes over external or WAN connections using wireless or wired mediums.

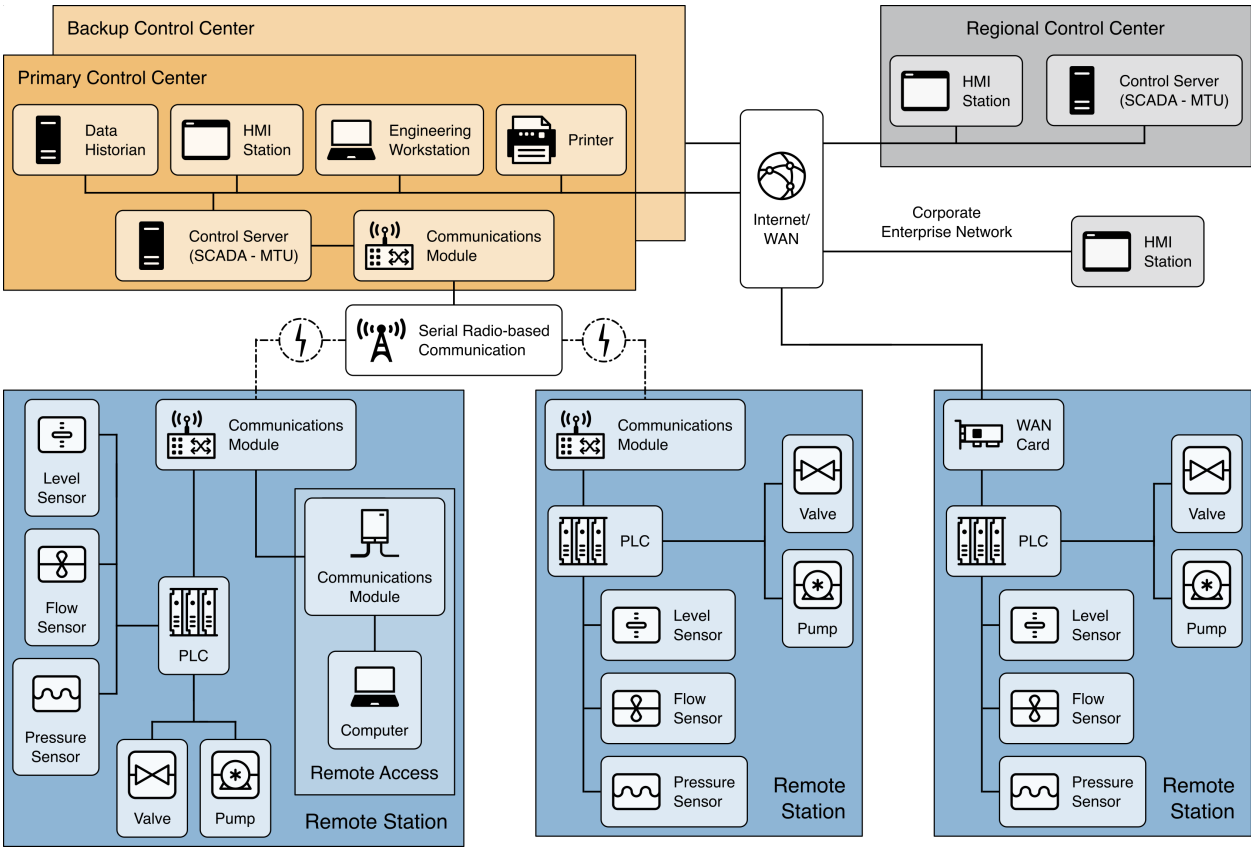

Fig. 20. An example SCADA system in an OT environment

Figure 21 shows an example defense-in-depth implementation for a SCADA system that assumes that the organization has already addressed Layer 1 and Layer 2. For Layer 3, the organization should consider incorporating the following capabilities in the security architecture:

- Separate networks into different zones or regions, which is important for applying a defense-in-depth strategy in a SCADA environment. Additional separation should be considered for security systems (e.g., physical monitoring and access controls, doors, gates, cameras, VoIP, access card readers).
- Boundary devices (e.g., firewalls) are added between the different regions to control and monitor communications between the network segments. Industrial-class stateful firewalls may offer more support for OT-specific protocols and enhance protection for OT devices, like the PLC and controllers. Rules for inbound and outbound communication should be defined so that only authorized communication passes between regions.
- Use secure connections (e.g., VPN tunnel, encrypted channel, point-to-point connection) between network segments, such as between a regional center and primary control centers and between remote stations and control centers. For geographically distanced locations, secure connections can be connected over the internet/WAN. Devices in the network segments should only connect to other segments through the secure connection and should be restricted when accessing the internet.

- Implement a DMZ to separate the control centers from the enterprise network. Any communications between the enterprise network and the control centers must go through services within the DMZ. Since the DMZ connects to outside environments, the services within the DMZ must be monitored and protected to avoid compromises within the DMZ that might allow attackers to pivot to the OT environment without detection.

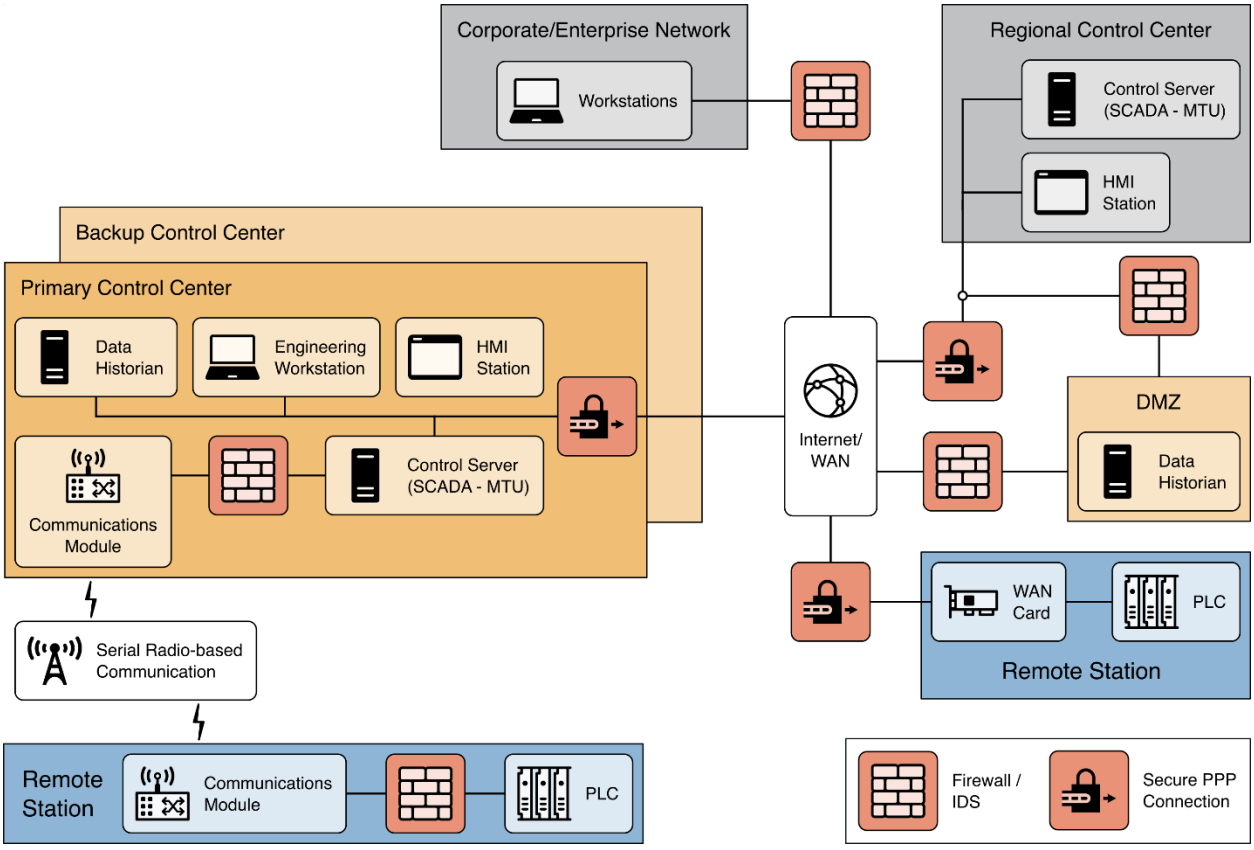

Fig. 21. A security architecture example for a SCADA system

For Layer 4 and Layer 5, organizations should consider applying the principle of least functionality to all remote station components, control center components, and DMZ devices to support application and device hardening. Organizations should identify and disable any non-essential capability, software, or ports on the devices. For example, a webserver or SSH server may be available in some newer PLCs or HMIs. If these services are not used, they should be disabled, and the associated TCP/UDP ports should be disabled. Only enable the functionality when required.

