Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date September 28, 2023

Original Release Date April 26, 2022

The attached draft document is followed by:

Status	Final
Series/Number	NIST SP 800-82r3
Title	Guide to Operational Technology (OT) Security
Publication Date	September 2023
DOI	https://doi.org/10.6028/NIST.SP.800-82r3
CSRC URL	https://csrc.nist.gov/pubs/sp/800/82/r3/final
Additional Information	

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-82r3 ipd

Guide to Operational Technology (OT) Security

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Victoria Pillitteri
Suzanne Lightman

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3.ipd

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

NIST Special Publication
NIST SP 800-82r3 ipd

Guide to Operational Technology (OT) Security

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Smart Connected Systems Division
Communications Technology Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3.ipd

April 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-82r3
Natl. Inst. Stand. Technol. Spec. Publ. 800-82r3, 317 pages (April 2022)
Initial Public Draft
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3.ipd

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

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

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

Public comment period: April 26, 2022 – July 1, 2022

Submit comments on this publication to: sp800-82rev3@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document provides guidance on how to secure operational technology (OT), while addressing their unique performance, reliability, and safety requirements. OT 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 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. The document provides an overview of OT and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Keywords

Computer security; distributed control systems (DCS); industrial control systems (ICS); information security; network security; operational technology (OT); programmable logic controllers (PLC); risk management; security controls; supervisory control and data acquisition (SCADA) systems

Acknowledgments for DRAFT Revision 3

The authors gratefully acknowledge and appreciate the significant contributions from Sallie Edwards, Blaine Jefferies, Adam Hahn, John Hoyt, Stephanie Saravia, Aslam Sherule, and Michael Thompson from The MITRE Corporation, and Megan Corso and Brett Ramsay from the Department of Defense. The authors wish to thank their colleagues who reviewed drafts of the document and contributed to its content, including Eran Salfati, Karen Scarfone and Isabel Van Wyk.

Acknowledgments for Previous Versions

The authors wish to thank their colleagues who reviewed drafts of the original version of the document and contributed to its technical content. The authors would particularly like to acknowledge Tim Grance, Ron Ross, Stu Katzke, and Freemon Johnson of NIST for their keen and insightful assistance throughout the development of the document. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of the publication. The authors would particularly like to thank the members of ISA99. A special acknowledgement to Lisa Kaiser, Department of Homeland Security, the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG), and Office of the Deputy Undersecretary of Defense for Installations and Environment, Business Enterprise Integration Directorate staff, Daryl Haegley and Michael Chipley, for their exceptional contributions to this publication. The authors would also like to thank the UK National Centre for the Protection of National Infrastructure (CPNI) for allowing portions of the *Good Practice Guide on Firewall Deployment for SCADA and Process Control Network* to be used in the document as well as ISA for allowing portions of the ISA-62443 Standards to be used in the document.

Note to Readers

This document is the third revision to NIST SP 800-82. Updates in this revision include:

- Expansion in scope from industrial control systems to operational technology (OT).
- Updates to OT threats and vulnerabilities.
- Updates to OT risk management, recommended practices, and architectures.
- Updates to current activities in OT security.
- Updates to security capabilities and tools for OT.
- Additional alignment with other OT security standards and guidelines, including the Cybersecurity Framework.
- New tailoring guidance for NIST SP 800-53 Revision 5 security controls
- An OT overlay for NIST SP 800-53 Revision 5 security controls that provides tailored security control baselines for low-, moderate-, and high-impact OT systems.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sp800-82rev3@nist.gov

Table of Contents

List of Appendices

List of Figures

List of Tables

Executive Summary

This document provides guidance for establishing secure operational technology (OT)[1] while addressing OT's unique performance, reliability, and safety requirements. OT 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 monitoring and/or control of devices, processes, and events. Examples include industrial control systems (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. The document provides an overview of OT and typical system topologies, identifies typical threats and vulnerabilities for these systems, and recommends security countermeasures to mitigate the associated risks.

OT is critical to the operation of U.S. critical infrastructures, which are often highly interconnected, mutually dependent systems. It is important to note that while federal agencies operate many of the nation's critical infrastructures, 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 as well as interconnections between business partners.

Initially, OT had little resemblance to traditional information technology (IT) systems in that OT systems were isolated, ran proprietary control protocols, and used specialized hardware and software. As OT are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and being designed and implemented using industry-standard computers, operating systems (OSs), and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for OT from the outside world than predecessor systems, creating a greater need to secure OT systems. The increasing use of wireless networking places OT implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. 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.

Although some characteristics are similar, OT also have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that logic executing in OT has a direct effect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information. OT have unique performance and reliability requirements and often use OSs and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of OT systems.

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

OT cybersecurity programs should always be part of broader OT safety and reliability programs at both industrial sites and enterprise cybersecurity programs, because cybersecurity is essential to the safe and reliable operation of modern industrial processes. Threats to OT systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious actions by insiders. OT security objectives typically follow the priority of integrity and availability, followed by confidentiality.

Possible incidents an OT system may face include the following:

- Blocked or delayed flow of information through OT networks, which could disrupt OT operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause operators to initiate inappropriate actions, which could have various negative effects.
- Modified OT software or configuration settings, or OT software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life.

Major security objectives for an OT implementation should include the following:

- **Restrict logical access to the OT network, network activity, and systems.** This may include using unidirectional gateways, utilizing a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and OT networks, and having separate authentication mechanisms and credentials for users of the corporate and OT networks. The OT system should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restrict physical access to the OT network and devices.** Unauthorized physical access to components could cause serious disruption of the OT's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
- **Protect individual OT components from exploitation.** This includes deploying security patches in as expeditious a manner as possible after testing them under field conditions; disabling all unused ports and services and assuring that they remain disabled; restricting OT user privileges to only those that are required for each user's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware. Keys of OT assets like programmable logic controllers (PLCs) and safety systems should be in the "Run" position at all times unless they are being actively programmed.

- **Restrict unauthorized modification of data.** This includes data that is in transit (at least across network boundaries) and at rest.
- **Detect security events and incidents.** Detecting security events, which have not yet escalated into incidents, can help defenders break the attack chain before attackers attain their objectives. This includes the capability to detect failed OT components, unavailable services, and exhausted resources that are important to provide proper and safe functioning of the OT system.
- **Maintain functionality during adverse conditions.** This involves designing the OT system so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the OT or other networks, nor causes another problem elsewhere, such as a cascading event. The OT system should also allow for graceful degradation such as moving from "normal operation" with full automation to "emergency operation" with operators more involved and less automation to "manual operation" with no automation.
- **Restore the system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly the system can be recovered after an incident has occurred.

To properly address security in an OT system, it is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experience to evaluate and mitigate risk to the OT system. The cybersecurity team should consist of a member of the organization's IT staff, control engineer, control system operator, network and system security expert, a member of the management staff, and a member of the physical security department at a minimum. For continuity and completeness, the cybersecurity team should consult with the control system vendor and/or system integrator as well. The cybersecurity team should coordinate closely with site management (e.g., facility superintendent) and the company's Chief Information Officer (CIO) or Chief Security Officer (CSO), who in turn, along with the Chief Executive Officer (CEO) or Chief Operating Officer (COO), accepts complete responsibility and accountability for the cybersecurity of the OT system and for any safety incidents, reliability incidents, or equipment damage caused directly or indirectly by cyber incidents. An effective cybersecurity program for an OT system should apply a strategy known as "defense-in-depth," layering security mechanisms such that the impact of a failure in any one mechanism is minimized. Organizations should not rely on "security by obscurity."

In a typical OT system this means a defense-in-depth strategy that includes:

- Developing security policies, procedures, training and educational material that apply specifically to the OT system.
- Considering OT security policies and procedures based on the National Terrorism Advisory System, deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the life cycle of the OT system, including architecture design, procurement, installation, maintenance, and decommissioning.

- Implementing a network topology for the OT system that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and OT networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).
- Employing a DMZ network architecture (e.g., prevent direct traffic between the corporate and OT networks).
- Ensuring that critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Disabling unused ports and services on OT devices after assuring through testing that it will not impact OT operation.
- Restricting physical access to the OT network and devices.
- Restricting OT user privileges to only those that are required to perform each user's function (e.g., establishing role-based access control, configuring each role based on the principle of least privilege).
- Using separate authentication mechanisms and credentials for users of the OT network and the corporate network (i.e., OT network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for user authentication
- Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the OT system.
- Applying security techniques such as encryption and/or cryptographic hashes to OT data storage and communications where determined appropriate.
- Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the OT system.
- Tracking and monitoring audit trails on critical areas of the OT system.
- Employing reliable and secure network protocols and services where feasible.

NIST, in cooperation with the public and private sector OT community, has developed specific guidance on the application of the security controls in NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations* [SP800-53r5], to OT. This guidance is included in Appendix F of this document.

While many of the controls in Appendix F of SP 800-53 Rev. 5 are applicable to OT as written, some controls require OT-specific interpretation and/or augmentation by adding one or more of the following to the control:

- **OT Discussion** provides organizations with additional information on the application of the security controls and control enhancements in Appendix F to OT and the environments in which these specialized systems operate. The guidance also provides information as to why a particular security control or control enhancement may not be applicable in some OT environments or may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). OT Discussion does not replace the original Supplemental Guidance in Appendix F.
- **Control Enhancements** (one or more) provide augmentations to the original control that may be required for some OT systems.

The most successful method for securing OT systems is to gather industry recommended practices and engage in a proactive, collaborative effort between management, the OT engineers and operators, the IT organization, and a trusted OT advisor. This team should draw upon the wealth of information available from ongoing federal government, industry groups, and vendor and standards activities listed in Appendix D.

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. The document gives an overview of OT systems and typical system topologies, identifies typical 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 specific to OT systems. Readers of this document should be acquainted with general computer security concepts and with 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 risk for 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

[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.

- Vendors that are developing products that will be deployed as part of an OT system

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.

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

- Appendix A lists acronyms and abbreviations used in this document.
- Appendix B contains a glossary of 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 an SP 800-53, Revision 5 OT overlay, listing 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 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 has an effect on the input in such a way as to maintain the desired control objective
- *manual mode*: the system is controlled completely 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 (BAS), physical access control systems (PACS), and the Industrial Internet of Things (IIoT). Diagrams depict the typical network topology, connections, components, and protocols 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, resulting 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 of OT continues to evolve to provide new capabilities while maintaining the typical long life cycles of these systems. The introduction of IT capabilities into physical systems

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

presents emergent behavior that has security implications. Engineering models and analysis are evolving to address these emergent properties, including safety, security, privacy, and environmental impact interdependencies.

2.2 OT-Based Systems and Their Interdependencies

OT is used in many industries and critical infrastructures, including those identified by the Cybersecurity and Infrastructure Security Agency (CISA) as critical infrastructure sectors listed below. Critical infrastructures that typically contain OT are bolded.

- **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 critical to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. 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]. Overall, critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies. 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 consisting 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, and rail systems, as well as wastewater collection systems.

SCADA systems and DCS are often networked together. This is the case for electric power control centers and electric power 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. As an 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, an event that would lead to loss of power at a transmission substation. This loss could cause a major imbalance, triggering a cascading failure across the power grid. This could result in large area blackouts that could 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 Figure 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 signals 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 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 opened, resulting in security personnel being sent to investigate; an environmental sensor alerting to 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 on the order of milliseconds to minutes.

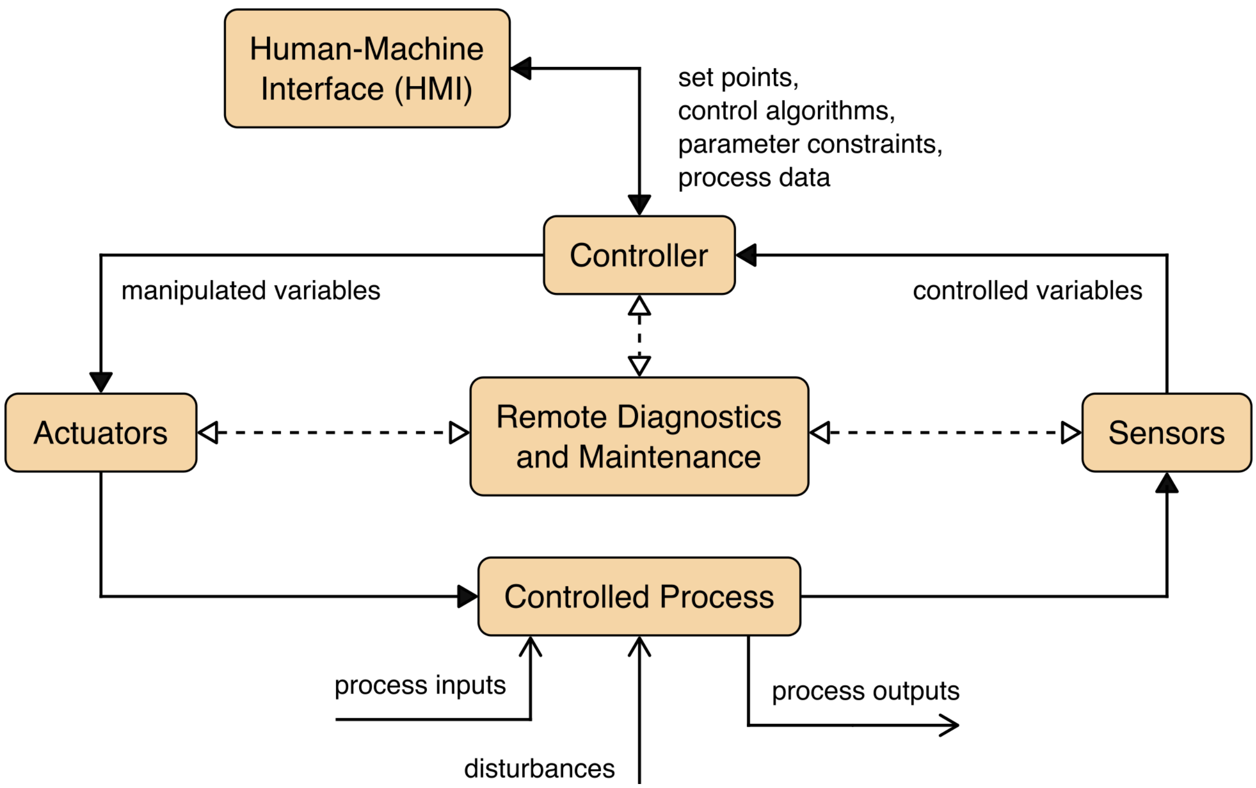

Figure 1: Basic operation of a typical OT system

2.3.1 OT System Design Considerations

The design of an OT system, including whether a SCADA, DCS, or PLC-based topology is used depends on many factors. 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.

- **Control Timing Requirements.** System processes have a wide range of time-related requirements, including very high speed, consistency, regularity, and synchronization. Humans may not be able to reliably and consistently meet these requirements; 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. Often a hierarchical/centralized control is used to provide human operators with a comprehensive view of the entire system.
- **Control Complexity.** Often control functions can be performed by simple controllers and preset algorithms. 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.** Availability (i.e., reliability) requirements of the system are also an important factor in design. Systems with strong availability/up-time requirements may require more redundancy or alternate implementations across all communications and control.
- **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. The design needs to address these requirements.
- **Safety.** The system's safety requirements are an important factor in design. 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 is an essential part of the safety system.

2.3.2 SCADA Systems

Supervisory control and data acquisition (SCADA) systems are used to control dispersed assets where 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 consisting of remote terminal units (RTUs) and/or PLCs, which 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 the transfer of information and data back and forth 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 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 into the system, although redundancy may not be a sufficient countermeasure in the face of 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 upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting.

The field sites at the bottom of Figure 2 perform local control of 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 running 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).

SCADA communication topologies vary among implementations. The various topologies used, including point-to-point, series, series-star, and multi-drop [AGA12], are shown in Figure 3. Point-to-point is functionally the simplest type; however, it can be expensive because of the individual channels needed for each connection. In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on 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 Figure 3 can be further augmented by using dedicated devices to manage communication exchanges and perform message switching and buffering. Large SCADA systems containing hundreds of RTUs often employ a sub-control server to alleviate the burden on the primary server. This type of topology is shown in Figure 4.

Figure 5 shows an example SCADA system implementation. This particular SCADA system 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 control center to field site communications, with two connections using 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 coming from field site alarm systems.