6. Applying the Cybersecurity Framework to OT

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

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

The CSF Functions guide the following actions:

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

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

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

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

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

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

6.1. Identify (ID)

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

6.1.1. Asset Management (ID.AM)

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

6.1.2. Governance (ID.GV)

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

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

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

OT-Specific Recommendations and Guidance

Organizations should consider:

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

6.1.3. Risk Assessment (ID.RA)

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

6.1.4. Risk Management Strategy (ID.RM)

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

6.1.5. Supply Chain Risk Management (ID.SC)

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

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

6.2. Protect (PR)

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

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

6.2.1.1. Logical Access Controls (PR.AC)

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

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

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

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

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

OT-Specific Recommendations and Guidance

Organizations should consider the following:

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

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

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

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

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

The following are additional physical security considerations:

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

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

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

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

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

6.2.1.4.1. Physical Token Authentication

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

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

Common forms of physical or token authentication include:

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

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

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

6.2.1.4.2. Biometric Authentication

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

Noted issues with biometric authentication include:

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

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

OT-Specific Recommendations and Guidance

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

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

6.2.1.4.3. Smart Card Authentication

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

6.2.1.4.4. Multi-Factor Authentication

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

OT-Specific Recommendations and Guidance

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

6.2.1.4.5. Password Authentication

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

compromised or an individual with access leaves the organization.

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

6.2.2. Awareness and Training (PR.AT)

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

6.2.3. Data Security (PR.DS)

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

Cryptography

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

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

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

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

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

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

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

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

6.2.4.1. Least Functionality (PR.IP-1)

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

Supplemental guidance can be found in the following document:

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

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

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

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

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

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

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

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

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

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

6.2.4.3. Backups (PR.IP-4)

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OT-Specific Recommendations and Guidance

Incident response planning may include the following elements:

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

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

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

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

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

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

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

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

6.2.5. Maintenance (PR.MA)

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

6.2.6. Protective Technology (PR.PT)

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

6.2.6.1. Logging (PR.PT-1)

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

Supplemental guidance can be found in the following document:

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

OT-Specific Recommendations and Guidance

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

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

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

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

6.2.7. Media Protection (PR.PT-2)

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

6.2.8. Personnel Security

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

6.2.9. Wireless Communications

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

Wireless LANs

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

Wireless Field Networks

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

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

- Implementing appropriately complex passwords and join keys

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

6.2.10. Remote Access

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

Regardless of the technology, organizations should consider the following:

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

Dial-Up Modems

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

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

VPNs

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

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

6.2.11. Flaw Remediation and Patch Management

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

6.2.12. Time Synchronization

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

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

6.3. Detect (DE)

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

6.3.1. Anomalies and Events (DE.AE)

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

Information Events

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

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

Operational Events

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

Physical Access Events

- Physical intrusions

Networking Events

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

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

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

6.3.2. Security Continuous Monitoring (DE.CM)

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

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

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

6.3.2.1. Network Monitoring (DE.CM-1)

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

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

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

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

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

Supplemental guidance can be found in the following documents:

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

Generally:

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

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

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

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

6.3.2.4. Vulnerability Scanning (DE.CM-8)

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

OT-Specific Recommendations and Guidance

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

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

6.3.3. Detection Process (DE.DP)

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

6.4. Respond (RS)

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

6.4.1. Response Planning (RS.RP)

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

6.4.2. Response Communications (RS.CO)

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

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

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

Internal Resources

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

External Industry Partners

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

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

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

6.4.3. Response Analysis (RS.AN)

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

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

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

OT-Specific Recommendations and Guidance

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

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

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

6.4.4. Response Mitigation (RS.MI)

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

OT-Specific Recommendations and Guidance

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

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

6.4.5. Response Improvements (RS.IM)

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

6.5. Recover (RC)

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

6.5.1. Recovery Planning (RC.RP)

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

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

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

6.5.2. Recovery Improvements (RC.IM)

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

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

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

6.5.3. Recovery Communications (RC.CO)

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

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

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

OT-Specific Recommendations and Guidance

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

Internal Communications

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

External Communications

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

References

[AGA12] American Gas Association (2006) Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan. AGA Report No. 12.

[ANSI-ISA-5-1] International Society of Automation (2009) Instrumentation Symbols and Identification, ANSI/ISA-5.1-2009. Available at https://webstore.ansi.org/Standards/ISA/ANSIISA2009

[ANSI-ISA-51-1] International Society of Automation (1993) Process Instrumentation Terminology, ANSI/ISA-51.1-1979 (R1993). Available at https://www.isa.org/products/isa-51-1-1979-r1993-process-instrumentation-termin

[ANSI-ISA-84] Instrumentation, Systems, and Automation Society (2004) Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware, and Software Requirements. ANSI/ISA-84.00.01-2004 Part 1. Available at https://webstore.ansi.org/standards/isa/ansiisa8400012004part

[ATTACK-ICS] The MITRE Corporation (2022) *ATT&CK® for Industrial Control Systems.* Available at https://attack.mitre.org/techniques/ics/

[Bailey] Bailey D, Wright E (2003) Practical SCADA for Industry. (IDC Technologies, Vancouver, Canada).

[Berge] Berge J (2002) Fieldbuses for Process Control: Engineering, Operation, and Maintenance. (International Society of Automation, Research Triangle Park, North Carolina).

[Boyer] Boyer S (2010) SCADA: Supervisory Control and Data Acquisition. 4th ed. (International Society of Automation, Research Triangle Park, North Carolina).

[CISA-CIVR] Cybersecurity and Infrastructure Security Agency (2021) Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. Available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[CNSS1253] Committee on National Security Systems (2014) Security Categorization and Control Selection for National Security Systems. CNSS Instruction (CNSSI) No. 1253. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CNSS4009] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. CNSS Instruction (CNSSI) No. 4009. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP6

[EO13636] Executive Order 13636 (2013) Improving Critical Infrastructure Cybersecurity. (The White House, Washington, DC), DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/DCPD-201300091

[Erickson] Erickson K, Hedrick J (1999) Plantwide Process Control. (John Wiley & Sons, Inc., New York, NY).

[FIPS140-2] National Institute of Standards and Technology (2001) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-2, Change Notice 2 December 03, 2002. https://doi.org/10.6028/NIST.FIPS.140-2

[FIPS140-3] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS180] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS186] National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 186-5. https://doi.org/10.6028/NIST.FIPS.186-5

[FIPS197] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST FIPS 197-upd1, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

[FIPS199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[FIPS200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[FIPS201] National Institute of Standards and Technology (2022) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3. https://doi.org/10.6028/NIST.FIPS.201-3

[FIPS202] National Institute of Standards and Technology (2015) SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 202. https://doi.org/10.6028/NIST.FIPS.202

[FISMA] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. https://www.govinfo.gov/app/details/PLAW-113publ283

[IEC61511] International Electrotechnical Commission (2016) Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, IEC 61511-1:2016. Available at https://webstore.iec.ch/publication/24241

[IEC62264] International Electrotechnical Commission (2013) Enterprise-control system integration - Part 1: Models and terminology, IEC 62264-1:2013. Available at https://webstore.iec.ch/publication/6675

[IIRA19] Industry IoT Consortium (2019) The Industrial Internet of Things Volume G1: Reference Architecture, Version 1.9. Available at https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[IR6859] Falco J, Stouffer K, Wavering A, Proctor F (2002) IT Security for Industrial Control Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) 6859. Available at https://doi.org/10.6028/NIST.IR.6859

[IR8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal or Interagency Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[IR8183A] Stouffer KA, Zimmerman T, Tang C, Pease M, Cichonski JA, Shah N, Downard W (2019) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183A, Vol. 1. https://doi.org/10.6028/NIST.IR.8183A-1

Stouffer KA, Zimmerman T, Tang C, Pease M, Cichonski JA, Shah N, Downard W (2019) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183A, Vol. 2. https://doi.org/10.6028/NIST.IR.8183A-2

Stouffer KA, Zimmerman T, Tang C, Pease M, Cichonski JA, Shah N, Downard W (2019) Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8183A, Vol. 3. https://doi.org/10.6028/NIST.IR.8183A-3

[ISA62443] International Society of Automation (2020) Security for industrial automation and control systems (all parts), ISA-62443. Available at https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

[ISADICT] International Society of Automation [2002] The Automation, Systems, and Instrumentation Dictionary, 4th Edition. International Society of Automation.

[ISO7498-1] ISO/IEC 7498-1:1994, Available at https://www.iso.org/standard/20269.html

[Knapp] Knapp E (2011) Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, (Syngress, Waltham, Massachusetts).

[OMB-A130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource

[OMB-M1917] Office of Management and Budget (2019) Enabling Mission Delivery through Improved Identity, Credential, and Access Management. (The White House, Washington, DC), OMB Memorandum M-19-17, May 21, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

[Peerenboom] Peerenboom J (2001) "Infrastructure Interdependencies: Overview of Concepts and Terminology." (NSF/OSTP Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training, Washington, DC).