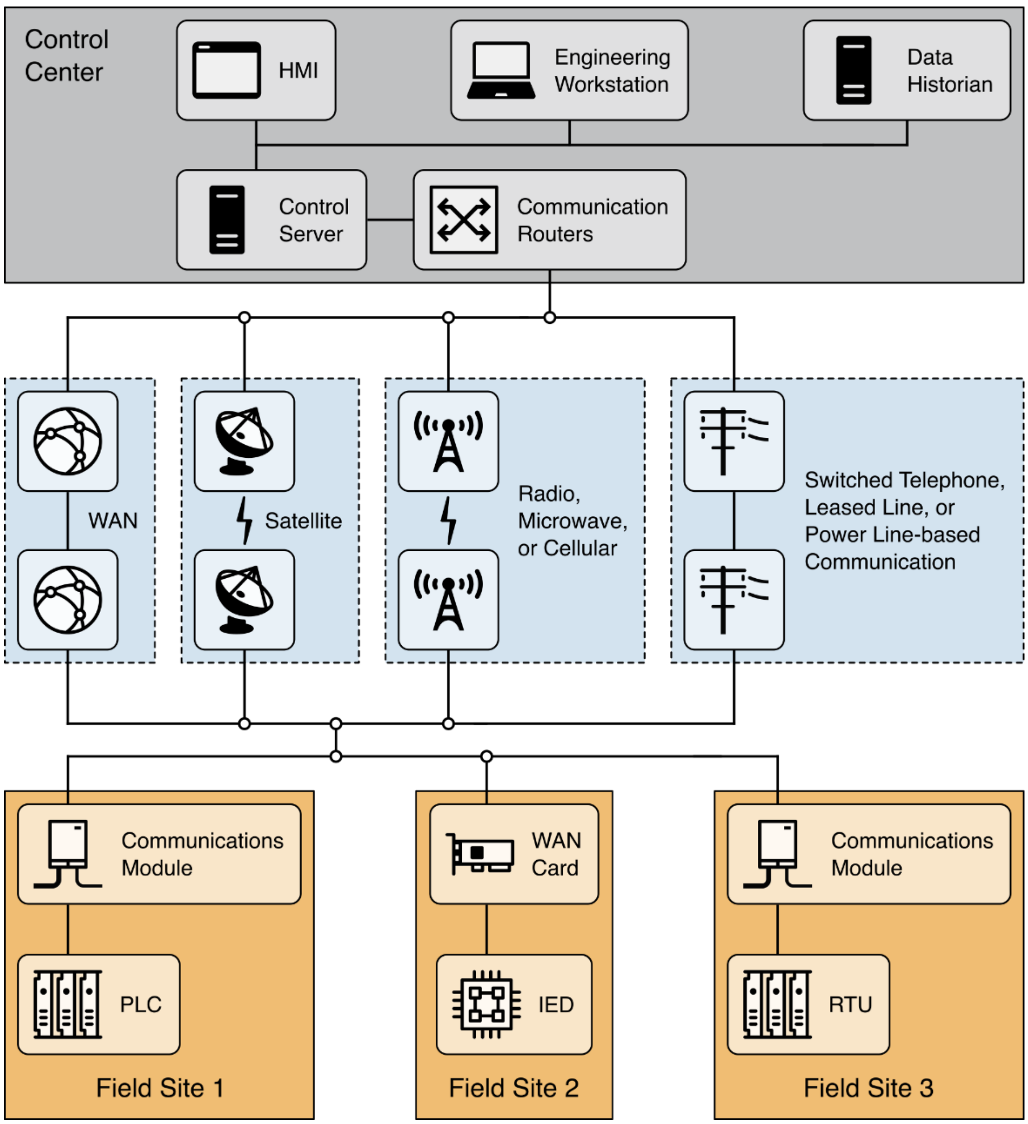

Figure 2: A general SCADA system layout showing control center devices, communications equipment, and field sites

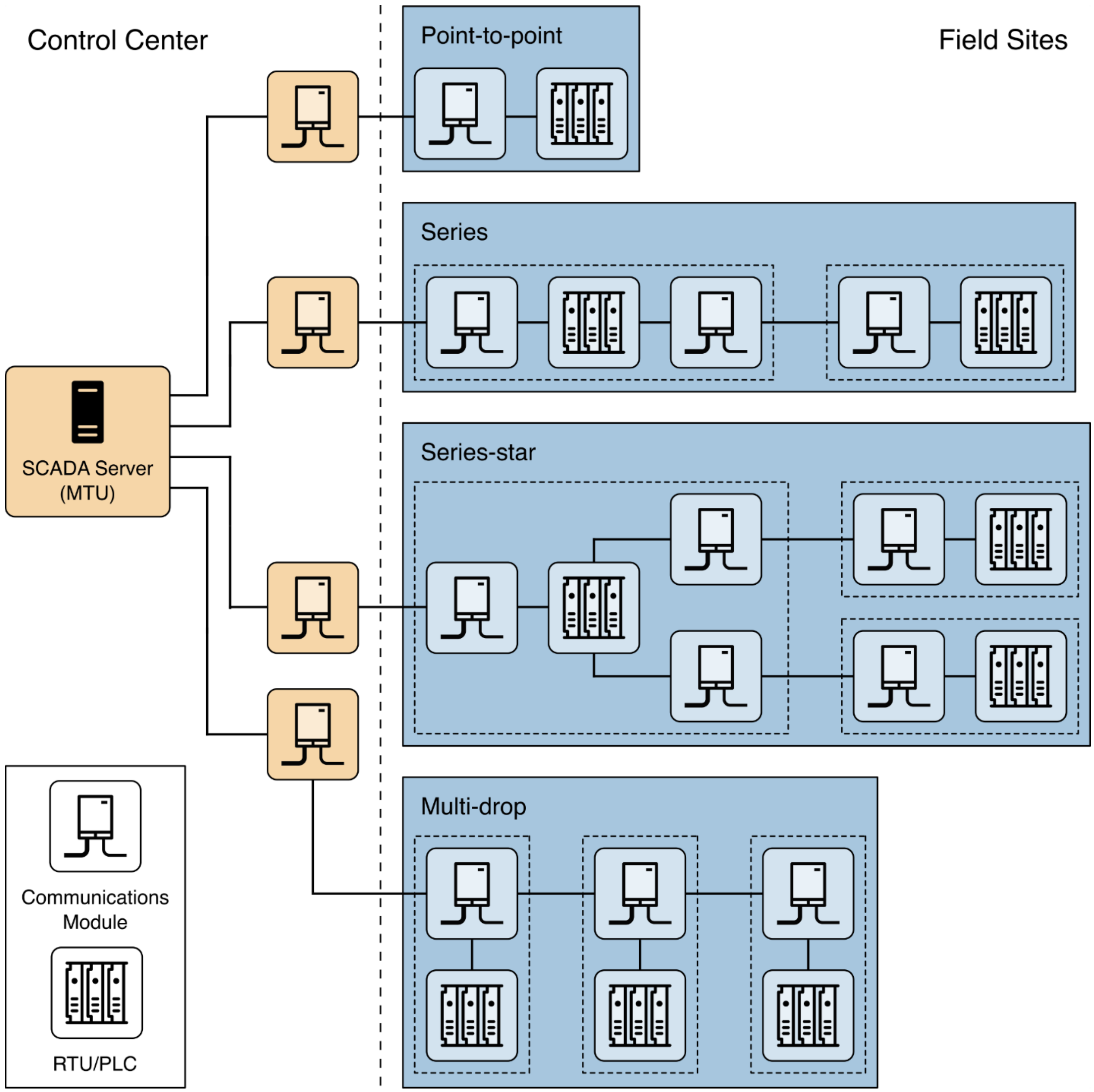

Figure 3: Examples of point-to-point, series, series-star, and multi-drop SCADA communications topologies

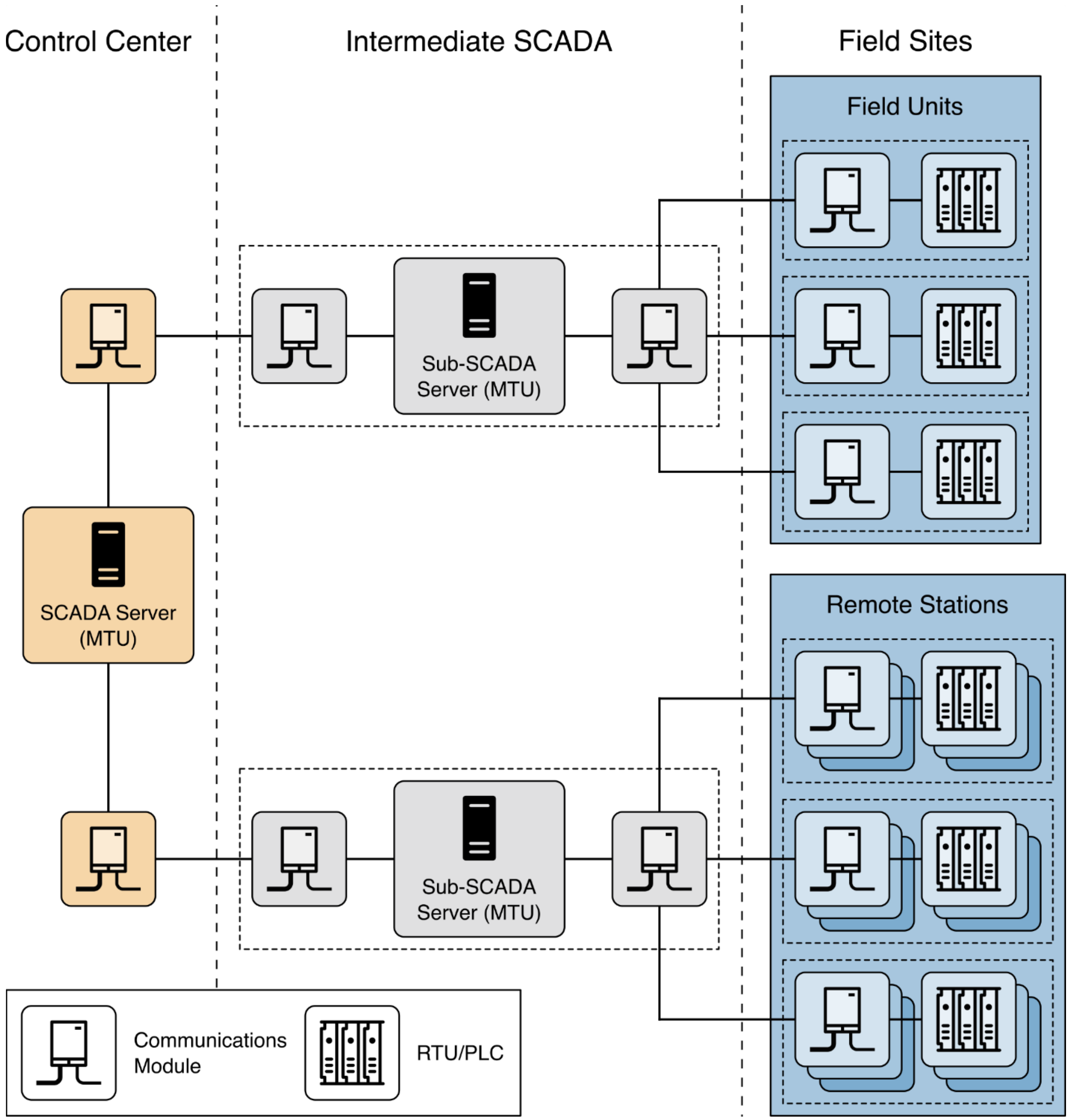

Figure 4: Example SCADA topology to support a large number of remote stations

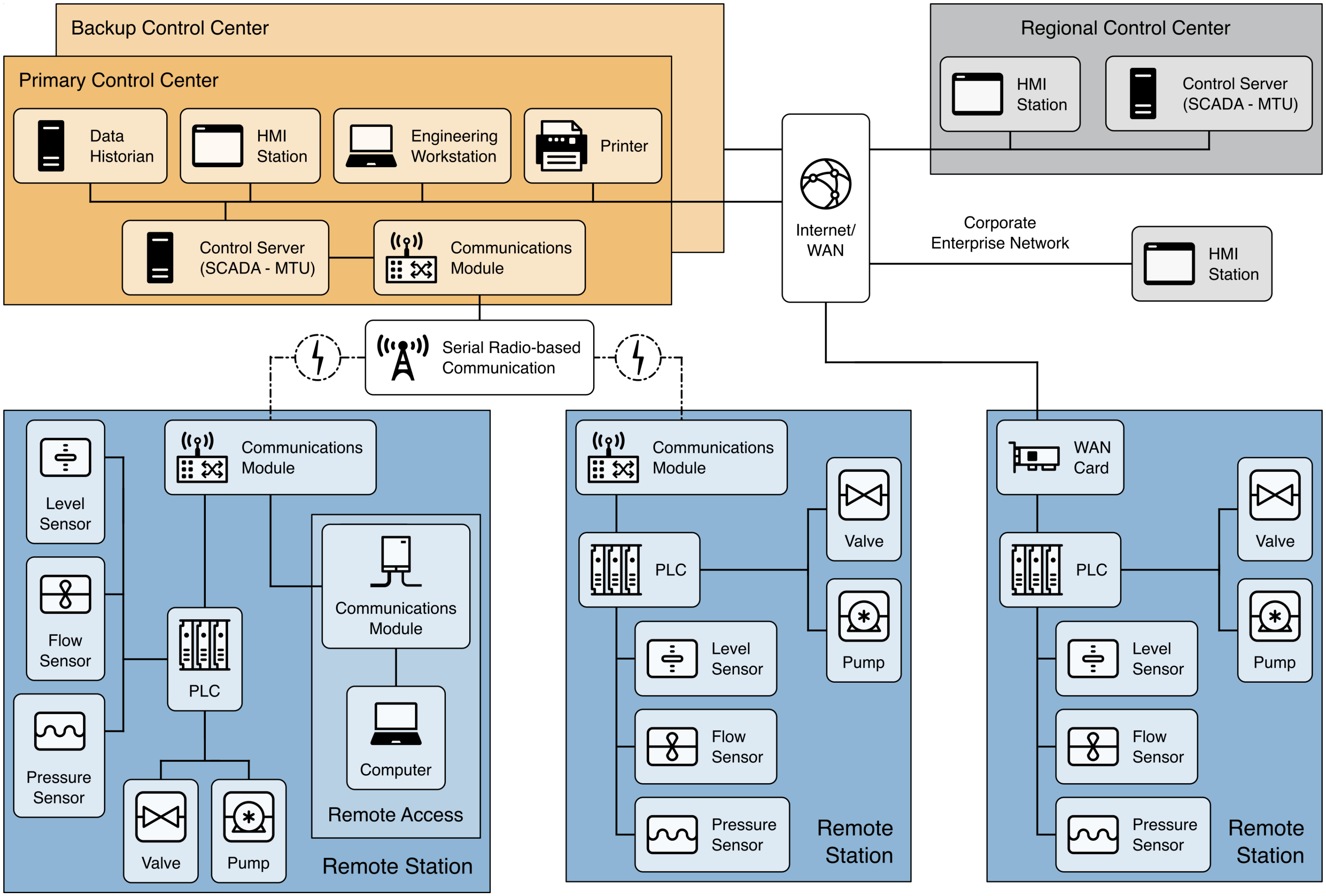

Figure 5: A comprehensive SCADA system implementation example

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 determined to be flooded or occupied by another train based on condition monitoring).