[PF] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.10

[PPD-21] Presidential Policy Directive 21 (2013) Critical Infrastructure Security and Resilience. (The White House, Washington, DC), February 12, 2013. Available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[PPD-41] Presidential Policy Directive 41 (2016) United States Cyber Incident Coordination. (The White House, Washington, DC), July 26, 2016. Available at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[RFC4949] Shirey R (2007) Internet Security Glossary, Version 2. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 4949. https://doi.org/10.17487/RFC4949

[Rinaldi] Rinaldi SM, Peerenboom JP, Kelly TK (2001) "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, Vol. 21, No. 6, pp. 11-25, December 2001). https://doi.org/10.1109/37.969131

[SP1058] Falco JA, Hurd S, Teumim D (2006) Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1058. https://doi.org/10.6028/NIST.SP.1058

[SP800-100] Bowen P, Hash J, Wilson M (2006) Information Security Handbook: A Guide for Managers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[SP800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP800-161] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1

[SP800-167] Sedgewick A, Souppaya MP, Scarfone KA (2015) Guide to Application Whitelisting. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-167. https://doi.org/10.6028/NIST.SP.800-167

[SP800-18r1] Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1

[SP800-207] Rose SW, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[SP800-28v2] Jansen W, Winograd T, Scarfone KA (2008) Guidelines on Active Content and Mobile Code. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-28, Version 2. https://doi.org/10.6028/NIST.SP.800-28ver2

[SP800-30r1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP800-34r1] Swanson MA, Bowen P, Phillips AW, Gallup D, Lynes D (2010) Contingency Planning Guide for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-34, Rev. 1, Includes updates as of November 11, 2010. https://doi.org/10.6028/NIST.SP.800-34r1

[SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP800-40r4] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4

[SP800-41r1] Scarfone KA, Hoffman P (2009) Guidelines on Firewalls and Firewall Policy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-41, Rev. 1. https://doi.org/10.6028/NIST.SP.800-41r1

[SP800-47] Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47. https://doi.org/10.6028/NIST.SP.800-47

[SP800-53Ar5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[SP800-53B] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53B

[SP800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-60v1r1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP800-60v2r1] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP800-61] Grance T, Kent K, Kim B (2004) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61. https://doi.org/10.6028/NIST.SP.800-61

[SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP800-67r2] Barker EB, Mouha N (2017) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-67, Rev. 2. https://doi.org/10.6028/NIST.SP.800-67r2

[SP800-73-4] Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016. https://doi.org/10.6028/NIST.SP.800-73-4

[SP800-76-2] Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2. https://doi.org/10.6028/NIST.SP.800-76-2

[SP800-78-4] Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4. https://doi.org/10.6028/NIST.SP.800-78-4

[USC44-3552] "Definitions," Title 44 *U.S. Code*, Sec. 3552. 2018 ed. Available at https://www.govinfo.gov/app/details/USCODE-2020-title44/USCODE-2020-title44-chap35-subchapII-sec3552

[Williams] Williams TJ (1989) A Reference Model For Computer Integrated Manufacturing (CIM). (Instrument Society of America, Research Triangle Park, NC). Available at http://www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html

Appendix A. List of Symbols, Abbreviations, and Acronyms

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

A3
Association for Advancing Automation

ABAC
Attribute-Based Access Control

ACC
American Chemistry Council

ACI
Aviation Cyber Initiative

ACL
Access Control List

AES
Advanced Encryption Standard

AFPM
American Fuel and Petrochemical Manufacturers

AGA
American Gas Association

AHA
American Hospital Association

AI
Artificial Intelligence

AMA
American Medical Association

AMWA
Association of Metropolitan Water Agencies

AO
Authorizing Official

APCP
American Hospital Association Preferred Cybersecurity Provider

API
American Petroleum Institute, Application Programming Interface

APPA
American Public Power Association

ASDSO
Association of State Dam Safety Officials

ATO
Air Traffic Organization

AWWA
American Water Works Association

BAD
Behavioral Anomaly Detection

BAS
Building Automation System

BCP
Business Continuity Plan

BES
Bulk Electric System

BPCS
Basic Process Control System

C-SCRM
Cybersecurity Supply Chain Risk Management

CCE
Consequence-Driven Cyber-Informed Engineering

CD
Compact Disc

CDC
Cybersecurity Defense Community

CEDS
Cybersecurity for Energy Delivery Systems

CEO
Chief Executive Officer

CERT
Computer Emergency Response Team

CESER
Cybersecurity, Energy Security, and Emergency Response

CFATS
Chemical Facility Anti-Terrorism Standards

CI
Critical Infrastructure

CIE
Cyber-Informed Engineering

CIGRE
International Council on Large Electric Systems

CIM
Computer Integrated Manufacturing

CIO
Chief Information Officer

CIP
Common Industrial Protocol, Critical Infrastructure Protection

CIPAC
Critical Infrastructure Partnership Advisory Council

CISA
Cybersecurity and Infrastructure Security Agency

CISO
Chief Information Security Officer

CMVP
Cryptographic Module Validation Program

CNSS
Committee on National Security Systems

CNSSI
Committee on National Security Systems Instruction

COO
Chief Operating Officer

COTS
Commercial Off-the-Shelf

CPNI
Centre for the Protection of National Infrastructure

CPS
Cyber-Physical System

CPU
Central Processing Unit

CRISP
Cybersecurity Risk Information Sharing Program

CS3STHLM
Stockholm International Summit on Cyber Security in SCADA and ICS

CSET
Cyber Security Evaluation Tool

CSF
Cybersecurity Framework

CSO
Chief Security Officer

CSRC
Computer Security Resource Center

CSRIC
Communications Security, Reliability, and Interoperability Council

CVE
Common Vulnerabilities and Exposures

CyOTE
Cybersecurity for the Operational Technology Environment

CyTRICS
Cyber Testing for Resilient Industrial Control Systems

DCS
Distributed Control System

DES
Data Encryption Standard

DHCP
Dynamic Host Configuration Protocol

DHS
Department of Homeland Security

DICWG
Digital Instrumentation and Control Working Group

DLP
Data Loss Prevention

DMZ
Demilitarized Zone

DNP3
DNP3 Distributed Network Protocol (published as IEEE 1815)

DNS
Domain Name System

DOE
Department of Energy

DoS
Denial of Service

DOT
United States Department of Transportation

DRP
Disaster Recovery Plan

DSS
Digital Signature Standard

DVD
Digital Video Disc

E-ISAC
Electricity Information Sharing and Analysis Center

EM
Electromagnetic

EMBS
IEEE Engineering in Medicine and Biology Society

EMP
Electromagnetic Pulse

EMS
Energy Management System

EPA
United States Environmental Protection Agency

EPRI
Electric Power Research Institute

ERM
Enterprise Risk Management

ESD
Emergency Shutdown

FAA
Federal Aviation Administration

FCC
Federal Communications Commission

FDA
United States Food and Drug Administration

FEMA
Federal Emergency Management Agency

FGS
Fire and Gas System

FHWA
Federal Highway Administration

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

FMCSA
Federal Motor Carrier Safety Administration

FMEA
Failure Mode and Effects Analysis

FRA
Federal Railroad Administration

FTA
Federal Transit Administration

FTP
File Transfer Protocol

GCC
Government Coordinating Council

GCIP
GIAC Critical Infrastructure Protection

GIAC
Global Information Assurance Certification

GICSP
Global Industrial Cyber Security Professional

GPS
Global Positioning System

GRID
GIAC Response and Industrial Defense

HART
Highway Addressable Remote Transducer Protocol

HC3
Health Sector Cybersecurity Coordination Center

HHS
Health and Human Services

HMI
Human-Machine Interface

HR
Human Resources

HSIN
Homeland Security Information Network

HSIN-CI
Homeland Security Information Network - Critical Infrastructure

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol Secure

HVAC
Heating, Ventilation, and Air Conditioning

I/O
Input/Output

I3P
Institute for Information Infrastructure Protection

IAARC
International Association for Automation and Robotics in Construction

IACS
Industrial Automation and Control System

IAEA
International Atomic Energy Agency

ICCP
Inter-Control Center Communications Protocol

ICS
Industrial Control System

ICSJWG
Industrial Control Systems Joint Working Group

ICSS
Integrated Control and Safety Systems

ID
Identification

IDS
Intrusion Detection System

IEC
International Electrotechnical Commission

IED
Intelligent Electronic Device

IEEE
Institute of Electrical and Electronics Engineers

IES
IEEE Industrial Electronics Society

IETF
Internet Engineering Task Force

IFIP
International Federation for Information Processing

IIC
Industry IoT Consortium, Industrial Internet of Things Consortium

IIoT
Industrial Internet of Things

INL
Idaho National Laboratory

IoT
Internet of Things

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

IR
Incident Response

ISA
International Society of Automation

ISAC
International Sharing and Analysis Center

ISCM
Information Security Continuous Monitoring

ISO
International Organization for Standardization

IT
Information Technology

ITL
Information Technology Laboratory

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

LOGIIC
Linking the Oil and Gas Industry to Improve Cybersecurity

MAC
Media Access Control

MARAD
Maritime Administration

MBR
Master Boot Record

MCAA
Measurement, Control, & Automation Association

MFA
Multi-Factor Authentication

MIB
Management Information Base

ML
Machine Learning

MTU
Master Terminal Unit

NAM
National Association of Manufacturers

NAWC
National Association of Water Companies

NCC
National Coordinating Center for Communications

NEA
Nuclear Energy Agency

NEI
Nuclear Energy Institute

NERC
North American Electric Reliability Corporation

NESCOR
National Electric Sector Cybersecurity Resource

NFS
Network File System

NFU
National Farmers Union

NGFW
Next Generation Firewall

NHTSA
National Highway Traffic Safety Administration

NICE
National Initiative for Cybersecurity Education

NIH
National Institutes of Health

NIMS
National Incident Management System

NIST
National Institute of Standards and Technology

NIST IR
National Institute of Standards and Technology Internal or Interagency Report