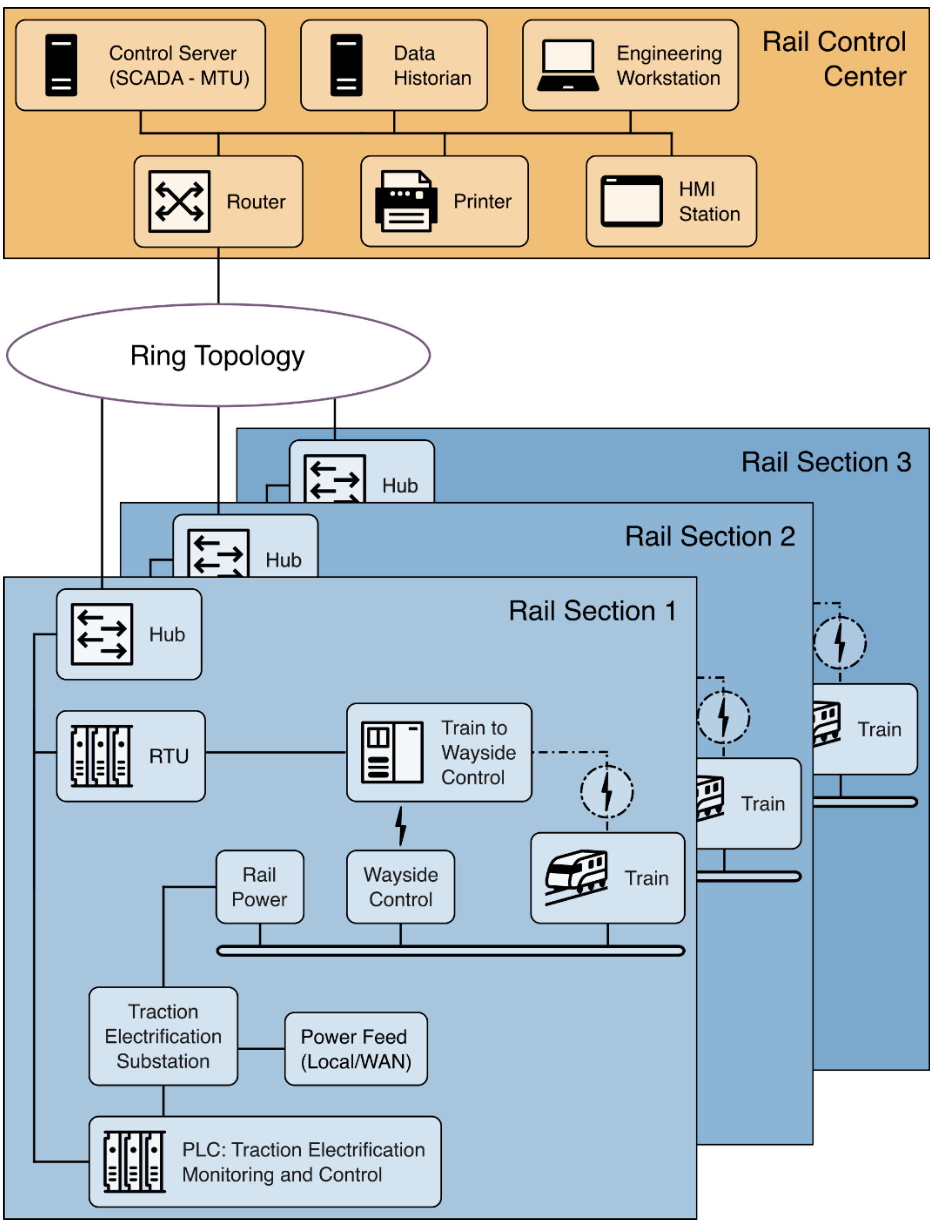

Figure 6: An example rail monitoring and control SCADA system implementation

2.3.3 Distributed Control Systems

Distributed control systems (DCS) are 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.

DCS are integrated as a control architecture containing a supervisory level of control overseeing 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. To accomplish the desired product and/or process tolerance around a specified set point, specific process controllers or more capable PLCs are employed in the field and are tuned to provide the desired tolerance as well as 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.

An example implementation showing the components and general configuration of a DCS is depicted in Figure 7. 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 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 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.

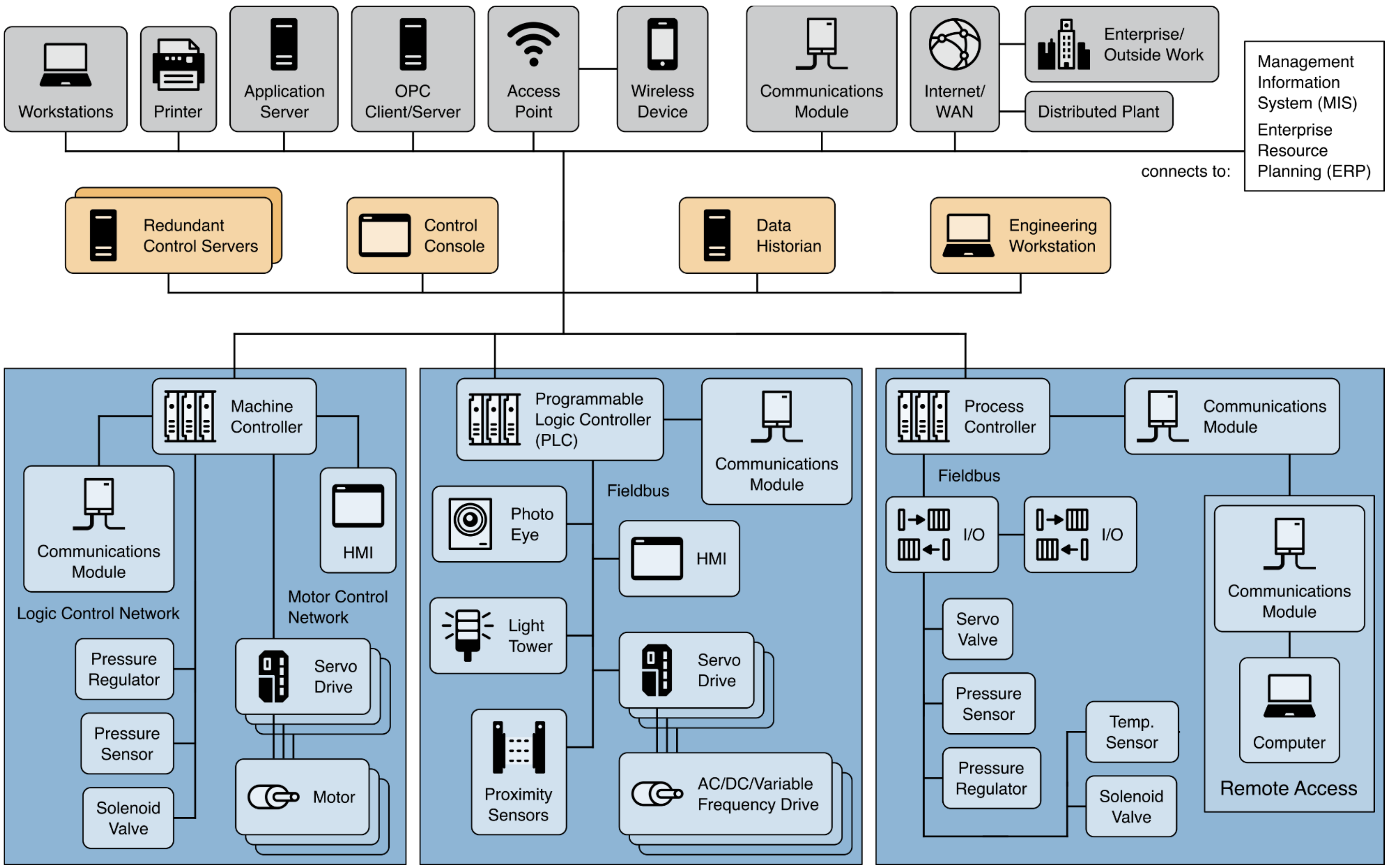

Figure 7: A comprehensive DCS implementation example

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 provide local management of processes through feedback control, as described in the sections above. In the case of SCADA systems, they may provide similar functionality to RTUs. When used in DCS, PLCs are implemented as local controllers within a supervisory control scheme.

In addition to PLC usage in SCADA and DCS, PLCs can 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, communication, arithmetic, and data and file processing.

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

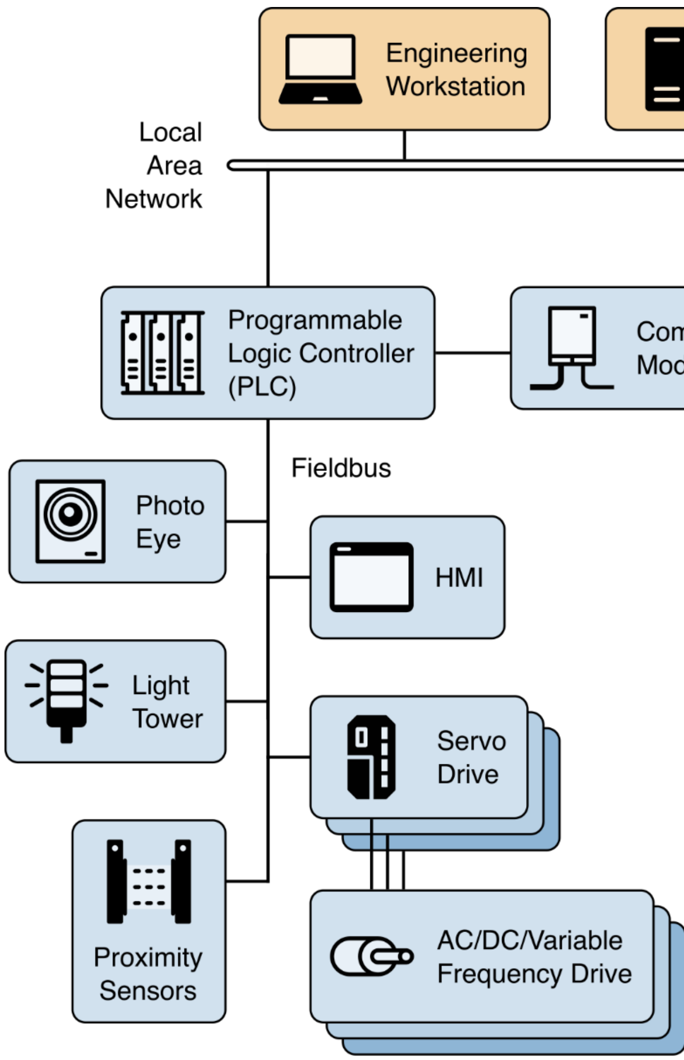

Figure 8: A PLC control system implementation example

2.3.5 Building Automation Systems

Building automation systems (BAS) are a type of OT used to control 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 BAS provide.

Some of the most common functions of BAS are maintaining the 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 upon device failure or an alarm condition).

An example of a BAS is shown in Figure 9. The architecture can be compared to a DCS, as it has a similar structure and distributed elements (typically throughout a building or buildings) which 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 if access should be granted.

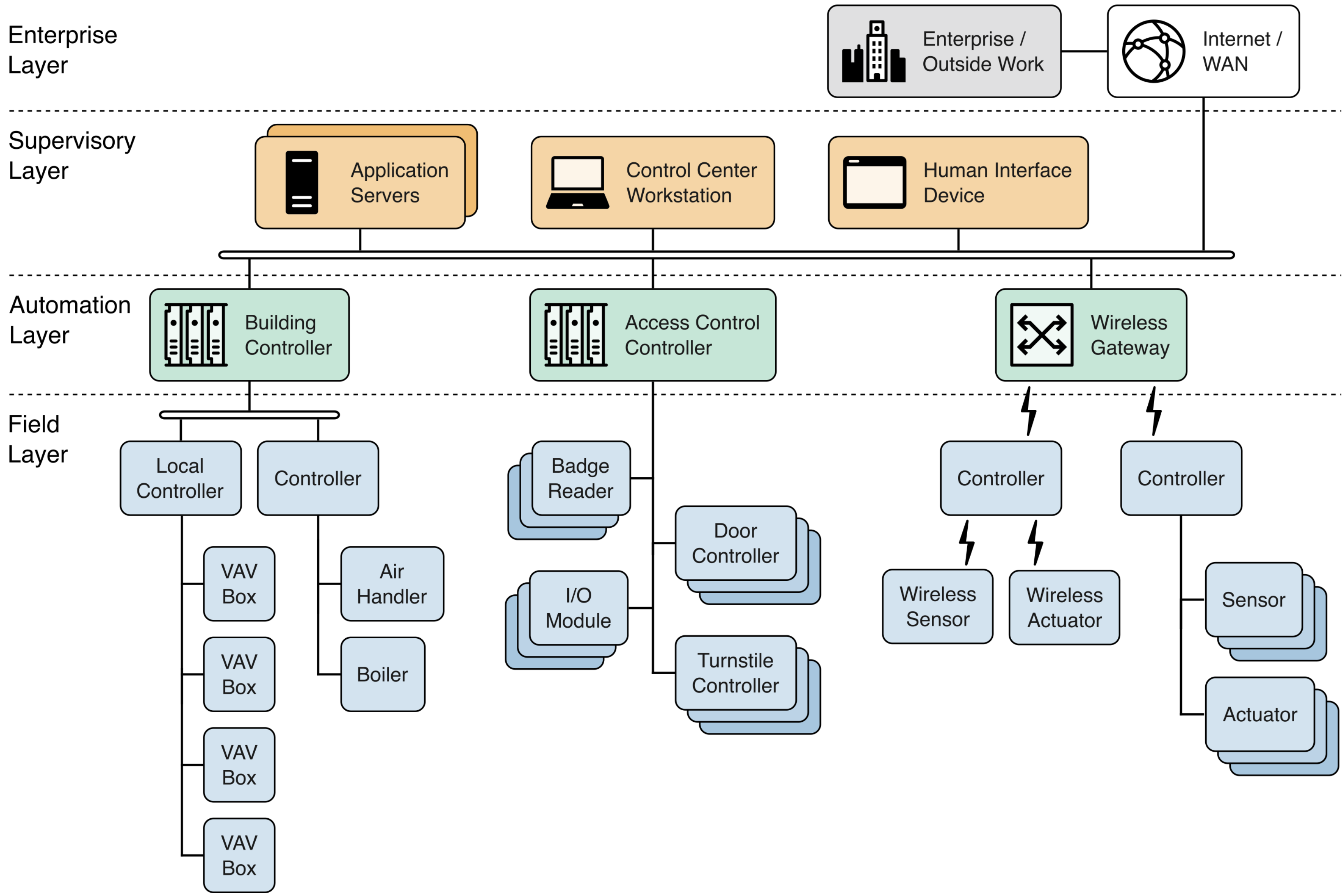

Figure 9: A comprehensive Building Automation System implementation example

2.3.6 Physical Access Control Systems

Physical access control systems (PACS) are 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/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. Most PACS require 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 to determine if 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.

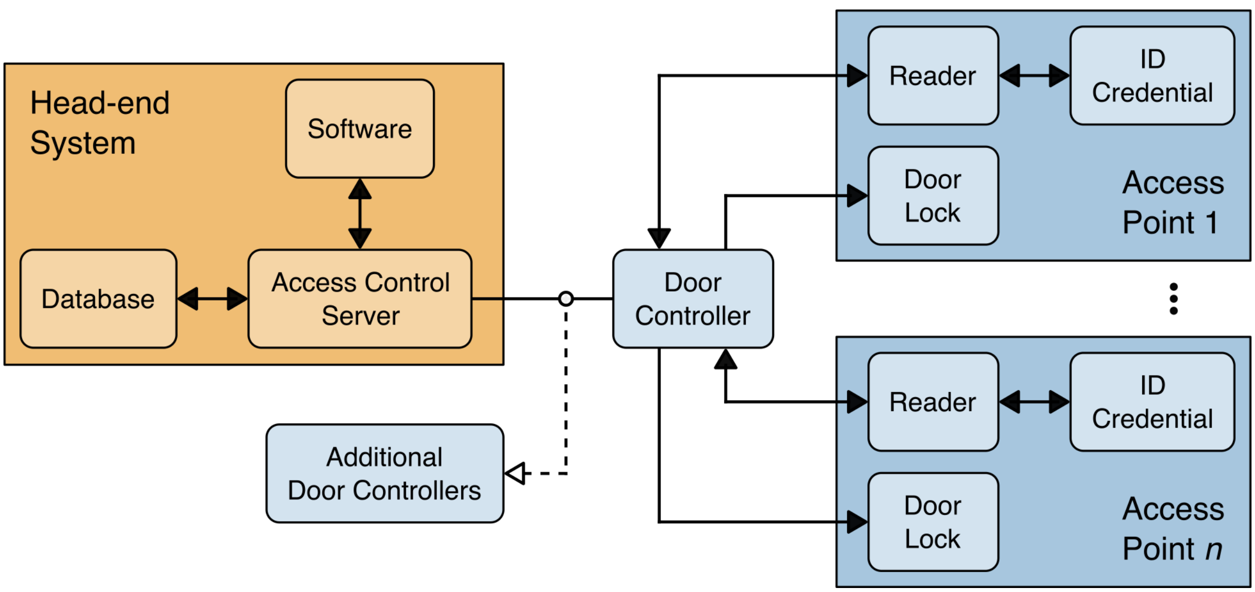

Figure 10: A Physical Access Control System implementation example

An example of a PACS is shown in Figure 10. 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 the door will be unlocked. 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.

2.3.7 Safety Systems

Many of the physical processes that OT systems control have the potential to create hazardous situations to 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). An *SIS* is a system that is composed of one or more Safety Instrumented Functions (SIFs). An *SIF* is an engineered system 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. They are implemented as part of an overall risk reduction strategy which is intended to reduce the likelihood and/or potential consequences of a previously identified event so it is within the organization's risk tolerance. Numerous other terms are associated with safety systems; however, the SIS is specifically designed in accordance with IEC 61511 [IEC61511]. SIS are typically found in chemical, refinery, and nuclear processes.

SIS are typically 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, SIS were designed to be standalone, physically and logically separated, and air gapped from the rest of the control system. In the configuration shown in Figure 11, the SIS and BPCS operated completely independent of each other with no direct communication between the systems. However, some modern SIS have been designed to allow communication with the control system. These types of SIS are called *Integrated Control and Safety Systems (ICSS)*. An ICSS solution may be an all-in-one device from a single vendor or may incorporate multiple devices from multiple vendors. While ICSS combine the functionality of both control and safety systems, the SIS still must comply with the requirements outlined in IEC 61511. One of the advantages to this ICSS methodology is the ability to communicate information from the SIS to the BPCS.