NITAAC
National Institutes of Health Information Technology Acquisition and Assessment Center

NRC
United States Nuclear Regulatory Commission

NREL
National Renewable Energy Laboratory

NTP
Network Time Protocol

NTSB
National Transportation Safety Board

NVD
National Vulnerability Database

OEM
Original Equipment Manufacturer

OMB
Office of Management and Budget

OPC
Open Platform Communications

OS
Operating System

OSI
Open Systems Interconnection

OT
Operational Technology

PACS
Physical Access Control System, Picture Archiving and Communications Systems

PC
Personal Computer

PERA
Purdue Enterprise Reference Architecture

PES
IEEE Power & Energy Society

PHA
Process Hazard Analysis

PHM4SM
Prognostics and Health Management for Reliable Operations in Smart Manufacturing

PHMSA
Pipeline and Hazardous Materials Safety Administration

PID
Proportional-Integral-Derivative

PIN
Personal Identification Number

PIV
Personal Identity Verification

PLC
Programmable Logic Controller

PNNL
Pacific Northwest National Laboratory

PNT
Positioning, Navigation, and Timing

PPD
Presidential Policy Directive

PRAM
Privacy Risk Assessment Methodology

PSCCC
IEEE Power System Communications and Cybersecurity

PSS
Process Safety Shutdown

PT
Pressure Transmitter

PTP
Precision Time Protocol

R&D
Research and Development

RAS
IEEE Robotics and Automation Society

RBAC
Role-Based Access Control

RDP
Remote Desktop Protocol

RF
Radio Frequency

RFC
Request for Comments

RFID
Radio Frequency Identification

RMF
Risk Management Framework

RPC
Remote Procedure Call

RPO
Recovery Point Objective

RTO
Recovery Time Objective

RTOS
Real-Time Operating System

RTU
Remote Terminal Unit

S4
SCADA Security Scientific Symposium

SBOM
Software Bill of Materials

SBU
Sensitive But Unclassified

SC
Security Category

SCADA
Supervisory Control and Data Acquisition

SCAI
Safety, Controls, Alarms, and Interlocks

SCC
Sector Coordinating Council

SD
Secure Digital

SDLC
Software Development Life Cycle, System Development Life Cycle

SDN
Software-Defined Networking

SEPA
Smart Electric Power Alliance

SGCC
Smart Grid Cybersecurity Committee

SHA
Secure Hash Algorithm

SIEM
Security Information and Event Management

SIF
Safety Instrumented Function

SIS
Safety Instrumented System

SOC
Security Operations Center

SOCMA
Society of Chemical Manufacturers and Affiliates

SP
Special Publication

SPAN
Switched Port Analyzer

SQL
Structured Query Language

SSA
Sector-Specific Agency

SSCP
Secure SCADA Communications Protocol

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSPP
Substation Serial Protection Protocol

TC
Technical Committee

TCP
Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

TFTP
Trivial File Transfer Protocol

TIP
Technical Information Paper

TLS
Transport Layer Security

TLV
Type, Length, Value

TPM
Trusted Platform Module

TSA
Transportation Security Administration

TT
Temperature Transmitter

UDP
User Datagram Protocol

UPS
Uninterruptible Power Supply

U.S.
United States

USB
Universal Serial Bus

USDA
United States Department of Agriculture

VAV
Variable Air Volume

VDP
Vulnerability Disclosure Policy

VLAN
Virtual Local Area Network

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

VTS
IEEE Vehicular Technology Society

WAF
Web Application Firewall

WAN
Wide Area Network

WG
Working Group

Wi-Fi
Wireless Fidelity

WINS
World Institute of Nuclear Security

ZTA
Zero Trust Architecture

Appendix B. Glossary

Selected terms used in this publication are defined below. Source references are included for certain definitions.

access control list
A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources. [RFC4949] (adapted)

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.

alarm
A device or function that signals the existence of an abnormal condition by making an audible or visible discrete change, or both, so as to attract attention to that condition. [ANSI-ISA-5-1]

antivirus tools
Software products and technology used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system.

attack
An attempt to gain unauthorized access to system services, resources, or information or an attempt to compromise system integrity, availability, or confidentiality.

authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS200]

authorization
The right or a permission that is granted to a system entity to access a system resource. [RFC4949] (adapted)

backdoor
An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.

buffer overflow
A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. [SP800-28v2]

cleartext
Information that is not encrypted.

communications router
A communications device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [USC44-3552] (adapted)

configuration (of a system or device)
Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections.

configuration control
Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation. [CNSS4009] (adapted)

control
The part of the OT system used to monitor and control the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.

control algorithm
A mathematical representation of the control action to be performed. [ISADICT]

control center
An equipment structure or group of structures from which a process is measured, controlled, and/or monitored. [ANSI-ISA-51-1]

control loop
A control loop consists of sensors for measurement, controller hardware (e.g., PLCs), actuators (e.g., control valves, breakers, switches, and motors), and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.

control network
Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.

control server
A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as remote terminal units (RTUs) and programmable logic controllers (PLCs), over an OT network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.

control system
A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs, BAS, and other types of OT measurement and control systems.

controlled variable
The variable that the control system attempts to keep at the set point value. The set point may be constant or variable. [ISADICT]

controller
A device or program that operates automatically to regulate a controlled variable. [ANSI-ISA-51-1]

cycle time
The time, usually expressed in seconds, for a controller to complete one control loop where sensor signals are read into memory, control algorithms are executed, and corresponding control signals are transmitted to actuators that create changes to the process resulting in new sensor signals. [ISADICT]

data diode
A network appliance or device that allows data to travel only in one direction. Also referred to as a *unidirectional gateway*, deterministic one-way boundary device, or unidirectional network.

data historian
A centralized database that supports data analysis using statistical process control techniques.

database
A repository of information that usually holds plant-wide information including process data, recipes, personnel data, and financial data. [IR6859] (adapted)

demilitarized zone
An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. [SP800-41r1]

denial of service
The prevention of authorized access to a system resource or the delaying of system operations and functions. [RFC4949]

diagnostics
Information concerning known failure modes and their characteristics. Such information can be used in troubleshooting and failure analysis to help pinpoint the cause of a failure and help define suitable corrective measures. [ISADICT]

disaster recovery plan
A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [SP800-34r1] (adapted)

discrete process
A type of process where a specified quantity of material moves as a unit (part or group of parts) between work stations and each unit maintains its unique identity. [ISADICT]

distributed control system
In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit. [ISADICT]

disturbance
An undesired change in a variable being applied to a system that tends to adversely affect the value of a controlled variable. [ANSI-ISA-51-1]

domain
An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. [RFC4949] (adapted)

encryption
Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state. [RFC4949] (adapted)

enterprise
An organization that coordinates the operation of one or more processing sites.

fault tolerant
A system having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault.

field device
Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

field site
A subsystem that is identified by physical, geographical, or logical segmentation within the ICS. A field site may contain RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

fieldbus
A digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment, such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network, and each message identifies a particular sensor on the network.

File Transfer Protocol
An standard for transferring files over the internet. FTP programs and utilities are used to upload and download web pages, graphics, and other files between local media and a remote server that allows FTP access.

firewall
An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). [RFC4949]

human-machine interface
The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software. [IR6859]

identification
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. [SP800-47]

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. [FIPS200]

industrial control system
General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as programmable logic controllers (PLC). An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

information security program plan
Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. [OMB-A130]

input/output
A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications. [ISADICT]

insider
An entity inside the security perimeter that is authorized to access system resources but uses them in a way that is not approved by those who granted the authorization.

integrity
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [USC44-3552] (adapted)

intelligent electronic device
Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers). [AGA12]

internet
The single interconnected worldwide system of commercial, government, educational, and other computer networks that share the set of protocols specified by the Internet Architecture Board (IAB) and the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). [RFC4949] (adapted)

intrusion detection system
A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. [RFC4949] (adapted)

intrusion prevention system
A system that can detect an intrusive activity and also attempt to stop the activity, ideally before it reaches its targets.

jitter
The time or phase difference between the data signal and the ideal clock.

key logger
A program designed to record which keys are pressed on a computer keyboard in order to obtain passwords or encryption keys and thus bypass other security measures.

local area network
A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

machine controller
A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage. [IR6859]

maintenance
Any act that either prevents the failure or malfunction of equipment or restores its operating capability. [ISADICT]

malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. [SP800-53r5] (adapted)

manipulated variable
In a process that is intended to regulate some condition, a quantity or a condition that the control alters to initiate a change in the value of the regulated condition. [ISADICT]

master terminal unit
See *Control Server*.

modem
A device used to convert serial digital data from a transmitting terminal to a signal suitable for transmission over a telephone channel to reconvert the transmitted signal to serial digital data for the receiving terminal. [IR6859]

operating system
An integrated collection of service routines for supervising the sequencing of programs by a computer. An operating system may perform the functions of input/output control, resource scheduling, and data management. It provides application programs with the fundamental commands for controlling the computer. [ISADICT]

operational controls
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). [FIPS200]

operational technology
A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

password
A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS140-2]

phishing
Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites).

plant
The physical elements necessary to support the physical process. This can include many of the static components not controlled by the ICS. However, the operation of the ICS may impact the adequacy, strength, and durability of the plant's components.

port
The entry or exit point from a computer for connecting communications or peripheral devices.

port scanning
Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

predisposing condition
A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation. [SP800-30r1]

pressure regulator
A device used to control the pressure of a gas or liquid. [IR6859]

pressure sensor
A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium. Pressure sensors can also use differential pressure to obtain level and flow measurements. [IR6859] (adapted)

printer
A device that converts digital data to human-readable text on a paper medium. [IR6859] (adapted)

process controller
A type of computer system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs. [IR6859] (adapted)

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. [ISADICT]

protocol
A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [RFC4949]

protocol analyzer
A device or software application that enables the user to analyze the performance of network data so as to ensure that the network and its associated hardware/software are operating within network specifications. [ISADICT]

real time
Pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process.

redundant control server
A backup to the control server that maintains the current state of the control server at all times. [IR6859]

relay
An electromechanical device that completes or interrupts an electrical circuit by physically moving conductive contacts. The resultant motion can be coupled to another mechanism such as a valve or breaker. [ISADICT]

remote access
Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. [SP800-53r5]

remote diagnostics
Diagnostic activities conducted by individuals who are outside of an information system security perimeter.

remote maintenance
Maintenance activities conducted by individuals communicating through an external network. [SP800-53r5]

remote terminal unit
A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs. [IR6859]

risk
The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. [FIPS200] (adapted)

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. [SP800-39] (adapted)

risk management
The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. [FIPS200] (adapted)

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. [RFC4949] (adapted)

safety instrumented system
A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated. Other terms commonly used include emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS). [ANSI-ISA-84]

SCADA server
The device that acts as the master in a SCADA system.

security audit
Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. [ISO7498-1]

security controls
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS199]

security plan
Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [SP800-18r1]

security policy
Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.

sensor
A device that produces a voltage or current output that is representative of some physical property being measured (e.g., speed, temperature, flow). [ISADICT]

set point
An input variable that sets the desired value of the controlled variable. This variable may be manually set, automatically set, or programmed. [ISADICT]

single loop controller
A controller that controls a very small process or a critical process. [IR6859]

social engineering
An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. [SP800-61r2]

supervisory control
A term that is used to imply that the output of a controller or computer program is used as input to other controllers. See *Control Server*. [ISADICT]

supervisory control and data acquisition
A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. [ISADICT]

technical controls
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [FIPS200]

threat
Any circumstance or event with the potential to adversely impact agency operations (including safety, mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [FIPS200] (adapted)

threat event
An event or situation that has the potential for causing undesirable consequences or impact. [SP800-30r1]

threat source
The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. *Synonymous with threat agent.* [FIPS200]

Transmission Control Protocol
TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees the delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Trojan horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. [RFC4949]

unauthorized access
A person gains logical or physical access without permission to a network, system, application, data, or other resource. [SP800-61]

unidirectional gateway
Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information at all back to the source network. The software replicates databases and emulates protocol servers and devices.

valve
An in-line device in a fluid-flow system that can interrupt flow, regulate the rate of flow, or divert flow to another branch of the system. [ISADICT]

virtual private network
A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. [RFC4949] (adapted)

virus
A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. [RFC4949] (adapted)

vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [FIPS200]

wide area network
A physical or logical network that provides data communications to a larger number of independent users than are typically served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

wireless device
Any device that can connect to an OT network via radio or infrared waves, usually to collect or monitor data but also to modify control set points in some cases.

workstation
A computer used for tasks such as programming, engineering, and design. [IR6859]

worm
A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. [RFC4949] (adapted)

Appendix C. Threat Sources, Vulnerabilities, and Incidents

Several terms are used to describe the interrelated concepts of threat, threat source, threat event, and incident. A *threat* is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats have some intent or method that may exploit a vulnerability through either intentional or unintentional means. This intent or method is referred to as the *threat source*. A *vulnerability* is a weakness in an information system (including an OT), system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A *threat event* is an event or situation that has the potential to cause undesirable consequences or impacts. When a threat event occurs, it becomes an *incident* 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.

This appendix explores OT-specific threat sources, vulnerabilities, and incidents. It also cites examples of OT-specific incidents to illustrate their potential impacts. Each organization calculates risk based on the specific threats, vulnerabilities, impacts, and likelihood of incidents within their environment.

C.1. Threat Sources

Threats to OT can come from numerous sources that can be classified as adversarial, accidental, structural, or environmental. **Table 13** lists and defines known threat sources to OT. These threat sources should be considered part of the risk management strategy. The threat source must be well understood in order to define and implement adequate protection. For example, environmental events (e.g., floods, earthquakes) are well understood but may vary in their magnitude, frequency, and ability to compound other interconnected events. However, adversarial threats depend on the resources available to the adversary and the emergence of previously unknown vulnerabilities or attacks.

Table 13. Threats to OT

Type of Threat Source	Description	Characteristics
ADVERSARIAL - Bot network operators - Criminal groups - Hackers/hacktivists - Insiders - Nations - Terrorists	Individuals, groups, organizations, or nation-states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged user or administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities (e.g., operator accidentally typing 100 instead of 10 as a set point; engineer making a change in the production environment while thinking that they are in the development environment)	Range of effects

Type of Threat Source	Description	Characteristics
STRUCTURAL - Hardware failure • Processors, input/output cards, communications cards • Networking equipment • Power supply • Sensor, final element • HMI, displays - Software failure • OS • General-purpose applications • Mission-specific applications - Environmental controls failure • Temperature control • Humidity control - Communications degradation • Wireless • Wired	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters, including failures of critical infrastructures within the control of the organization	Range of effects
ENVIRONMENTAL - Natural or human-caused disaster • Fire • Flood/tsunami • Windstorm/tornado • Hurricane • Earthquake • Bombing • Animal interference • Solar flares, meteorites - Critical infrastructure failure • Telecommunications • Electrical power • Transportation • Water/wastewater	Natural disasters and failures of critical infrastructures on which the organization depends but that are outside of the control of the organization. Note: Natural and human-caused disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities that house mission-critical systems, making those systems unavailable for three weeks).	Range of effects

C.2. Vulnerabilities and Predisposing Conditions

Vulnerabilities are weaknesses in information systems, system procedures, controls, or implementations that can be exploited by a threat source. *Predisposing conditions* are properties of the organization, mission or business process, architecture, or information systems that contribute to the likelihood of a threat event. The order of these vulnerabilities and predisposing conditions does not reflect priority in terms of likelihood of occurrence or severity of impact. Additionally, the vulnerabilities and predisposing conditions identified in this section should not be considered a complete list, nor should they be assumed to occur in every OT environment.

Vulnerabilities and predisposing conditions are grouped according to where they exist, such as in the organization's policy and procedures, or the inadequacy of security mechanisms

implemented in hardware, firmware, and software. The former is referred to as being in the organization and the latter as being in the system. Understanding the source of vulnerabilities and predisposing conditions can help identify optimal mitigation strategies. Deeper analysis may uncover that causes and observations may not be one-to-one – that is, some underlying causes may exhibit multiple symptoms, and some symptoms may come from more than one cause.

Any given OT will usually exhibit a subset of the identified vulnerabilities in this appendix but may also contain additional vulnerabilities and predisposing conditions that are unique to a particular technology or implementation. Specific current information on OT vulnerabilities can be found on the CISA website, though many vendors publish notifications and patches that are not always found on the CISA website. It is beneficial to maintain relationships with vendors in order to stay up to date with known vulnerabilities.

Some vulnerabilities and predisposing conditions can be mitigated. Others can only be accepted and controlled by appropriate countermeasures but will result in some residual risk to the OT environment. For example, some existing policies and procedures may be changed with a level of effort that the organization considers acceptable, while others are more expeditiously dealt with by instituting additional policies and procedures.

Vulnerabilities in the products and services acquired from outside of the organization are rarely under the direct control of the organization. Changes may be influenced by market forces, but this is a slow and indirect approach. Instead, the organization may change predisposing conditions to reduce the likelihood that a systemic vulnerability will be exploited.