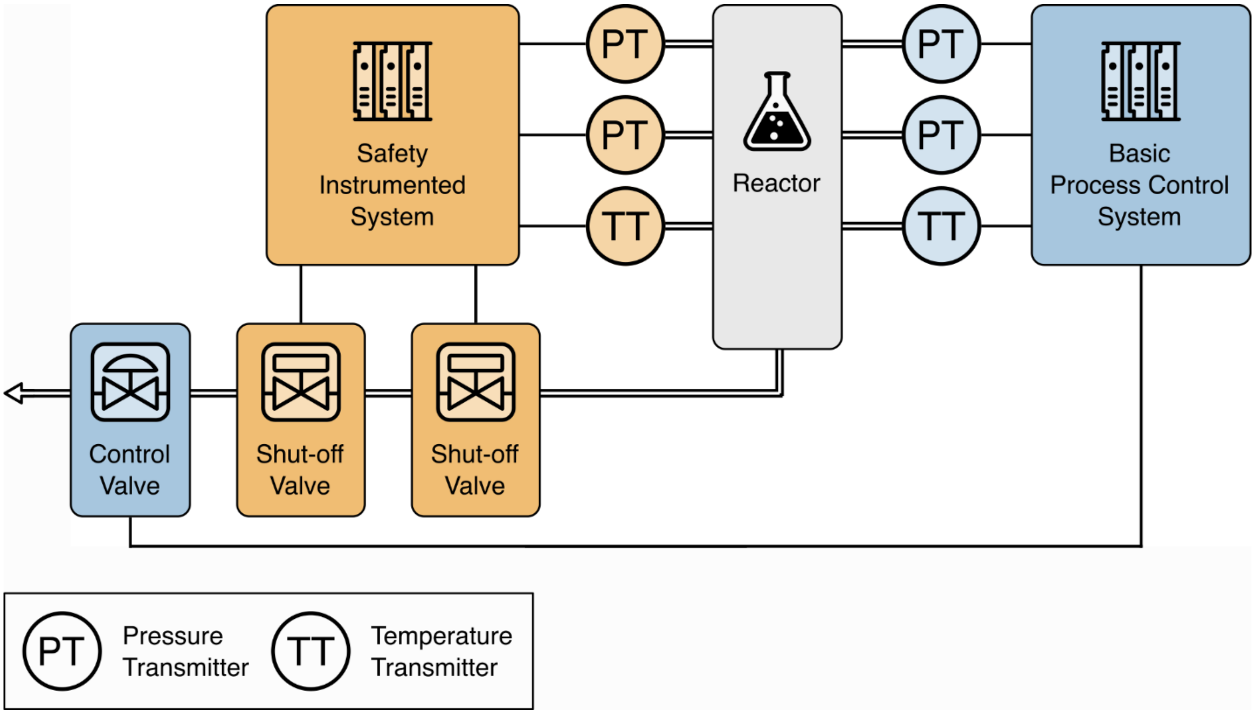

Figure 11: A Safety Instrumented System implementation example

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 the systems become even more interconnected, control of physical processes remains a relatively unique and critical concept of OT.

The Industrial IoT Consortium proposes a three-tier system architecture model for representing IIoT systems [IIRA19], consisting of 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 Figure 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 datacenter, an off-site datacenter, or in the cloud.

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 the business perspective, the location of the edge depends on the business objectives.

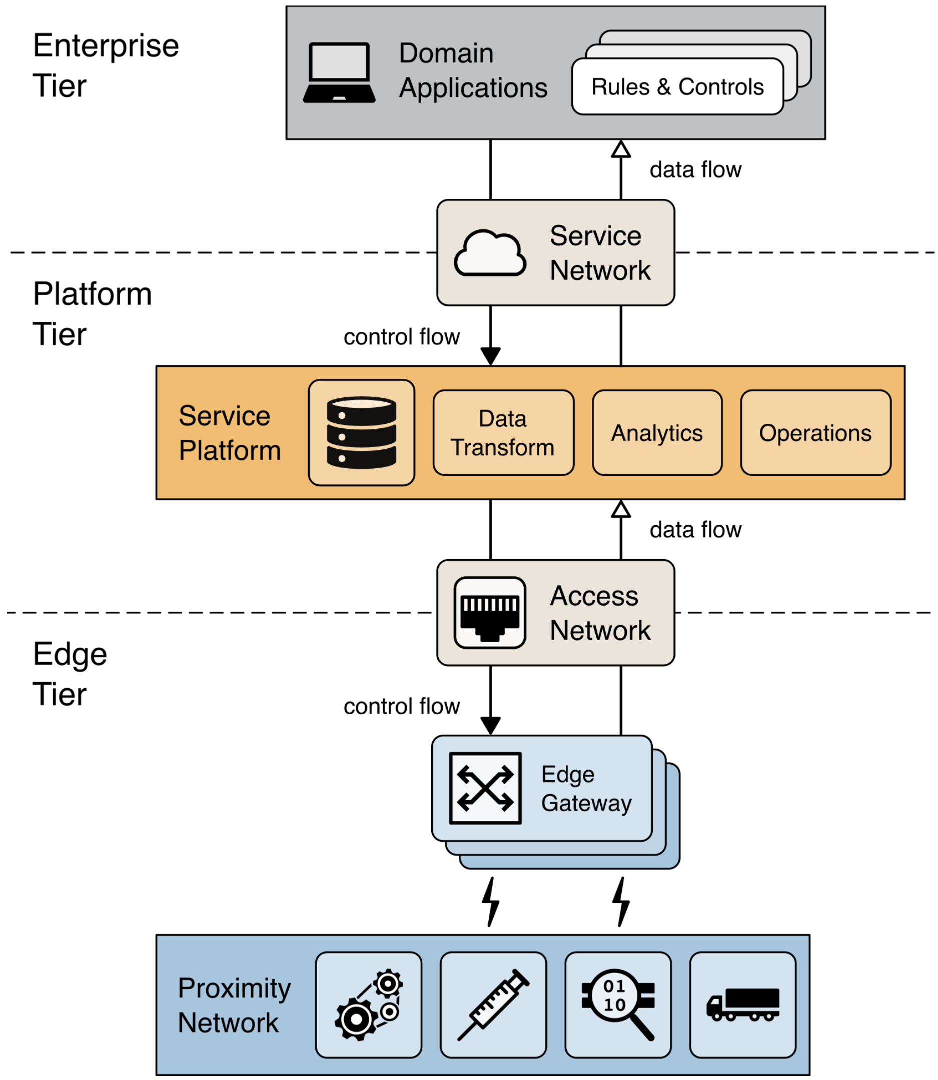

Figure 12: A three-tiered Industrial Internet of Things system architecture

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, defining 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. 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.

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 times of cyber-attack [Knapp].

Initially, OT systems had little resemblance to IT systems in that OT were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Ethernet, Internet Protocol (IP), and wireless devices are now replacing the older proprietary technologies, which increases the likelihood of cybersecurity vulnerabilities and incidents. As OT continues to adopt IT technologies to promote corporate connectivity and remote access capabilities, such as using industry standard computers, OSs, and network protocols, OT systems and devices are increasingly resembling IT systems. This integration supports new IT capabilities, but it 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.

The following lists some special considerations when considering security for OT:

- **Timeliness and Performance Requirements.** OT 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 they can typically withstand some level of delay and jitter. For some OT, automated response time or system response to human interaction is very critical. Many OT 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 not acceptable. Outages often must be planned and scheduled days or weeks in advance. Exhaustive pre-deployment testing is essential to ensure 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 the adverse impact 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 human safety, fault tolerance to prevent 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 of the particular physical domain.

- **System Operation.** OT OSs and control networks are often quite different from their IT counterparts, requiring different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers, not IT personnel. Assumptions that differences are insignificant can have disastrous consequences on system operations.

- **Resource Constraints.** OT and their RTOS are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems are often lacking resources common on modern IT systems. Many systems may not have 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 policy 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/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, when applied to OT, 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 in some instances available only from a single vendor. In some instances, third-party security solutions are not allowed due to OT vendor licensing and service agreements, and loss of service support can occur 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 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. 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 not acceptable. • 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.
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/weeks in advance. • High availability requires exhaustive pre-deployment testing.

Category	Information Technology	Operational Technology
Risk Management Requirements	• Manage data • Data confidentiality and integrity is paramount. • Fault tolerance is less important – momentary downtime is not a major risk. • Major risk impact is 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 not be acceptable. • Major risk impacts are regulatory non-compliance, environmental impacts, and 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 differing 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 perhaps 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 communications protocols • Primarily wired networks with some localized wireless capabilities • Typical IT networking practices	• Many proprietary and standard communication protocols • Several types of communications media used, including dedicated wire and wireless (radio and satellite) • Complex networks that sometimes require the expertise of control engineers
Change Management	• Software changes are applied in a timely fashion in the presence of good security policy and procedures. 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 often must be planned and scheduled days/weeks in advance. OT may use OSs that are no longer supported.
Managed Support	• Allow for diversified support styles.	• Service support is usually via 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. Some of the OSs and applications running 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 risk 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 review and update their OT cybersecurity plans and programs regularly 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, defining policies and procedures, identifying the cyber risk management capabilities that include people, process, and technology, as well as 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 risk to the systems and the organization. If there aren't sufficient time and resources to secure the system properly 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 the Sections listed in Section 3.3.10.

Organizations may also wish to consult ISA-62443-2-1, *Security for Industrial Automation and Control Systems: Security Program Requirements for IACS Asset Owners*, which describes another view of the elements of a cybersecurity program for use in the OT environment. It provides guidance on how to meet the cybersecurity requirements described for each element of the cybersecurity program [ISA62443].

3.1 Establish a Charter for OT Cybersecurity Program

Senior management must demonstrate a clear commitment to cybersecurity and should communicate its importance throughout the organization. Cybersecurity is a business responsibility shared by all members of the organization and especially by its leaders and IT and OT teams. Commitment to cybersecurity, both IT and OT, 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 the OT resources and provides a mandate for the most senior person responsible to establish and maintain the cybersecurity program (e.g., CISO). In this section, the focus is on the OT-specific program. However, the OT cybersecurity program should be integrated with the overall cybersecurity program for the organization.

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 scope, responsibility, and authority to lead the OT cybersecurity program. The OT cybersecurity manager should define the roles and responsibilities of system owners, mission/business process managers, and users. The OT cybersecurity manager should 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. In the long run, it will be more effective if the team can share resources with others in the organization that have similar objectives.

3.2 Business Case for OT Cybersecurity Program

The cybersecurity of OT systems is a critical component in the overall security for the organization. An OT cybersecurity program considers the characteristics of OT systems that differ from IT systems, necessitating special consideration in securing OT.

Attacks on OT systems are increasing and can cause physical damage or even halt production. As OT systems are increasingly being connected to IT networks, relying on traditional measures is not enough to protect such systems from cyber-attack. e.g., traditional measures like air gap are no longer realistic as systems are more connected to the enterprise network for productivity or efficiency reasons. Also, OT systems can be used as an entry point to the organizational IT systems and other enterprise systems. Therefore, security measures tailored to the OT system are required to protect the organization. The OT cybersecurity program can provide an organization-wide strategy to secure the system.

The ability to perform its missions and goals is an important requirement for many organizations and OT operators. Managing the risk of the OT system to ensure the organization meets its goals and missions is a high priority for these OT operators. The potential impact of a cybersecurity event could be severe—it could impact the organization’s mission and objectives, the environment, regulatory compliance, and even human safety. An OT cybersecurity program can provide a methodology and strategy to mitigate the risks.

3.2.1 Benefits of Cybersecurity investments

OT cybersecurity supports the mission and business functions of the organization. Investment in OT cybersecurity can provide 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 cost

A strong OT cybersecurity program is fundamental to a sustainable business operation. An OT cybersecurity program with OT-specific security policies can potentially enhance system reliability and availability. This also includes minimizing unintentional OT system information security impacts from inappropriate testing, policies, and misconfigured systems. The importance of secure systems should be further emphasized as business reliance on interconnectivity increases. Denial of service (DoS) attacks and malware (e.g., worms, viruses) have become very common and have already impacted OT systems. Cyber-attacks can have significant physical and consequential impacts. The major categories of impacts are as follows:

- **Physical Impacts.** Physical impacts encompass the set of direct consequences of OT failure. The potential effects of paramount importance include personal injury and 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 from physical impacts ensuing from an OT incident. Physical impacts could result in repercussions to system operations, which in turn inflict a greater economic loss on the facility, organization, or others dependent on the OT systems. Unavailability of critical infrastructure (e.g., electrical power, transportation) can have economic impact far beyond the systems sustaining direct and physical damage. These effects could negatively impact the local, regional, national, or possibly global economy.
- **Social Impacts**. Another second-order effect, the consequence from the loss of national or public confidence in an organization, is many times overlooked. It is, however, a very real consequence that could result from an OT incident.

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

- Impact on national security—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

Undesirable incidents of any sort detract from the value of an organization, but safety and security incidents can have negative impacts that last longer than other types of incidents on all stakeholders—employees, shareholders, customers, and the communities in which an organization operates. The list of potential business consequences needs to be prioritized to focus on the consequences that senior management will find the most compelling. The highest priority items should be evaluated to estimate the annual business impact, preferably but not necessarily 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 allocation of resources needed for development, implementation, and maintenance of the program. Without a strong commitment by senior management, it may be difficult to prioritize the allocation of resources to sustain the program.

The first step in developing an OT security program is to identify the business objectives and missions of the organization, and how the cybersecurity program can lower risk and protect the organization's ability to perform its mission. 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

Costs and resources required to develop, implement, and maintain the security program should be considered. The economics benefit of the cybersecurity program may be evaluated similar to worker health and safety programs. However, an attack on the OT system could have significant consequences that far exceed the monetary costs.

3.2.3 Resources for Building Business Case

Significant resources can be found in external resources from other organizations in similar lines of business—either individually or in information sharing exchanges, trade and standards organizations, consulting firms, and internal resources in related risk management programs or engineering and operations. External organizations can often provide useful tips as to what factors most strongly influenced management to support their efforts and what resources within their organizations proved most helpful. For different industries these factors may be different, but there may be similarities in the roles that other risk management specialists can play.

Appendix D provides a list and short descriptions of some of the 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 based on their experiences with related incidents in the organization. This information is helpful from the standpoint of prioritizing threats and estimating business impact. These resources can also provide insight into which managers are focused on dealing with which risks and, thus, which managers might be the most appropriate or receptive to serving as a champion.

3.2.4 Presenting the OT Cybersecurity Business Case to Leadership

It is critical for the success of the OT cybersecurity program that it receives senior management buy-in and that they actively participate in the program. Organization-level management that encompasses both IT and OT operations has the perspective to understand the risks and 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 obtain management buy-in is to base the business case on a successful example. The business case should inform management that the other organization had the same problem and then present the solution they have found and how they were able to solve it. This will often prompt management to ask how this solution might be applicable to their organization.

When presenting the business case to leadership, it may 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 for OT systems. The security measures or tools that work well with IT systems may not work effectively in the OT environment.
- Compensatory measures may be an effective solution to secure 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, when implemented and maintained, provide a security roadmap that helps to manage OT cybersecurity risk. These recommendations are independent, which allows the organization to select approaches and technologies most suitable to their needs.

An OT cybersecurity program typically tailors to a specific OT environment. An organization may have multiple sites, each with multiple specific OT environments. In such a situation, it is recommended that an organizational-level OT security program be defined whose recommendations 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. The organizational information security program typically focuses on confidentiality, integrity, and availability, in that order, of information for the entire organization. Information security programs generally do not specifically address all the security and operational needs of an OT environment. In the OT environment, the focus is usually on safety, availability, integrity, and confidentiality, in that order. 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 twenty years. As a result, many legacy systems may contain hardware and software that are no longer supported by the vendors and cannot be patched or updated to protect against known vulnerabilities. In that case, the security program should tailor to the unique characteristics of the legacy system to determine if the controls are applicable. In situations where 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, e.g., using a firewall with deep packet inspection capability that can monitor and block advanced threats like malware, disabling unused ports in switches, or physically securing switches.

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 in this program are viewed through the lens of corporate risk management. To help design and drive a cybersecurity program with a risk management perspective, the risk management framework defined by NIST 800-37r2 [SP800-37r2] is used to define the core tasks and the processes for implementing a cybersecurity program. This is briefly summarized in the subsection "Implement an OT Security RMF" and further elaborated in Section 4.

The OT cybersecurity program also needs to 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 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 the guidance to the specific organization.