C.2.1. Policy and Procedure Vulnerabilities and Predisposing Conditions

Vulnerabilities and predisposing conditions are often introduced into the OT environment because of incomplete, inappropriate, or nonexistent security policy, including documentation, implementation guides (e.g., procedures), and enforcement. Management support of security policy and procedures is the cornerstone of any security program. Organization security policy can reduce vulnerabilities by mandating and enforcing proper conduct. Written policy and procedures are mechanisms for informing staff and stakeholders of decisions about behavior that is beneficial to the organization. From this perspective, policy is an educational and instructive way to reduce vulnerabilities. Enforcement is a partner to policy and encourages people to do the proper thing. Various forms of corrective action are the usual consequences to personnel not following policy and procedures. Policies should be explicit about the consequences to individuals or organizations that do not conform.

There is usually a complex policy and procedure environment that includes laws, regulations, overlapping jurisdictions and spheres of influence, economics, custom, and history. The larger enterprise is often subdivided into organizational units that should work together to reduce vulnerabilities. The scope and hierarchical relationship among policies and procedures needs to be managed for maximum effectiveness.

Table 14 presents examples of observed policy and procedure vulnerabilities and predisposing conditions for OT.

Table 14. Policy and procedure vulnerabilities and predisposing conditions

Vulnerability	Description
Inadequate organizational ownership of risk assessments	Risk assessments should be performed with acknowledgement from appropriate levels within the organization. The lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
Inadequate security policy for OT	Vulnerabilities are often introduced into the OT environment due to inadequate policies or the lack of policies specifically for OT system security. Controls and countermeasures should be derived from a risk assessment or policy to ensure uniformity and accountability.
Inadequate OT security training and awareness program	A documented formal OT security training and awareness program is designed to keep staff up to date on organizational security policies and procedures, threats, industry cybersecurity standards, and recommended practices. Without adequate ongoing training on specific OT policies and procedures, staff cannot be expected to maintain a secure OT environment.
Lack of inventory management policy	Inventory policy and procedures should include installation, removal, and changes made to hardware, firmware, and software. An incomplete inventory could lead to unmanaged and unprotected devices within the OT environment.
Lack of configuration management policy	Lack of policy and procedures for OT configuration management can lead to an unmanageable and highly vulnerable inventory of hardware, firmware, and software.
Inadequate OT equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an OT malfunction.
Lack of administrative mechanisms for security policy enforcement	Without accountability for enforcing policy, there is limited ability to ensure that security policies are followed adequately. Administrative mechanisms should be in place to ensure accountability.
Inadequate review of the effectiveness of the OT security controls	Procedures and schedules should exist to determine the extent to which the security program and its constituent controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the OT. The examination is sometimes called an “audit,” “evaluation,” or “assessment.” Policy should address the stage of the life cycle, purpose, technical expertise, methodology, and level of independence.
No OT-specific contingency plan	A contingency plan (e.g., business continuity plan, disaster recovery plan) should be prepared, tested, and available in the event of a major hardware or software failure or destruction of facilities. The lack of a specific plan for the OT could lead to extended downtimes and production losses.
Lack of adequate access control policy	Access control enforcement depends on policy that correctly models roles, responsibilities, and authorizations. The policy model must enable the way the organization functions.
Lack of adequate authentication policy	Authentication policies are needed to define when authentication mechanisms (e.g., passwords, smart cards) must be used, how strong they must be, and how they must be maintained. Without this policy, systems may not have appropriate authentication controls, making unauthorized access to systems more likely. Authentication policies should be developed as part of an overall OT security program, taking into account the capabilities of the OT and its personnel to handle more complex passwords and other mechanisms.

Vulnerability	Description
Inadequate incident detection and response plan and procedures	Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods for collecting, analyzing, and reporting data.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single-point-of-failure possibilities.

C.2.2. System Vulnerabilities and Predisposing Conditions

Security controls must clearly identify the systems to which they apply. Systems range widely in size, scope, and capability. At the small end of the spectrum, a system may be an individual hardware or software product or service. At the other end of the spectrum are large and complex systems, systems-of-systems, and networks, all of which incorporate hardware architectures and software frameworks (including application frameworks) to support operations. An organization may choose to identify security zones such that security controls may be applied to all systems within the security zone.

System vulnerabilities can occur in the hardware, firmware, and software used to build the OT. Sources of vulnerabilities include design flaws, development flaws, misconfigurations, poor maintenance, poor administration, and connections with other systems and networks. Many of the controls in the NIST SP 800-53 and the OT overlay in Appendix F specify what the system must do to mitigate these vulnerabilities.

Vulnerabilities can also exist in the auxiliary components that support the OT systems. A subset of those vulnerabilities with the potential to impact the physical process are described in this section.

The potential vulnerabilities and predisposing conditions commonly found within OT systems are categorized into the following tables:

- **Table 15.** Architecture and design vulnerabilities and predisposing conditions
- **Table 16.** Configuration and maintenance vulnerabilities and predisposing conditions
- **Table 17.** Physical vulnerabilities and predisposing conditions
- **Table 18.** Software development vulnerabilities and predisposing conditions
- **Table 19.** Communication and network configuration vulnerabilities and predisposing conditions
- **Table 20.** Sensor, final element, and asset management vulnerabilities and predisposing conditions

Table 15. Architecture and design vulnerabilities and predisposing conditions

Vulnerability	Description
Inadequate incorporation of security into architecture and design	Incorporating security into the OT architecture and design must start with a budget and schedule designated for OT. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
Inadequate management of change that allows insecure architecture to evolve	The network infrastructure within the OT environment has often been developed and modified based on business and operational requirements with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within the infrastructure. Without remediation, these gaps may represent backdoors into the OT. Sensors and controllers that were historically simple devices are now often manufactured as intelligent devices. In some cases, sensors and controllers may be replaced with IIoT devices that allow direct internet connections. Security should be incorporated into change management for all OT devices, not just traditional IT components.
No security perimeter defined	If the OT does not have a security perimeter clearly defined, it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability. Having both types of traffic on a single network creates challenges for meeting the requirements of control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in OT functions.
Control network services dependent on a non-control network	When IT services such as a Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network. This causes the OT network to become dependent on the IT network, which may not have the reliability and availability requirements needed by OT.
Inadequate collection of event data history	Forensic analysis depends on the collection and retention of sufficient data. Without proper and accurate data collection, it may be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures. Event data for an OT environment could include physical process data, system use data, and network data.

Table 16. Configuration and maintenance vulnerabilities and predisposing conditions

Vulnerability	Description
Hardware, firmware, and software that are not under asset management	The organization does not know what it has (e.g., make, model), where they are, or what version it is, resulting in an inconsistent and ineffective defense posture. To properly secure an OT, there should be an accurate inventory of the assets in the environment. Procedures should be in place to manage additions, deletions, and modifications of assets, which include asset inventory management. These procedures are critical to executing business continuity and disaster recovery plans.

Vulnerability	Description
Hardware, firmware, and software are not under configuration management	The organization does not know the patch management status, security settings, or configuration versions that it has, resulting in an inconsistent and ineffective defense posture. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure that an OT is protected against inadequate or improper modifications before, during, and after system implementation. To properly secure an OT, there should be an accurate listing or repository of the current configurations.
OS and vendor software patches may not be developed until long after security vulnerabilities are found	Because of the tight coupling between OT software and the underlying OT, changes must undergo expensive and time-consuming comprehensive regression testing. The elapsed time for such testing and the subsequent distribution of updated software provides a long window of vulnerability. Vulnerability management procedures should include flexibility for interim alternative mitigations.
Vendor declines to develop patches for vulnerability	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Security patch support may not be available for legacy OT, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where patches may never be available or replacement plans.
Lack of a vulnerability management program	Vulnerabilities not considered by the organization could result in exploitation. Vulnerability management procedures should be in place to determine a plan of action or inaction upon the discovery of a vulnerability. Some OT considerations are: availability concerns may push patching until the next planned operational downtime; security patch support may not be available for OT systems that use outdated OSs; isolated systems may not require immediate patching; and OT exposed to the internet may need to be prioritized for patching.
Inadequate testing of security changes	Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the OT. Documented procedures should be developed for testing all changes for security impacts. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
Poor remote access controls	There are many reasons why an OT may need to be remotely accessed, including vendors and system integrators performing system maintenance functions or OT engineers accessing geographically remote system components. The concept of least privilege should be applied to remote access controls. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access or authorized individuals from gaining excessive access to the OT.
Poor configurations are used	Improperly configured systems may leave unnecessary ports and protocols open. These unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.
Critical configurations are not stored or backed up	Procedures should be available for restoring OT configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent the loss of data. Documented procedures should be developed for maintaining configuration settings.
Data unprotected on portable device	System security could be compromised if sensitive data (e.g., passwords, dial-up numbers) is stored in cleartext on lost or stolen portable devices, such as laptops and mobile devices. Policy, procedures, and mechanisms are required for protection.

Vulnerability	Description
Vendor default passwords are used	Most vendor default passwords are easy to discover within vendor product manuals, which are also available to adversaries. Using the default password can drastically increase OT vulnerability.
Password generation, use, and protection do not comply with policy	Password policy and procedures must be followed to be effective. Violations of password policy and procedures can increase OT vulnerability.
Inadequate access controls applied	Access controls must match how the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in an OT user having too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System configured improperly results in an operator being unable to take corrective actions in an emergency situation
Improper data linking	OT data storage systems may be linked to non-OT data sources. An example of this is database links, which allow data from one database (e.g., data historian) to be automatically replicated on others. Data linkage may create a vulnerability if it is not properly configured and may allow unauthorized data access or manipulation.
Malware protection is not installed or up to date	The installation of malware (i.e., malicious software) is a common attack. Malware protection software, such as antivirus software, should be kept current in a dynamic environment. Outdated malware protection software and definitions leave the system open to malware threats.
Malware protection implemented without sufficient testing	Malware protection software that is deployed without sufficient testing could impact normal operation of the OT and block the system from performing necessary control actions.
Denial of service (DoS)	OT software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.
Intrusion detection and prevention software is not installed	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to ensure that it does not compromise normal operation of the OT.
Logs are not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur and perform adequate forensics.

Table 17. Physical vulnerabilities and predisposing conditions

Vulnerability	Description
Unauthorized personnel have physical access to equipment	Physical access to OT equipment should be restricted to only the necessary personnel while taking safety requirements into account, such as emergency shutdown or restarts. Improper access to OT equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage to or destruction of data and hardware • Modification of the operational process • Unauthorized changes to the functional environment (e.g., data connections, unauthorized use of removable media, adding/removing resources) • Disconnection of physical data links • Undetectable interception of data (e.g., keystroke and other input logging)
Radio frequency, electromagnetic pulse (EMP), static discharge, brownouts, and voltage spikes	Some hardware used for OT systems is vulnerable to radio frequency, electromagnetic pulses (EMP), static discharge, brownouts, and voltage spikes. The impacts can range from the temporary disruption of command and control to permanent damage to circuit boards. Proper shielding, grounding, power conditioning, and/or surge suppression is recommended.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the OT and could create an unsafe situation. Loss of power could also lead to insecure default settings. If the program file or data is stored in volatile memory, the process may not be able to restart after a power outage without appropriate backup power.
Loss of environmental control	The loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, such as processors overheating. Some processors will shut down to protect themselves. Others may continue to operate in a minimal capacity and produce intermittent errors, continually reboot, or become permanently inoperable.
Unsecured physical ports	Unsecured universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives or keystroke loggers.

Table 18. Software development vulnerabilities and predisposing conditions

Vulnerability	Description
Improper data validation	OT software may not properly validate user inputs or received data to ensure validity. Invalid data may result in numerous vulnerabilities, including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities are not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.

Table 19. Communication and network configuration vulnerabilities and predisposing conditions

Vulnerability	Description
Data flow controls are not employed	Data flow controls based on data characteristics are needed to restrict the information that is permitted between systems. These controls can prevent the exfiltration of information and illegal operations.
Firewalls are nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, thus allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping, and providing individuals with unauthorized access to systems.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
Standard, well-documented communication protocols are used in plaintext	Adversaries that can monitor the OT network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols, such as telnet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Network File System (NFS). The use of such protocols also makes it easier for adversaries to perform attacks against the OT and manipulate OT network activity.
Authentication of users, data, or devices is substandard or nonexistent	Many OT protocols have no authentication at any level. Without authentication, there is the potential to replay, modify, or spoof data or devices, such as sensors and user identities.
Use of unsecure OT protocols	OT protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. The incorrect implementation of the protocols can also lead to additional vulnerabilities.
Lack of integrity checking for communications	Integrity checks are not built into most OT protocols, so adversaries could manipulate communications undetected. To ensure integrity, the OT can use lower-layer protocols (e.g., IPsec) that offer data integrity protection when traversing untrusted physical media.
Inadequate authentication between wireless clients and access points	Strong mutual authentication between wireless clients and access points is needed to ensure that legitimate OT clients do not connect to a rogue access point deployed by an adversary and that adversary clients do not connect to any of the OT wireless networks.
Inadequate data protection between wireless clients and access points	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.

Table 20. Sensor, final element, and asset management vulnerabilities and predisposing conditions

Vulnerability	Description
Unauthorized physical access to sensors or final elements	Physical access to sensors and final elements allows for direct manipulation of the physical process. Many devices are configured on a fieldbus such that physical access to the sensor network allows for manipulation of controlling parameters. Physical access to the whole of the loop should be managed to prevent incidents.
Unauthorized wireless access to sensors or final elements	Wireless access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices allow for wireless configuration (e.g., Bluetooth, Wi-Fi, WirelessHART). Wireless access should be securely configured or disabled using hardware write-protect where possible to prevent unauthorized modification of the sensors and final elements that are connected to both the physical process and the OT environment.
Inappropriate segmentation of the asset management system	Most architectures are designed for PLCs, RTUs, DCS, and SCADA controllers to manipulate the process and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

C.3. Threat Events and Incidents

A threat event is an event or situation that could potentially cause an undesirable consequence or impact to operations resulting from some threat source. NIST SP 800-30, Rev. 1 [SP800-30r1] Appendix E identifies a broad set of threat events that could potentially impact information systems. The properties of OT may also present unique threat events, such as how the threat events can manipulate OT processes to cause physical damage. **Table 21** provides an overview of potential OT threat events and leverages MITRE's ATT&CK® for Industrial Control Systems [ATTACK-ICS].

Table 21. Examples of potential threat events

Threat Event	Description
Denial of control	Temporarily prevents operators and engineers from interfacing with process controls. An affected process may still be operating during the period of control loss but not necessarily in a desired state.
Manipulation of control	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment. These changes could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (e.g., prematurely shutting down transmission lines), an environmental incident, or even disabled control equipment.
Spoofed reporting message	False information sent to an OT system operator, either for evasion or to impair process control. The adversary could make the defenders and operators think that other errors are occurring in order to distract them from the actual source of the problem (i.e., alarm floods).
Theft of operational information	Adversaries may steal operational information for personal gain or to inform future operations.

Threat Event	Description
Loss of safety	Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow future unsafe conditionals to go unchecked.
Loss of availability	Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.

Numerous OT incidents have been reported and documented. Descriptions of these events help demonstrate the severity of the threat sources, vulnerabilities, and impacts within the OT domain. As mentioned in Appendix C.2, the four broad categories of threat sources are adversarial, accidental, structural, and environmental. Often, the incident can be the result of multiple threat sources (e.g., an environmental event causes a system failure, which is responded to incorrectly by an operator and results in an accidental event).

Below is a limited selection of reported incidents that fall into each of the four categories. The incidents have been additionally categorized into malicious or non-malicious and direct or indirect to further distinguish the possible causes of OT incidents.

M = Malicious. The event was initiated by someone for a harmful purpose. The initiator may or may not have been targeting the OT or known the potential consequences.

N = Non-malicious. There does not appear to be evidence that the initiating event was intended to cause an incident.

D = Direct. The event was designed to discover, inhibit, impair, or otherwise impact the OT system.

I = Indirect. The event was not believed to be designed to discover, inhibit, impair, or otherwise impact the OT system. The OT system shut down or caused disruption as a result of impact to the supporting infrastructure.

C.3.1. Adversarial Events

- **[M][D] Marconi wireless hack.**[9] In 1903, Italian radio pioneer Guglielmo Marconi was preparing for his first public demonstration of long-distance secure wireless communications from Cornwall to Professor Fleming at the Royal Institution of London. Inventor and magician Nevil Maskelyne hacked the system and sent a comical message in Morse code referencing "rats." Maskelyne then published an explanation of his hack in the trade journal *The Electrician*.
- **[M][I] Worcester air traffic communications.**[10] In March 1997, a teenager in Worcester, Massachusetts, disabled part of the public switched telephone network using a dial-up modem connected to the system. This disabled phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. The tower's main radio transmitter and another transmitter that activated runway lights were also shut down, as well as a printer that controllers used to monitor flight

[9] Additional information on the Marconi wireless hack incident can be found at https://www.osti.gov/biblio/1505628.
[10] Additional information on the Worcester air traffic communications incident can be found at http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html

progress. The attack also disabled phone service to 600 homes and businesses in the nearby town of Rutland.

- **[M][D] Maroochy Shire sewage spill.**[11] In the spring of 2000, a former employee of an Australian organization that developed manufacturing software applied for a job with the local government but was rejected. Over a two-month period, the disgruntled employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.
- **[M][I] Night Dragon.**[12] McAfee reported a series of attacks that were designed to steal sensitive data from global oil, energy, and petrochemical industries. Adversaries exfiltrated proprietary operations data and project financing information with regard to oil and gas field bids and operations.
- **[M][D] Iranian centrifuge, Stuxnet.**[13] Stuxnet was a Microsoft Windows computer worm discovered in July 2010 that specifically targeted industrial software and equipment. The worm initially spread indiscriminately but included a highly specialized malware payload that was designed to only target particular SCADA systems that were configured to control and monitor specific industrial processes.
- **[M][D] German steel mill attack.**[14] In 2014, hackers manipulated and disrupted control systems to such a degree that a blast furnace could not be properly shut down, resulting in unspecified "massive" damage.
- **[M][I] Shamoon.**[15] In 2012, Saudi Aramco experienced a malware attack that targeted their refineries and overwrote the attacked systems' master boot records (MBRs), partition tables, and other data files. This caused the systems to become unusable.
- **[M][D] New York dam.**[16] In 2013, an Iranian computer security company obtained remote access to a computer that controlled the SCADA system for the Bowman Dam located in Rye, New York. The adversary was able to view water levels, temperature, and the status of the sluice gate. The sluice gate control was disconnected for maintenance at the time of adversarial remote access, so the dam could not be remotely controlled.
- **[M][D] Dragonfly campaign, Havex.**[17] The energy sector was targeted during a multi-year cyber-espionage campaign that primarily used Havex malware. Havex was a remote access Trojan that used the Open Platform Communications (OPC) standard to gather information about connected ICS devices on a network. The campaigns were exploratory.