3.3.1 Establish OT Cybersecurity Governance

The governance should include policies, procedures, and processes to manage the organization's regulatory, legal, risk, environmental, and operational requirements. The governance should ensure that the policies, procedures, and processes are well understood by the staff and inform the management of OT cybersecurity risk. To establish an effective OT cybersecurity governance capability, develop a process and assign the responsibility and accountability to the appropriate role in the corporate risk management function to ensure that the various elements of an OT cybersecurity program are operational and effective, and that it is integrated with the corporate risk management function. Typically, a cybersecurity governance process should include the following:

- Ensure that 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 with corporate risk management processes

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

3.3.2 Build and Train a Cross-Functional Team to Implement 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 of 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 provider.

From a safety perspective, there are serious consequences relating to major accident hazards and loss of containment due to equipment failure or operator mistakes. Cybersecurity is another threat to the safety and reliability of industrial processes, so including the 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 spread, and complexities. These factors along with 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 corporate risk management function.

The responsibility and accountability for implementing and managing cybersecurity functions typically falls under the IT and OT infrastructure organization, whereas the 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 on 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. Third-party providers include, for example, service providers, contractors, and other organizations providing 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 details with specific examples for establishing a cross-functional team are also provided in NISTIR 8183A, *Cybersecurity Framework Manufacturing Profile - Low Impact Level Example Implementations Guide* [IR8183A].

3.3.3 Define 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 tradeoffs, 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 [SP800-37r2], Prepare Step, Task P-2, Risk Management Strategy. Section 3 provides additional information on organization-level system-level task to prepare for implementing the NIST Risk Management Framework.

The OT cybersecurity strategy:

- Refines and supplements, as necessary, 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: 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. The acceptable risk tolerance for OT drives the priorities for the OT cybersecurity operation. The program should address both IT and OT concerns and requirements; for example, IT may concern 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 details and specific examples for establishing an OT cybersecurity strategy are also provided in NISTIR 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 a cybersecurity program. OT-specific security policies and procedures should be derived from existing IT cybersecurity and plant operational policies and procedures where possible for consistency throughout the organization.

As discussed earlier, organizational management is responsible for developing and communicating the risk tolerance level of the organization—the level of risk the organization is willing to accept—which allows the OT cybersecurity manager to determine the risk management strategy. The development of the cybersecurity policies should be based on a risk assessment that will set the security priorities and goals for the organization so that the risks posed by cyber threats are managed sufficiently. Procedures that support the policies need to be developed so that the policies are implemented fully and properly for the 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 details with examples of establishing OT-specific policies and procedures are also provided in NISTIR 8183A, *Cybersecurity Framework Manufacturing Profile - Low Impact Level Example Implementations Guide* [IR8183A].

3.3.5 Establish Cybersecurity Awareness Training Program for OT Organization

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

Further guidance for OT cybersecurity awareness training can be found in Section 6 and Appendix D. Additional details with specific examples for OT cybersecurity awareness training are also provided in NISTIR 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 with responsibility for the mission or business function establish and conduct 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 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 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 organizations policies and procedures. The tools used for maintenance logging and tracking should be controlled and managed. Ensure that the processes and tools allow 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 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 performed.

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

3.3.8 Develop 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 with 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 details with specific examples for OT incident response are also provided in NISTIR 8183A, *Cybersecurity Framework Manufacturing Profile – Low Impact Level Example Implementations Guide* [IR8183A].

3.3.9 Develop 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 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) or both to prepare the OT organization to respond appropriately to significant disruptions in their operation 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 OT assets and services affected by cybersecurity incidents.
- Establish communication plans to coordinate restoration activities with internal and external stakeholders and executive management team.
- Establish communication plans to manage public relations.
- Establish a lessons learned task as part of the recovery process for continuous improvement of the cybersecurity capabilities – 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 details with specific examples for OT recovery and restoration are also provided in NISTIR 8183A, *Cybersecurity Framework Manufacturing Profile - Low Impact Level Example Implementations Guide* [IR8183A].

3.3.10 Summary of OT Cybersecurity Program Content

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

Table 2: Sections with additional guidance on 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 OT Cybersecurity Program	Section 4, Appendix D
Define OT Cybersecurity Strategy	Section 5, 6, Appendix C, D
Define OT-Specific Policies and Procedures	Section 6
Establish Cybersecurity Awareness Training Program for OT Organization	Section 6, Appendix D
Implement a Risk Management Framework for OT	Section 4, 6, Appendix C, D
Develop Maintenance Tracking Capability	Section 6
Develop Incident Response Capability	Section 6, Appendix C
Develop Recovery and Restoration Capability	Section 6

4 Risk Management for OT Systems

Organizations manage risk every day when meeting their business objectives. These risks may include financial, equipment failure, and personnel safety, to name just a few. 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 management of risk is conducted as an interactive ongoing process as 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 are 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 and the Privacy Framework.

A risk management process is employed throughout an organization using a three-level approach to address risk at the (i) organization level; (ii) mission/business process level; and (iii) system level (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 having a shared interest in the mission/business success of the organization.

This section focuses primarily on OT system considerations at the system level; however, 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 NIST SP 800-53, Revision 5 [SP800-53r5] control families. Throughout the following discussion of risk management, OT system considerations and the impact that these considerations have on the risk management process are discussed.

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 Revision 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 to include 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: (i) how to prepare for risk assessments; (ii) how to conduct risk assessments; (iii) how to communicate risk

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 operation of an information system and to 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.

assessment results to key organizational personnel; and (iv) how to maintain the risk assessments over time.

4.1 Managing OT Security Risk

While the risk management process presented in NIST SP 800-39 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 Figure 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. As the environment in which organizations operate is always changing, risk management must be a continuous process where 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.

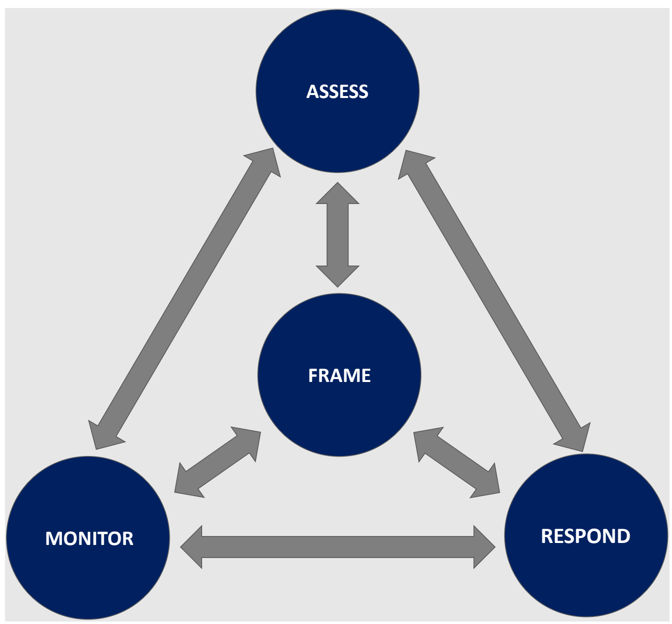

Figure 13: Risk Management Process: Frame, Assess, Respond, Monitor

Organization-wide risk management is applied at three levels, as Figure 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/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.

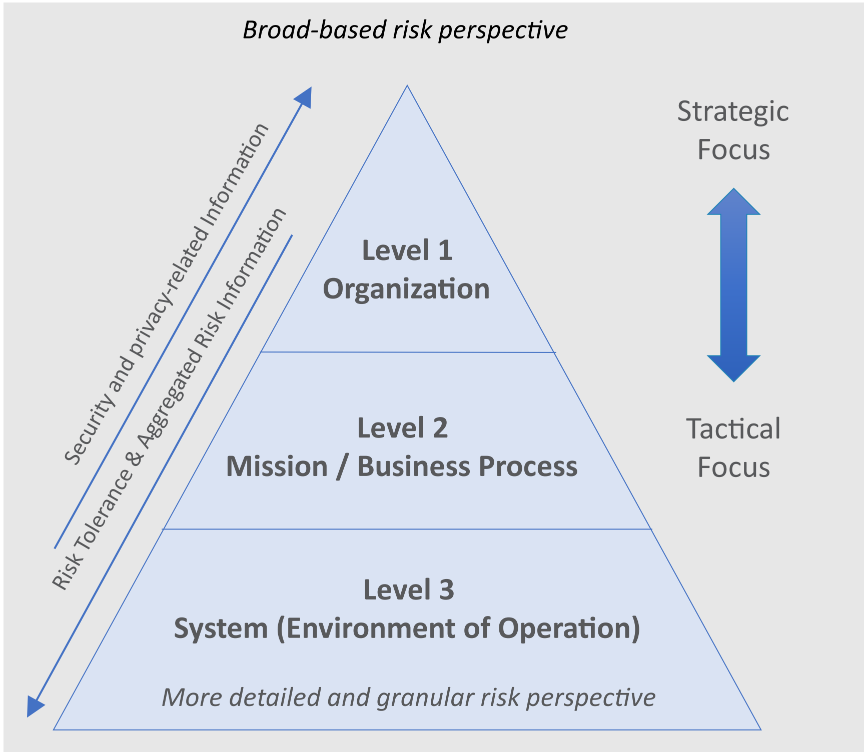

Figure 14: Risk Management Levels: Organization, Mission/Business Process, and System

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 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 is the major consideration that 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 possible from the resulting OT system malfunction from the cyber incident, taking into consideration any previously performed safety impact assessments performed by the organization regarding the employees and the

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

public. The importance of safety and developing/ensuring a safety culture plays a critical role in the determination of risk tolerance.

Organizations should consider incorporating an analysis of cybersecurity effects on OT systems that impact environmental and personnel safety and mitigating controls. More specifically, organizations may want to consider having 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 and 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 organization tolerance levels.

Another major concern for OT system operators is typically the availability of services provided by the OT system. The OT system may be part of critical infrastructure (for example, 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 level(s) of redundancy required to achieve the desired resilience levels for their operating environments and incorporate these requirements into the risk framing. This may help organizations make risk decisions that avoid unintended consequences on those who depend on the services provided. More specifically, organizations consider identifying interdependent OT systems that pose cybersecurity risks that threaten system availability.

Additionally, organizations may want to 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 the organization. Impact propagation could occur due to both physical and logical dependencies. Proper communication of 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 propagated to the connected OT systems. An example could be if a virus or worm propagated to a connected OT and then impacted that system. Physical damage could also propagate to other interconnected OT. If an incident impacts the physical environment of an OT, it may also impact other related physical domains. For example, the impact could result in a physical hazard which degrades nearby physical environments. Additionally, the impact could also degrade common shared dependencies (e.g., power supply) or result in a shortage of material needed for a later stage in an industrial process.

CISA serves to promote a cohesive effort between government and industry that will improve CISA's ability to anticipate, prioritize, and manage national-level OT risk. CISA assists OT systems' vendors and asset owners, operators, and 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 might 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. Organizations may also need to consider that the impact of a cyber incident in an OT environment may include both physical and digital effects and, therefore, the risk assessments need to incorporate these additional effects, including:

- Impacts on safety and use of safety assessments
- Physical impact 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 also select appropriate risk assessment methodology(ies) 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 & 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 operation 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; and
- 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.

Additionally, to support risk framing, organizations may also need to determine how OT systems interact or depend on IT. 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, which specifies that systems are categorized as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability [FIPS199]. Another approach, based on ISA 62443-3-2 [ISA62443], provides example definitions for assisting organizations with determining a system categorization utilizing OT impacts.

Table 3 provides possible example categories and impact levels 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 High Impact instead of Moderate as shown in the table.

Table 3: Possible Definitions for OT Impact Levels Based on Product Produced, Industry, and Security Concerns

Category	High	Moderate	Low
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 expecting 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; little to no impact on community
Cost (% of Revenue)	> 25%	> 5%	< 5%
Legal	Felony criminal offense or compliance violation affecting license to operate	Misdemeanor criminal offense or compliance violation resulting in fines	None
Public Confidence	Loss of brand image	Loss of customer confidence	None
People Onsite	Fatality	Loss of workday or major injury	First aid or recordable injury
People Offsite	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); the threat event will be initiated; and 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, or other factors. In some situations, organizations may find that there is minimal organizational historical data. In these cases, organizations may want to consider extending their analysis to consider industry-specific data that may describe cybersecurity events reported for similar organizations.

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

OT-Specific Recommendations and Guidance

Organizations establishing definitions for event likelihood may want to review Appendix G of 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 (intentional threat actors) and non-adversarial (errors, accidents, acts of nature, etc.) events. Additionally, organizations will want to establish definitions for the likelihood an event will 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 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 the OT Environment

Leveraging the outputs of framing risk, such as acceptable risk assessment methodologies, risk management strategy, and risk tolerance, risk assessments are conducted to 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/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 arising from those threats and vulnerabilities may occur.

When the organization conducts a risk assessment that includes OT systems, there may be additional considerations that do not exist when doing a risk assessment of traditional IT systems. Because the impact of a cyber incident in an OT may include both physical and digital effects, risk assessments need to incorporate those potential effects.

OT-Specific Recommendations and Guidance

Organizations need to consider that 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 NVD, and MITRE ATT&CK for ICS framework 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-Specific Recommendations and Guidance

The physical operating environment is another aspect that organizations should consider when working with an OT system. 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 in the framing component so that the risks arising from these constraints are identified and considered. 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
- Ensure that physical security personnel understand the relative risks and physical security countermeasures associated with the OT system environments they protect
- Ensure that physical security personnel are aware of which areas of an OT system production environment house data acquisition and operate in sensitive spaces
- Mitigate business continuity risk by specifying immediate response plans if physical safety is jeopardized

Risk assessments also require reviewing digital and non-digital mechanisms 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. Therefore, these non-digital mechanisms may help reduce any negative impact that a digital incident on the OT might have and are incorporated into the risk assessment process. For example, OT often have non-digital control mechanisms that can prevent the OT from operating outside of a safe boundary, and thereby limit the impact of an attack (e.g., a mechanical relief pressure valve). In addition, analog mechanisms (e.g., meters, alarms) can be used to observe the physical system state to 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 that measure and display the state of the physical system (e.g., temperature, pressure, voltage, current) and can provide the operator with accurate information in situations 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) provide operators with the ability 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 be able to prevent the physical process from entering an undesired state in situations 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 rise of internal fluid pressure in excess of a specified value, thus bringing the process to a safer state. The device also may be designed to prevent excessive internal vacuum. The device may be 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 consider the potential impact that a cyber incident may have on OT by analyzing all digital and non-digital control mechanisms and the extent to which they can mitigate potential negative impacts to the OT. There are multiple considerations when considering the possible mitigation effects of digital and non-digital control mechanisms, such as how non-digital control mechanisms may require additional time and human involvement to perform necessary monitoring or control functions. For example, such mechanisms may require operators to travel 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. Privacy risk assessments sometime require a different approach, so organizations may want to consider utilizing the NIST Privacy Risk Assessment Methodology (PRAM)—a tool that applies the risk model from NISTIR 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 (e.g., identify possible courses of actions to address risk, evaluate those possibilities considering the organization's risk tolerance and other considerations determined during framing, and choose 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 those options.[8]

OT-Specific Recommendations and Guidance

For an OT system, available risk responses may be constrained by system requirements, potential adverse impact 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 the effect of an incident to acceptable levels.

4.1.4 Monitoring Risk in an OT Environment

Monitoring risk is the fourth component of the 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 the other components.

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

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

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

4.2 Special Areas for Consideration

4.2.1 Supply Chain Risk Management

Cybersecurity risks can arise from products or services acquired to support OT needs. These risks can be introduced anywhere in the supply chain and at any stage across the life cycle. These risks—whether malicious, natural, or unintentional—have the potential to compromise the availability and integrity of critical OT systems and components, and the availability, integrity, and confidentiality of the data utilized by the OT, causing harms ranging from minor disruption to life-safety impacts.

With few exceptions, organizations with responsibility for OT rely upon suppliers and other third-party providers and their extended supply chains for a range of needs. These supply-side organizations perform critical roles and functions, to include manufacturing and provisioning technology products, providing software upgrades and patches, performing integration services, or otherwise supporting day-to-day operations and maintenance of OT systems, components, and operational environments. For this reason, it is necessary and important that OT organizations should seek to understand and mitigate the supply chain-related risk that can be inherited from these supply-side organizations and the products and services 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. Vetting suppliers and service providers should be done to ascertain their capabilities, trustworthiness, the adequacy of their internal security practices, and the effectiveness of safeguards, and to understand their supply chain relationships and any risks that may be associated with those relationships and dependencies. Requirements for and evaluation of products and discrete components should go beyond an assessment of whether functional and technical requirements are satisfied and address applicable C-SCRM factors such as, but not limited to, 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, implementing the key practices, C-SCRM security controls, and C-SCRM risk management process activities described in the publication. For organizations at the early stage of establishing a C-SCRM program, there is extensive guidance about how to go about doing this in a phased approach that begins with putting the foundational elements in place, then matures and expands upon this 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, and supplemental C-SCRM security control guidance, as well as 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 be complementary to such assessments, though they may use different approaches and cover different areas. Safety assessments are concerned primarily with the physical world. Information security risk assessments primarily look at the digital world. However, in an OT environment, the physical and the digital are intertwined, and significant overlap may occur.