[11] Additional information on the Maroochy Shire sewage spill incident can be found at http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.
[12] Additional information on Night Dragon was published as a McAfee white paper at https://www.heartland.org/_template-assets/documents/publications/29423.pdf.
[13] Additional information on the Stuxnet worm can be found at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[14] Additional information on the German steel mill incident can be found at http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[15] Additional information on Shamoon can be found at https://www.cisa.gov/uscert/ics/monitors/ICS-MM201209.
[16] The U.S. Department of Justice indictment for the New York dam attacks can be found at https://www.justice.gov/opa/file/834996/download.
[17] Additional information on the Dragonfly/Energetic Bear Campaign can be found at https://www.osti.gov/servlets/purl/1505628.

- **[M][D] Ukrainian power grid, BlackEnergy3.**[18] On December 23, 2015, Ukrainian power companies experienced a cyberattack that caused power outages and impacted over 225,000 customers in Ukraine. Over 50 regional substations experienced malicious remote operation of their breakers. KillDisk malware was used to erase files on targeted systems, including at least one Windows-based HMI. The actors also corrupted the firmware of serial-to-Ethernet devices at the substations. This was the first known cyber attack on a power grid.
- **[M][D] Ukrainian power grid, Industroyer.**[19] On December 17, 2016, a cyber attack occurred at a substation outside of Kyiv, Ukraine, and resulted in an outage for customers of one substation for approximately one hour. This attack was the first known malware specifically designed to attack the power grid.
- **[M][I] Maersk, NotPetya.** In 2017, the NotPetya malware encrypted computers globally with no method for decryption. Although the malware initially targeted Ukrainian companies, it spread throughout the world with significant impacts to Maersk, FedEx, Merck, and Saint-Gobain. The malware destroyed data and disrupted shipping operations for Maersk, costing the company over $300 million in repairs and recovery efforts.
- **[M][D] Saudi Petrochem, TRITON.**[20] A petrochemical facility in Saudi Arabia was attacked using malicious software that targeted the industrial SIS. The SIS initiated a safe shutdown of the petrochemical process in 2017 when the triple-redundant processors identified mismatched code amongst the processors.
- **[M][I] Norsk Hydro, LockerGoga.**[21] In March 2019, Norsk Hydro experienced a cyberattack that used LockerGoga ransomware to encrypt its computer files. The aluminum and renewable energy company transitioned to manual operations and was transparent with the public on its progress to recovery. Norsk Hydro's transparency throughout the discovery and recovery process is well regarded by the security industry.
- **[M][I] Colonial Pipeline.**[22] In May 2021, over 5,500 miles of pipeline transporting more than 100 million gallons per day of refined products to the East Coast of the U.S. shutdown operations because of a ransomware attack. Colonial Pipeline was a victim of a ransomware cyber attack that encrypted their IT systems by exploiting a legacy VPN profile. The investigation is ongoing, but at the time of this writing, there is no evidence that the ransomware had any direct impact on the OT environment. Colonial made the decision to shut down the physical operations on the pipeline to contain any potential damage. Colonial Pipeline also decided to pay the ransom to cybercriminal group Darkside in order to have all possible tools, including the decryption tools, available to

[18] Additional information about the first Ukrainian power grid attack can be found at https://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.
[19] Additional information on Industroyer malware can be found at https://us-cert.cisa.gov/ncas/alerts/TA17-163A.
[20] Additional information on the TRITON attack can be found at https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections.
[21] Additional information on Norsk Hydro attack can be found at https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/, https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880, and https://www.darkreading.com/application-security/ransomware/norsk-hydro-this-is-how-you-react-to-a-ransomware-breach/a/d-id/750396.
[22] Additional information on the Colonial Pipeline incident can be found at https://www.c-span.org/video/?512247-1/senate-homeland-security-hearing-colonial-pipeline-cyber-attack and https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf.

bring the pipeline system back online. The U.S. Government was able to recover some of the ransom payment.[23]

- **[M][I] Ransomware targeting healthcare.**[24] A string of malware delivered via phishing attacks targeted the healthcare and public health sectors to disrupt services and steal data. In fall 2020, a CISA Alert (AA20-302A) was issued to warn healthcare and public health sector companies of the prevalence of these attacks.

C.3.2. Structural Events

- **[N][D] Bellingham, Washington, gasoline pipeline failure.**[25] In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline and ignited 1.5 hours later, causing three deaths, eight injuries, and extensive property damage. The pipeline failure was exacerbated by control systems that were unable to perform control and monitoring functions. Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation. A key recommendation from the NTSB report issued in October 2002 was to utilize an offline development and testing system for implementing and testing changes to the SCADA database.
- **[M][I] CSX train signaling system.**[26] In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the East Coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida, headquarters and shut down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, 10 Amtrak trains were affected in the morning. Trains between Pittsburgh, PA, and Florence, South Carolina, were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia, to Washington and New York was delayed for more than two hours. Long-distance trains were also delayed between four and six hours.
- **[N][D] Browns Ferry-3 PLC failure.**[27] In August 2006, TVA was forced to manually shut down one of their plant's two reactors after unresponsive PLCs problems caused two water pumps to fail and threatened the stability of the plant itself. Although there were dual redundant PLCs, they were connected to the same Ethernet network. Later testing on the failed devices discovered that they would crash when they encountered excessive network traffic.

[23] Additional information can be found at https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
[24] Additional information on the series of malware targeting healthcare can be found at Ransomware Activity Targeting the Healthcare and Public Health Sector | CISA.
[25] Additional information on the Bellingham, Washington, gasoline pipeline failure incident can be found at http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.
[26] Additional information on the CSX train signaling system incident can be found at http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807.
[27] Additional information on the Browns Ferry -3 PLC failure incident can be found at http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf.

C.3.3. Environmental Events

- **[N][I] Fukushima Daiichi nuclear disaster.**[28] The Great East Japan Earthquake on March 11, 2011, struck off the coast of Japan and sent a massive tsunami inland toward the nuclear plant. The tsunami compromised the plant's seawall, flooding much of the plant, including the location housing the emergency generators. This emergency power was critical for operating the control rooms and providing coolant water for the reactors. The loss of coolant caused the reactor cores to overheat to the point where the fuel's zirconium cladding reacted with water, releasing hydrogen gas and fueling large explosions in three of the four reactor buildings. This resulted in large-scale radiation leakage that has impacted plant employees, nearby citizens, and the local environment. Post-event analysis found that the plant's emergency response center had insufficient secure communication lines to provide other areas of the plant with information on key safety-related instrumentation.

C.3.4. Accidental Events

- **[N][D] Vulnerability scanner incidents.**[29] While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. In a separate incident, a ping sweep was being performed on an ICS network to identify the hosts that were attached to the network for inventory purposes, and it caused a system that controlled the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers.
- **[N][D] Penetration testing incident.**[30] A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system, and the utility was not able to send gas through its pipelines for four hours.
- **[N][I] NERC Enforcement Action.**[31] In 2019, a U.S. energy company was fined $10 million by NERC for cybersecurity violations that took place between 2015 and 2018. The inability to comply with U.S. standards for cybersecurity was seen as a risk to the security and reliability of the overall power system.
- **[N][D] NASA fire.**[32] A security patch was applied to an OT component that controlled a large engineering oven. The patch and associated reboot caused the oven to stop running, which led to a fire that destroyed the spacecraft hardware. The reboot also impeded alarm activation, which allowed the fire to go undetected for 3.5 hours before discovery.

[28] Additional information can be found at http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf and http://pbadupws.nrc.gov/docs/ML1414/ML14140A185.pdf.
[29] Additional information on the vulnerability scanner incidents can be found at https://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf.
[30] Additional information on penetration testing incidents can be found at https://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf.
[31] For additional information about fines imposed on energy companies, see Enforcement Actions 2019 (nerc.com).
[32] For additional information on accidental OT losses from applying IT security controls in NASA, see Final Report - IG-17-011 (nasa.gov).

- **[N][D] Hatch Nuclear Power Plant.**[33] In 2008, the Hatch nuclear power plant in Georgia was forced into an emergency shutdown for forty-eight hours after a software update was installed on a single Windows computer. When the updated computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown.

[33] Additional information can be found at https://www.homelandsecuritynewswire.com/cyber-mishap-causes-nuclear-power-plant-shutdown