It is important that organizations consider all aspects of risk management for safety (e.g., risk framing, risk tolerances), as well as 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 developed by the information security risk assessment process.

Safety systems may also reduce the impact of a cyber incident to the OT. Safety systems are often deployed to perform specific monitoring and control functions to ensure the safety of people, the environment, process, 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. Ensure adequate separation of components consistent with the risk of compromise. Evaluate the impact of the implemented security controls on the safety system to determine if they negatively impact the system.

4.3 Applying the Risk Management Framework for OT Systems

The NIST Risk Management Framework (RMF) applies the risk management process and concepts (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 Figure 15, while shown sequentially, can be implemented in a different order to be consistent with established management and system development life cycle processes.

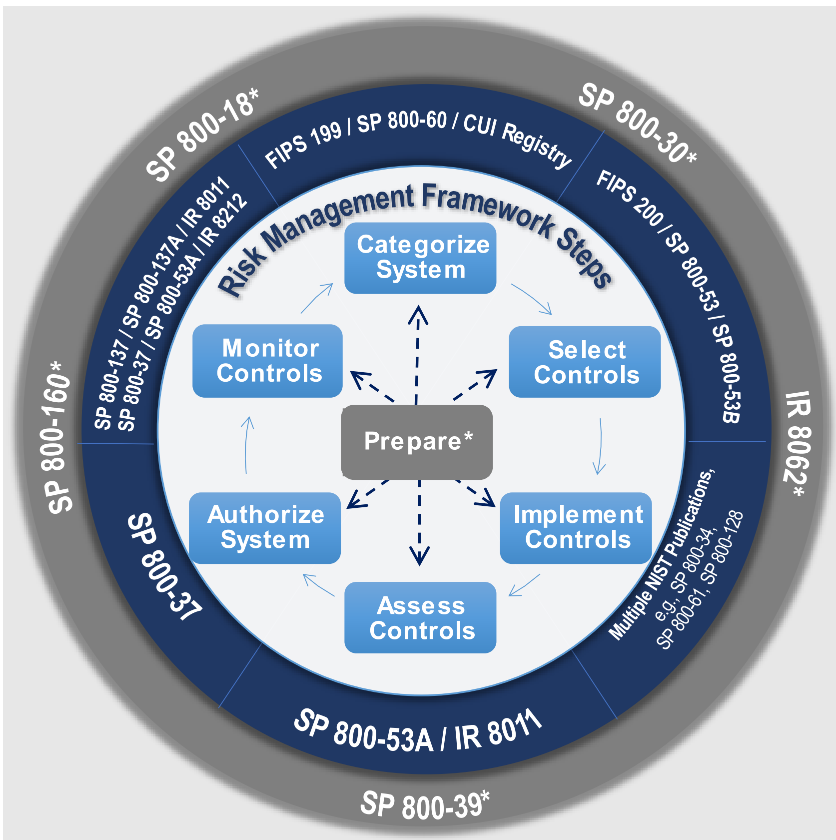

Figure 15: Risk Management Framework Steps

4.3.1 Prepare

The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and system levels of the organization to help prepare the organization to 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. See Table 6 for 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/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 personnel include 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/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 if 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.

Tasks	Outcomes	OT-Specific Guidance
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/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 having an interest in the system are identified. [*Cybersecurity Framework*: **ID.AM**; **ID.BE**]	Example OT personnel include Process/Plant Manager, 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.	

Tasks	Outcomes	OT-Specific Guidance
	[*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 to 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 impact of the loss of confidentiality, integrity, and availability of the information and system is 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 impact should there be a breach of security. It is important to remember that for an OT, availability is generally the greatest concern. 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/business processes. [*Cybersecurity Framework*: **Profile**] Security categorization results reflect the organization's risk management strategy.	OT and IT systems may have different categorization criteria.
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 determine the initial selection of 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 systems determined 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 can be utilized as 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 activity should, as its primary goal, focus on meeting the intent of the original controls whenever possible or feasible. For example, in situations where the OT cannot support, or the organization determines 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 non-automated 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 may leverage an organization-defined control selection approach.
TASK S-2 CONTROL TAILORING	Controls are tailored, producing tailored 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.

Tasks	Outcomes	OT-Specific Guidance
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 the control effectiveness may be necessary due to unique operational, environmental, and/or availability constraints.
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 a security specification and are expected to be incorporated into the systems during the development and implementation phases of the system development life cycle.

In contrast, for legacy systems, the security control selection process is applied from a gap analysis perspective when organizations are anticipating significant changes to the systems (e.g., during major upgrades, modifications, or outsourcing). Since the systems already exist, organizations likely have 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 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 [SP800-53A] 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.	Consider the use of tabletop exercises or simulations to reduce the impact to production OT. Use automation to conduct assessments with care to ensure that the OT system is not

Tasks	Outcomes	OT-Specific Guidance
	Use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.	adversely impacted by the testing process.
TASK A-4 ASSESSMENT REPORTS	Security and privacy assessment reports that provide findings and recommendations are completed.	
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 control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]	Ensure remediation actions do not have a negative impact on the efficiency and safe operations of OT. Consider 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, taking into account planned schedule maintenance or shutdown(s) of the OT system.

4.3.6 Authorize

The Authorize step results in a management decision to authorize the operation of a system and to explicitly accept the risk to operations, assets, and individuals based on the implementation of an agreed-upon set of controls. A new system is not placed into production/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 acceptable range 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 the 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 takes performance impacts and Safety Systems as critical considerations.
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 networks is different: Internet access, email, and remote access will typically be permitted on the corporate network and not allowed on the 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, man-in-the-middle or other network-based attacks). Utilizing separate networks allows greater flexibility to address security and performance requirements between the two environments

Practical considerations, such as digital transformation, 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 these connections. This section outlines security strategies for organizations to consider when architecting their OT environments to support cybersecurity objectives.

5.1 Cybersecurity Strategy

The adoption of a cybersecurity strategy can help organizations with cybersecurity decisions by providing context for decisions that would otherwise be more ad hoc. This can result in a more systematic implementation of risk decisions into the development and operations of systems supporting a comprehensive and sustainable cybersecurity program. 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 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—to proactively identify and rid the system of weaknesses and defects that lead to security vulnerabilities; to proactively understand the certainty and uncertainty of adversarial and non-adversarial threats; and to 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 to ensure that the system is resilient to such events.

OT-specific Guidance and Recommendations

When planning their 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. Also, 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 to cybersecurity in its systems. This approach allows an organization to consider all aspects of the system life cycle, from procurement to decommissioning, with cybersecurity in mind. As a result, the organization can track 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. The organization may, for example, want its systems to display certain characteristics such as resiliency or trustworthiness. A strategy provides a framework that can help incorporate those characteristics into the final systems. The strategy can also include considerations such the flexibility to adopt new technologies (e.g., crypto agility, artificial intelligence [AI]/machine learning [ML] technologies, digital twins). Finally, a 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 Guidance and Recommendations

OT assets are often very long-lived 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 the latest security updates applied, deeply affecting security. Adoption of a security strategy can assist an organization in understanding the life cycle of its OT systems and adjusting approaches to maintain cybersecurity.

5.1.2 Defense-in-Depth Strategy

Defense-in-depth is a multifaceted strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. It’s considered a best practice. Many cybersecurity architectures incorporate the principles of defense-in-depth, and the strategy has been integrated into numerous standards and regulatory frameworks.

The basic concepts are to prevent single points of failure in the 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 Guidance and Recommendations

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 organizations may find that they can be applied to a wide range of OT environments including ICS, SCADA, IoT, IIoT, and Hybrid environments.

Organizations should also consider that 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 required 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 with business networks and cloud infrastructures. Additionally, the introduction of IIoT systems into OT environments may have unintended cybersecurity consequences.

Similarly, cloud computing capabilities such as 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, 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. Also, organizations may find 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 Guidance and Recommendations

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, 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 assist organizations with strengthening their overall cybersecurity defenses. As a result, adversaries may find it increasingly difficult to penetrate the environment without detection. In the following sections, specific defense-in-depth layers are discussed, 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 supporting the OT environment. Sections 3 and 4 discuss the program and risk management considerations for organizations to establish their cybersecurity program. 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. The assets being safeguarded may include control systems, tools, equipment, the environment, the surrounding community, and intellectual property including proprietary data such as process settings and customer information. Organizations may also need to consider additional environmental, safety, regulatory, legal, and other requirements when implementing physical security to protect their environments.

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 creating 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 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 detection of unauthorized access.
- **People and Asset Tracking.** Locating people and vehicles in a facility can be important for safety reasons, and it is increasingly important for security reasons as well. 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 needing assistance, and to support emergency response.

OT-Specific Guidance and Recommendations

Organizations should consider if physical security of remote assets is implemented at differing levels and whether these 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 which, 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 supporting physical security devices (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. While network security can encompass numerous aspects, this section focuses on several foundational elements to assist organizations with planning and implementing their network security capabilities. These include applying network architecture principles of segmentation and isolation; centralizing logging; network monitoring; and malicious code protection. Additionally, this section will discuss 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 segment and isolate IT and OT devices. Organizations should begin this process by considering how to characterize devices. For example, devices might be segmented based on management authority, level of trust, functional criticality, data flow, location, or other logical combinations. Organizations might also consider using an industry-recognized model such as the Purdue Model [Williams], ISA-95 Levels [IEC62264], Three-Tier IIoT System Architecture [IIRA19], or a combination of these models to organize their OT network segmentation. An additional network segmentation option for organizations to consider is incorporating the concept of a Demilitarized Zone (DMZ) as an enforcement boundary between network segments as depicted in Figure 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.

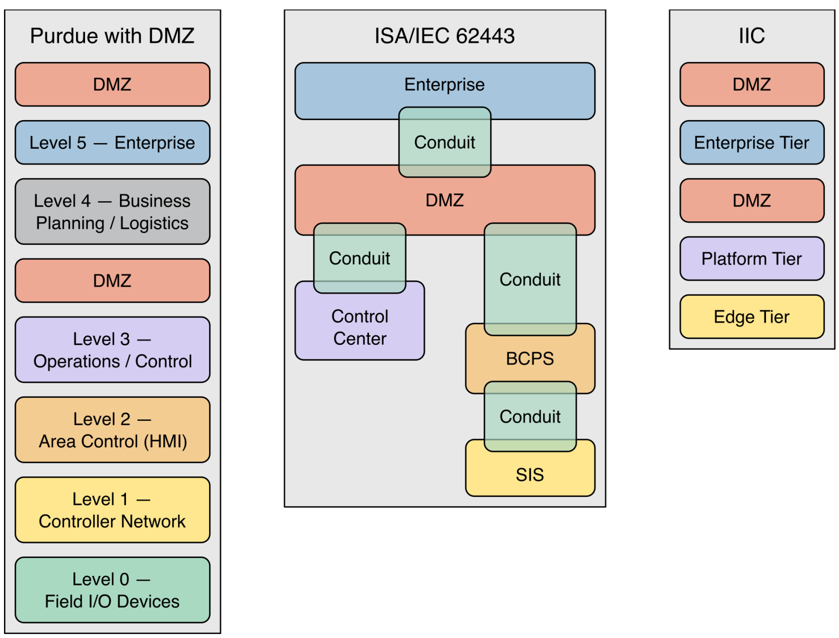

Figure 16: High-level example of Purdue Model and IIoT Model for network segmentation with DMZ segments

OT-Specific Guidance and Recommendations

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 communication between levels, tiers, or zones. When organizing assets, organizations should consider how the zone and isolation configuration impact day-to-day operations, safety, and response capabilities.

When properly configured, network architectures are used to support segmentation and isolation through 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 in the policy engines of the network devices to support monitoring communication between segments and permitting only authorized communications. Network devices such as switches, routers, firewalls, and unidirectional gateways/data-diodes that support traffic enforcement capabilities can be used to implement network segmentation and isolation.

Firewalls are commonly used to support network isolation and are typically 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 Guidance and Recommendation

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 utilizing 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 or the Industrial IoT Consortium (IIC) architectures as well.

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 will want to 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 might protect the 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 devices such as 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 Guidance and Recommendation

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

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

5.2.3.3 Network Monitoring

Network monitoring involves organizations 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), or Intrusion Detection/Prevention systems (IDS/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

Additionally, organizations may 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 Guidance and Recommendation

OT system traffic is typically more deterministic – repeatable, predictable, and designed – than IT network traffic. Organizations may leverage the deterministic nature of OT environments to support network monitoring for anomaly and error detection.

Organizations may want to 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 (listen/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 not be able to determine if encrypted network communication is malicious and could either generate false positive or false negative alerts for the traffic. Changing the data collection point to capture network traffic either before or after encryption (e.g., using host-based network monitoring tools) could assist with improving monitoring capabilities when encrypted communication is expected.

IDS and IPS products are effective in detecting and preventing well-known Internet attacks, and some IDS and IPS vendors have incorporated attack signatures for various OT protocols such as Modbus, DNP3, and ICCP. An effective IDS/IPS deployment typically involves both host-based and network-based capabilities. Organizations should consider the impact automated responses associated with IPS might 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 instead of in-line network taps that could create a communication point of failure. 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 the addition of the tools does not adversely impact operational performance or safety.

5.2.3.4 Zero-Trust Architecture (ZTA)

ZTA is a cybersecurity paradigm focusing 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, along with 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 ZTA and, instead, may need to integrate several technologies with varying maturity levels to support their environment.
- Migrating an existing environment may require more investments in time, resources, and technical ability to implement zero-trust principles.

OT-Specific Guidance and Recommendations

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 ZTA on 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 the impact on operations and safety function. For example, would any adverse impacts occur 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 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 provide hardware implementation for Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA). Overall, hardware security capabilities provide the capability to 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 Guidance and Recommendations

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 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 Guidance and Recommendations

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 the rules and settings properly support the organizational security objectives.

5.2.5.2 Patching

Patches have two main purposes: to fix vulnerabilities and to enhance functionality. While enhancing software functionality is important, in the context of defense-in-depth software security, the focus of patching is associated with reducing vulnerabilities. As a result, patch management is a defense-in-depth capability to support 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 the patches do not impact operational capabilities or safety. OT operational requirements can also impact the frequency patches are applied. For example, some OT environments must run nearly continuously for extended periods of time or have small maintenance windows when approved updates could be applied. 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 investigating 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.

OT-Specific Guidance and Recommendations

Whenever possible, patches should be tested on a sandbox system (test environment) to ensure they do not cause problems before being deployed to 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, or 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

For organizations developing in-house systems and components, policies and procedures to support and validate secure code development practices should be incorporated 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 industry 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 for cybersecurity settings supporting both secure configurations and application hardening is important to meet organization and regulatory security requirements. These settings may include setting access controls for restricting 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 running on the system.

Encrypting data that flows over networks (in transit) or data stored in memory and hard drives (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 choice on where to include encryption in the defense-in-depth strategy.

OT-Specific Guidance and Recommendations

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), for securing the data.

Encryption can also be used on hard drives to protect information at rest. Full disk encryption is recommended for portable laptops and devices. Organizations may also want to consider encrypting folders containing 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 if an encrypted packet is malicious, resulting in either false-positive or false-negative alerts.

5.3 Additional Cybersecurity Architecture Considerations

When establishing a security architecture for supporting OT and IIoT environments, 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. 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 isolation of safety systems from other OT systems, is required. Additionally, safety requirements can influence 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 (e.g., 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 destruction to property and avoids cascading event or secondary hazards. Cyber-related events such as the loss of network communications could trigger these fail-safe events. To minimize false positives, define the thresholds that OT components can operate at with reduced or disrupted capabilities such as lost network communications.

5.3.2 Availability Considerations

Operational continuity management requires managing availability at multiple levels – data, applications, IT infrastructure, power, and other supporting utilities such as HVAC, water, steam, compressed air, etc. 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.

Data, Applications, and Infrastructure

Architecture requirements and design should support the redundancy needs of the 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 take into consideration any redundant communication and protect it to the same security level as the primary.

Additionally, a data backup and restoration process will facilitate speedy recovery of systems in case of data 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 list (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. Periodic testing of data backup and restore capabilities will ensure that they will be available when the need arises.

Primary and Alternate Power Sources

Architectural considerations should include the impact of power outage for 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 need to 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. Appropriate cybersecurity practices should be implemented to protect these systems from cyber-attacks.

Other Utilities

Industrial facilities typically have monitoring and controls systems that manage uninterruptable power supplies (UPSs), HVAC, fire alarm systems, boilers, cooling water plant, steam, compressed air, etc. These monitoring and controls systems are also vulnerable to cyber-attacks and can affect the OT systems. Appropriate cybersecurity practices should be implemented to protect these systems from cyber-attacks.

OT-Specific Guidance and Recommendations

Disaster recovery planning is another important activity for OT systems, especially where there are safety concerns. Organizations should establish and maintain a disaster recovery plan (DRP) detailing 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 also 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 of the critical infrastructure industries have sites that are geographically distributed. Organizations should consider if 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 Guidance and Recommendations

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 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, the organization should consider whether security operation will be managed from a central security operations center (SOC) or from regionally distributed SOCs. 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.1.9.1) provides cybersecurity architecture requirements for bulk electric systems. Similar requirements and guidance exist for other regulated industries.

5.3.5 Environmental Considerations

Organizations should consider whether any of their processes and equipment pose environmental hazards. The hazard analysis will typically provide this information. If an environmental hazard has been identified, organizations should consider architectural measures to prevent environmental hazard due to cybersecurity failure.

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) do not have the ability to be authenticated. Without authentication, there is the potential to replay, modify, or spoof data. Organizations should make a risk-based decision considering 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, 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 Guidance and Recommendations

In addition to security architecture considerations, organizations may also need to consider the impact to policy management, enforcement, and governance to support IIoT. Additionally, integration of IIoT in OT environments may require a tighter collaboration between IT and OT security teams for managing the security operations. For example, real-time situational awareness should be shared between IT and OT security teams.

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 – for example, due to the increased communications requirements or the use of additional services such as cloud systems to support operational requirements.

OT-Specific Guidance and Recommendations

Organizations should consider the endpoint security capabilities of the IIoT devices being deployed. For example, the IIC suggests that organizations consider the following security capabilities:

- Endpoint tamper resistance capabilities
- Endpoint root of trust
- Endpoint identity
- Endpoint access control
- Endpoint integrity protection
- Endpoint data protection
- Endpoint monitoring & analysis
- Endpoint configuration and management

- Cryptographic techniques
- Capability to harden endpoints

Cybersecurity Capability Considerations

Compute resources including processing, memory, and storage vary among IIoT devices. Some IIoT devices may have constrained resources and others may have unused capabilities. Both cases 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 if 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 (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 will expand on the general OT and IIoT environments described in Section 2 to provide examples for how the general 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.

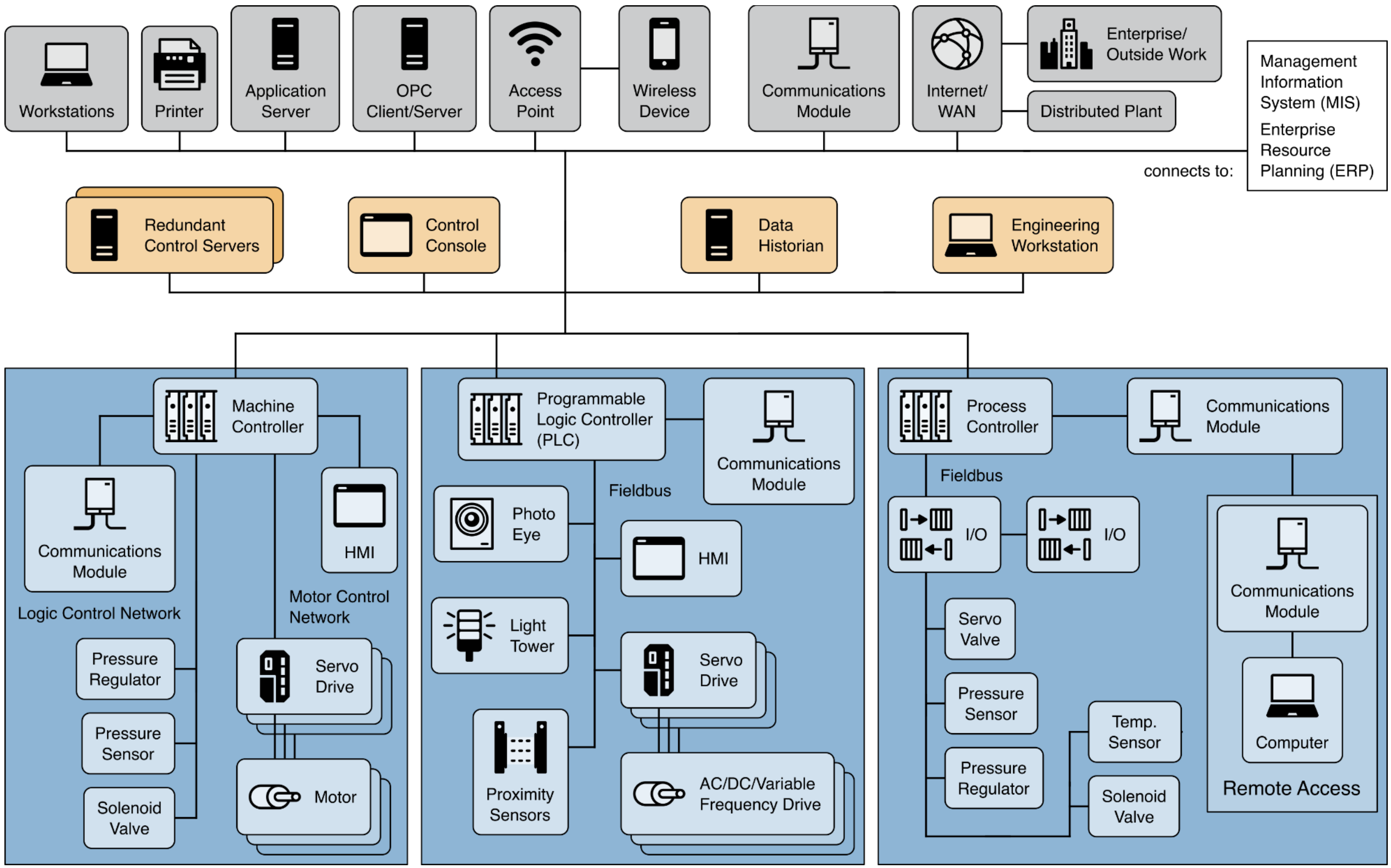

Figure 17: DCS implementation example

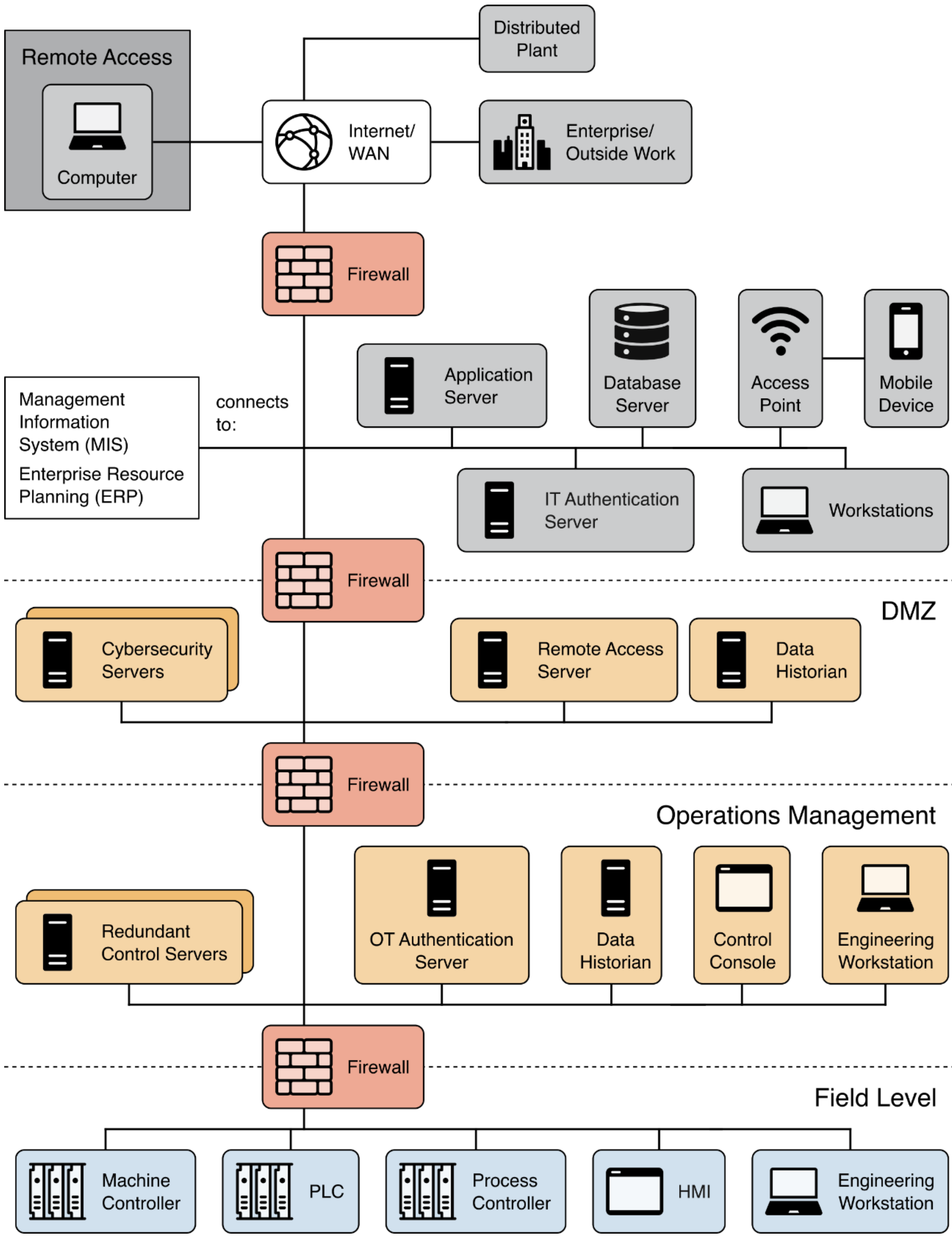

Figure 18: Defense-in-depth security architecture example for DCS system

For the Figure 18 example, the assumption is that the organization has already addressed Layer 1 – Security Management and Layer 2 – Physical Security. For Layer 3 – Network Security, the organization should consider incorporating the following capabilities in 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 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 includes the Purdue level 3 components. The DMZ includes devices that support bridging the operations management and enterprise tiers. Organizations should also consider if additional network segments are required for safety or security systems (e.g., physical monitoring and access controls, doors, gates, cameras, Voice over IP [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 within the DMZ that allow pivoting to the OT environment without detection.
- The security architecture diagram shows an IT authentication server in the Enterprise network to authenticate users in the Enterprise network, 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 – Hardware Security, and Layer 5 – Software Security, 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 from the devices. For example, a web server or SSH server may be available in some newer-model 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.

5.4.2 DCS/PLC-Based OT with IIoT

Building on the guidance for DCS/PLC-based OT environments in Section 5.4.1, Figure 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 different communication and architectural components supporting 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, allowing 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.

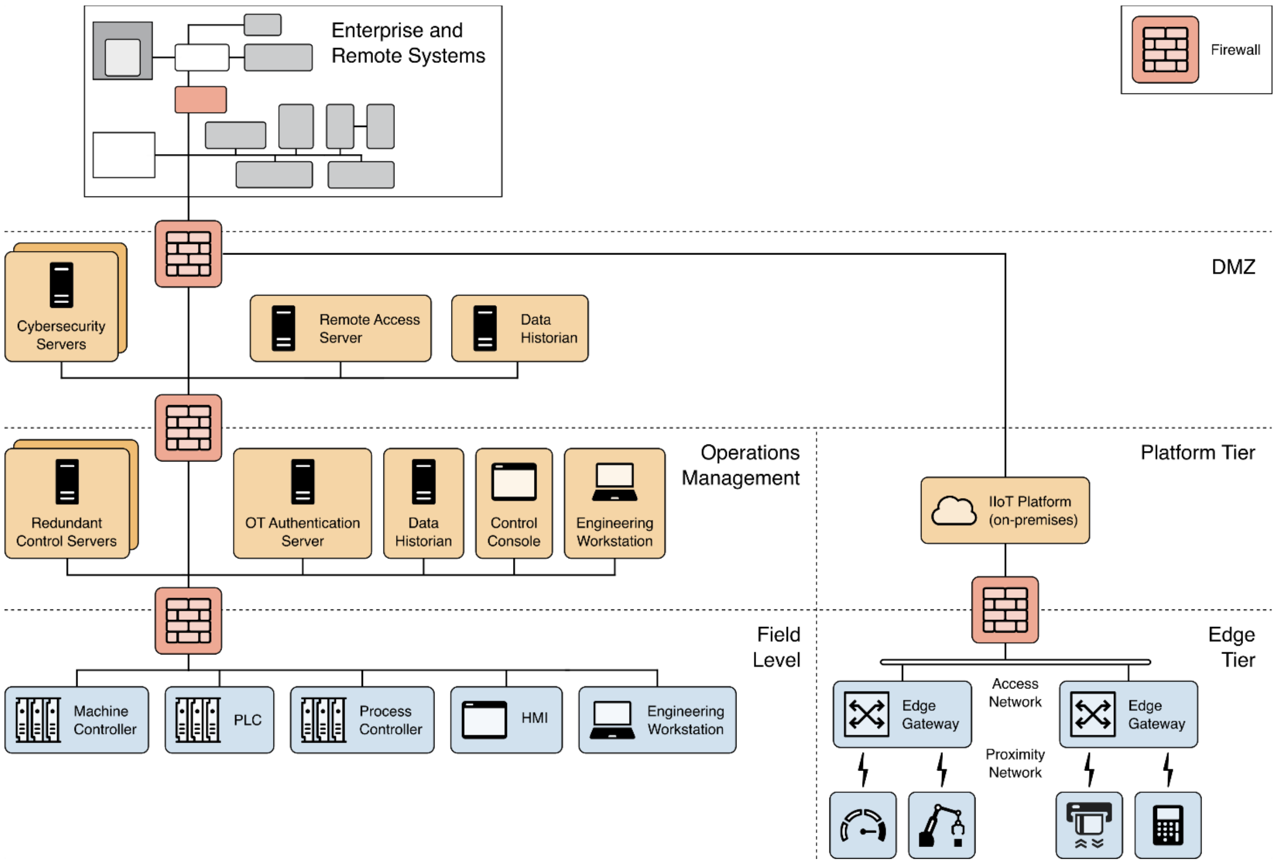

Figure 19: Security architecture example for DCS system with IIoT devices

Alternatively, some organizations may use cloud services for their IIoT platform. In this case, organizations should consider how to secure communications from the edge to the cloud IIoT platform. Organization should also consider routing the communication through the DMZ boundary firewall to manage and monitor them.

5.4.3 SCADA-Based OT Environments

An example implementation showing the components and general configuration of a SCADA system is depicted in Figure 20. 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.

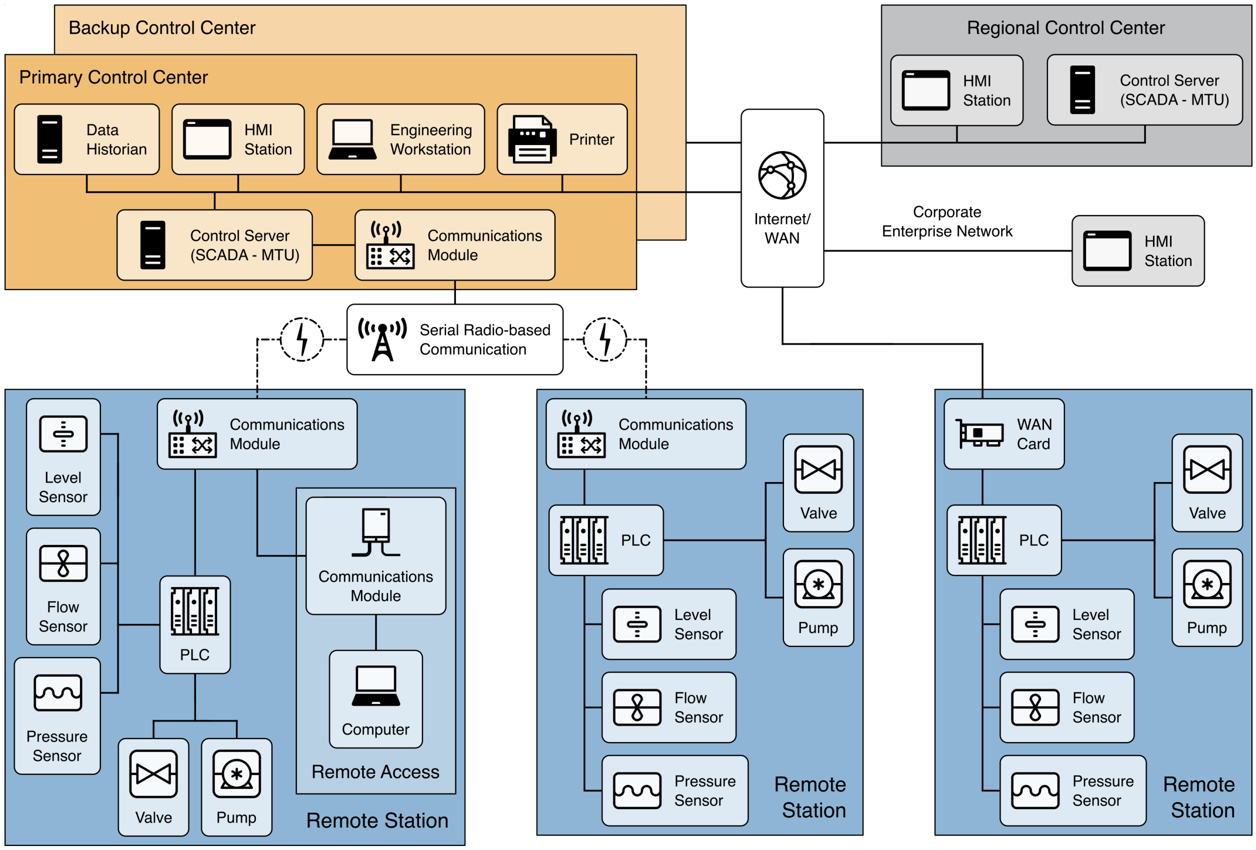

Figure 20: An example SCADA system in an OT environment

Figure 21 shows an example defense-in-depth implementation for the example SCADA system. For this example, the assumption is that the organization has already addressed Layer 1 – Security Management and Layer 2 – Physical Security. For Layer 3 – Network Security, the organization should consider incorporating the following capabilities in the security architecture:

- Separate networks into different zones or regions; it is an important step in applying a defense-in-depth strategy in the 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, enhancing 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 connection. Devices in the network segments should only connect to other segments through the secure connection and should be restricted in 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 pivoting to the OT environment without detection.

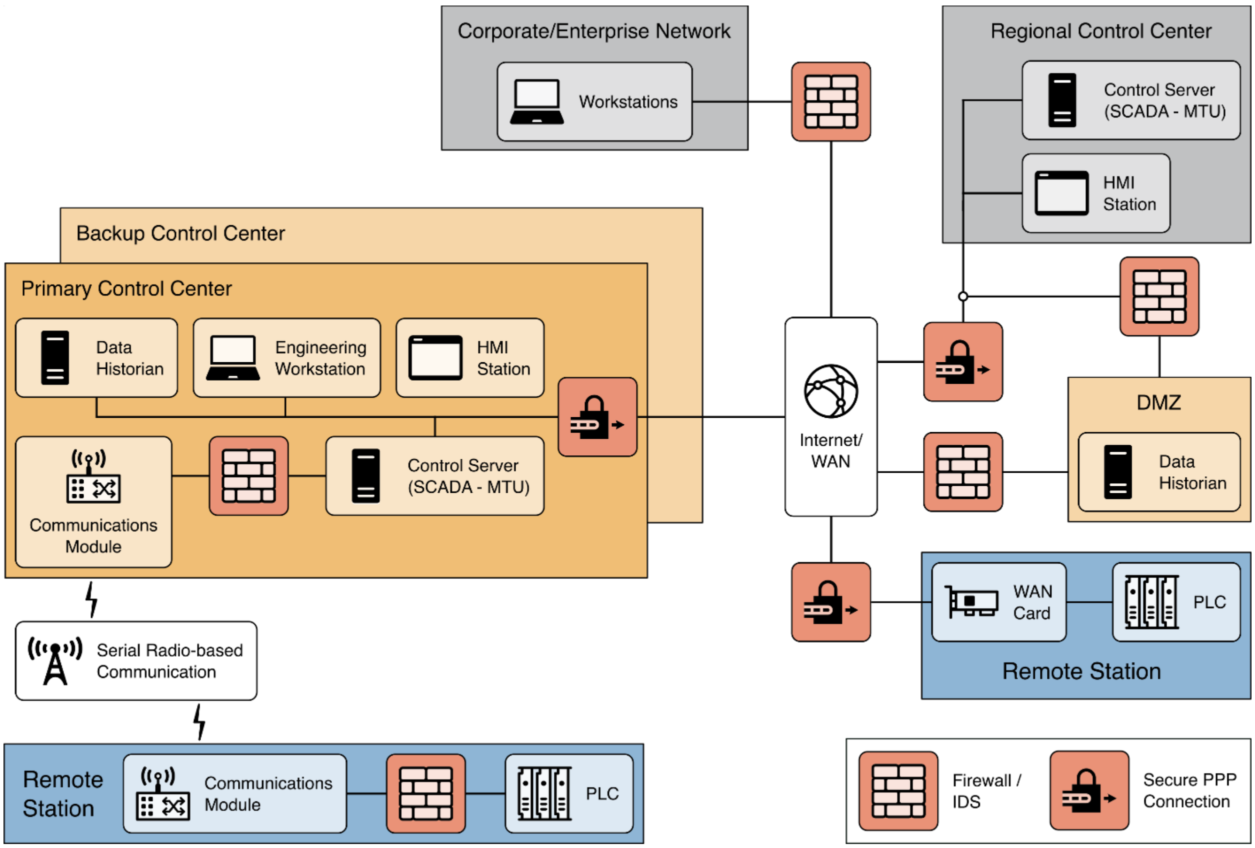

Figure 21: Security architecture example for SCADA system

For Layer 4 – Hardware Security, and Layer 5 – Software Security, 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 from the devices. For example, a webserver or SSH server may be available in some newer-model 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] as a means for guiding cybersecurity activities and considering 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 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.

All CSF Functions and selected CSF Categories and Subcategories are covered in this section. 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 risk to systems, people, assets, data, and capabilities.

6.1.1 Asset Management (ID.AM)

The ability for organizations to properly and consistently identify and consistently 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 environment 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 might include vendor, model, serial number, purchase information, and manufacturing/build information (e.g., provenance information).
- Software and firmware inventory management to track software and firmware installed with the OT components, including version numbers and location information, Software Bill of Materials (SBOM), etc.
- Vendor information to establish a repository of vendor information, points of contact, warranty information, locations of recall and update information, etc.
- 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 if 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 enable a manufacturer to understand the flow of data between networked components. Documenting data flows enables organizations to understand expected behavior of their networks. This understanding of how devices communicate assists with troubleshooting as well as response and recovery activities. This information can be leveraged during forensic activities or used for analysis to identify anomalies.

OT-Specific Recommendations and Guidance

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

6.1.1.2 Network Architecture Documentation (supports the outcome of ID.AM)

Network architecture documentation tools enable a manufacturer to 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 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 are only able to 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. Manual processes may be required to document these components.

Asset owners may also want to consider how automated scanning activity 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 utilizing physical inspections of OT network connections or analysis of 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 organization leadership incorporating risk management objectives along with resiliency, privacy, and cybersecurity objectives into the strategic planning process and providing the required resources to effectively implement and sustain the cybersecurity program. From this process, organization leadership develops and disseminates policies establishing security requirements for their environments. These policies include, for example, the identification and assignment of roles, responsibilities, management commitment, and compliance. The policies may also reflect coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring).

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*
- NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*

OT-Specific Recommendations and Guidance

Organizations should consider:

- Ensuring the cybersecurity program is provided sufficient resources to support the organization's IT and OT risk management strategy
- Ensuring that policies take into consideration the full life cycle of the OT systems
- Ensuring that legal and regulatory cybersecurity requirements affecting the OT operations are understood and managed

- Establishing one or more senior official positions with responsibility and accountability 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 resulting from cyber-incidents such as unauthorized access, use, disclosure, disruption, modification, or destruction of an information system or data. Organizations should consider the frequency for updating risk assessments and testing 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/financial impacts. As a result, organizations may find that determining a cost-to-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 loss of power, loss of control, loss of upstream feed, loss of downstream capacity, and 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 to include 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:

- Monitoring security groups, associations, and vendors for security alerts and advisories
- NVD for detailed information on known vulnerabilities for hardware and software assets

Threat information relevant to the environment can be obtained from both internal resources as well as 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/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*
- NISTIR 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 involving 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 are 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/ongoing 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 insertion of counterfeits, unauthorized production, malicious insiders, tampering, theft, and 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 the relationships or dependencies on other components. Having this information available can help an organization determine if 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*
- NISTIR 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 allow determining the authenticity of vendor-provided OT hardware, software, and firmware. Organizations should also consider if 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 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)

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 to identify and authorize a person, process, or device before granting physical or logical access to resources such as the system, information, or location being protected positively and uniquely. Access controls represent the policies, processes, and technology for specifying the use of system resources by only authorized users, programs, processes, or other systems. PR.AC controls allow organizations to manage the 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 consider the centralization of identification and authentication for users, devices, and processes within the OT environments to improve/reduce burden account management and enhance monitoring capabilities. Common network technologies such as Active Directory and, more generally, Lightweight Directory Access Protocol (LDAP) or similar technologies can be utilized to support centralization of identity management across environments. If authenticated accounts from the IT environment have access within the OT environment, organizations should weigh the increased risk from permitting that versus the benefits of using centralized accounts.

In situations where OT cannot support authentication, or the organization determines it is not advisable due to adverse impacts on performance, safety, or reliability, the organization should select compensating countermeasures, such as 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 systems, data, and networks of the organization. ACLs are sometimes used to support logical access controls. An ACL is one or more rules for determining whether an access request should be granted or denied; they are used to support the principle of least functionality and control access to restricted areas. They 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. An ACL 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.

Another technology for supporting logical access controls is called Role-Based Access Control (RBAC). 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 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 attributes associated with subjects (requesters) and the objects being accessed. Each object and subject have a set of associated attributes, such as location, time of creation, access rights, etc. Access to an object is authorized or denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and of 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 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.
- Implement solutions that provide credential management, authentication and 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 should be designed to minimize latency or delays in processing OT system access or commands.
- Implementing 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, plus ABAC integrated into physical security to sensitive areas may achieve the risk-based access control requirements for an organization.

6.2.1.2 Physical Access Controls (PR.AC-2)

Physical security controls are any physical measures that limit physical access to assets. These measures are employed to prevent many types of undesirable effects including unauthorized physical access to sensitive locations; 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.

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

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 if 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 creating 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 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 detection of unauthorized access.
- **People and Asset Tracking**. Locating people and vehicles in a facility can be important for safety reasons, and it is increasingly important for security reasons as well. 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 needing 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 be connected to OT devices or networks.
- **Cabling**. Unshielded twisted pair communications cable, while acceptable for the office environment, may not be suitable for some OT environment due to its 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, and conduits in addition to labeling to clearly delineate OT and IT network segments and reduce the risk of potential cross-connections.
- **Control Centers / Control Rooms**. Providing physical security for control centers/control rooms is recommended to reduce the potential of many threats including unauthorized access. The 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 for supporting 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/control rooms to be blast-proof, or to provide an offsite emergency control center/control room so that control can be maintained if the primary control center/control room 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 supports enforcing 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 communication between segments that has been explicitly authorized.

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 supporting 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. Additionally, this activity might 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 for supporting network isolation, modern firewalls such as stateful and deep packet inspection devices and devices specifically designed to support OT environments should be considered. 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.

Organizations should keep in mind that network isolation devices might 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 which 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)

6.2.1.4.1 Physical Token Authentication

The primary vulnerability that physical token authentication addresses is easily duplicating a secret code or sharing it with others. It eliminates the all-too-common scenario of a password to a "secure" system being on the wall next to a PC or operator station. 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. 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. Traditional passwords can become lost or stolen without notice, leaving credentials more vulnerable to exploitation.

Common forms of physical/token authentication include:

- Traditional physical lock 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 largest weakness is that physically holding the token means access is granted (e.g., anyone finding a set of lost keys now has access to whatever they open). Physical token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used along with the token.

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

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 the security level.

Noted issues with biometric authentication include:

- Distinguishing a real object from a fake (e.g., how to distinguish 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 (the probability of rejecting a valid biometric image, and the probability of 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 on safety glasses and/or gloves and industrial chemicals may impact biometric scanners.
- 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 [SP800-76].

OT-Specific Recommendations and Guidance

While biometrics can provide a valuable authentication mechanism, organizations may need to carefully assess this 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 about 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 could issue hundreds of 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 involving authentication, digital signatures, and key exchange from other parts of the system that do not have a need to know
- Enabling 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 to replace lost or stolen cards.

OT-Specific Recommendations and Guidance

Although smart cards offer useful functionality, in an OT context their implementation 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 capability 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 management of 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 take into consideration 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 allowing organizations to use the same credential mechanism in multiple applications with one to three factors for authentication (Card-Only, Card+PIN, Card+PIN+Biometric) depending on the risk-level of the resource being protected. 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 [SP800-73] and employ either cryptographic verification or biometric verification.

6.2.1.4.4 Multi-Factor Authentication

Organizations should consider that there are several possible factors for determining the authenticity of a person, device, or system, including something you know, something you have or something you are. When two or more factors are used, the process is known generically as multi-factor authentication (MFA). In general, the more factors that are used in the authentication process, the more robust the process. For example, authentication could be based on something known (e.g., PIN number or password), something possessed (e.g., key, dongle, smart card), or something you are such as a biological characteristic (e.g., fingerprint, retinal signature).

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 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 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 that need to know. Organizations may want to consider using a password management tool that is secure and accessible by those that need to know.

Some OT OSs make setting secure passwords difficult, as the password size is smaller than current password standards and the system allows only group passwords at each level of access, not 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 logon can result in policies such as auto-logoff timeout and administrator password replacement being pushed down, and that can be detrimental to the operation of the OT system.

The following are general recommendations and considerations with regards to the use of passwords.

- Change all default passwords in OT components.
- Passwords should have appropriate length, strength, and complexity balanced between 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 delayed access during critical events. Organizations should consider physical or network isolation for devices where password protection is not recommended.
- Copies of shared or master 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 protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks.

2798

6.2.2 Awareness and Training (PR.AT)

The Awareness and Training category provides policy and procedures for ensuring that all users are provided 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 OT-specific security awareness and training for the environment and specific applications. In addition, organizations identify, document, and train all personnel having 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 and identifying anomalous behavior in the OT environment, guidance on 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 responsibility should be provided training, but the training 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.

Use of cryptography can support data security requirements. Encryption, digital signatures, hashing, and other cryptographic functions are available to prevent unauthorized access or 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] 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 file types and data to protect (both physical and electronic) 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/computer aided manufacturing files, operating manuals and documentation, electrical diagrams, network diagrams, historical production data [NISTIR 8183]). Organizations should consider centralizing critical data within secure storage locations.

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

Information flows from the OT security domain to other security domains, and connections between security domains are monitored. 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 consideration for wiping, sanitizing, or otherwise destroying critical data and media prior to disposal. The asset disposal program should include any removeable media and mobile devices as well as 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). First identify which data is critical, then implement cryptographic mechanisms (e.g., encryption) to prevent unauthorized access or 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 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. Degradation of performance of the end device or system caused by encryption, or any other security technique, should be considered. Before deploying encryption within an OT environment, solutions should be tested to determine if 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/decryption devices, anomaly detection tools supporting OT environments may not be able 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, which 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 if cryptographic protection with remote key management may be beneficial, such as when the units being protected are 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 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 entails configuring systems to only provide essential functions and services. Some of the functions and services routinely provided by default 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 may not be necessary for their proper operation, some of which may be enabled by default and without knowledge of the organization. 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 to 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, allowing organizations 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 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. Additionally, organizations should establish the system development life cycle (SDLC) approach to document, test, and approve changes before deploying 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 allow organizations to prevent accidental reconfiguration or identify intentional reconfiguration of components to unapproved or untested versions.

In some cases, the use of automated configuration management tools might 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 consider potential impact to the OT system. In some cases, these tools transfer numerous types of data over the manufacturing system network, and potentially large amounts of data. 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 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 should be developed of all backups maintained, including installation media, license keys, and configuration information. Additional measures should be taken to ensure that backups are readily available when needed:

- Verify the backups for reliability and integrity (if technically possible).
- Establish an onsite location for backups that is accessible to all personnel who may need access during a recovery event.
- Establish an alternative secondary storage location for additional copies of backups to ensure that the same incident that disrupts primary data cannot modify or destroy the backup (e.g., store PLC logic and configuration files at an offsite, geographically diverse location that cannot be destroyed by the same [hurricane, wildfire, tornado] that may destroy the PLC).
- Include testing of restoration process from backup data as part of contingency plan testing.
- Ensure 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 implement 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. This is particularly important 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, the environments containing 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).

  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 significantly increased roles in security 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 be a few seconds; however, if the site relies on external power, the UPS battery life may need to be hours. It should be sized, at a minimum, 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 establish a regular review and update for 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, along with 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 may involve typical time spans of days, weeks, or months to recover from a natural disaster, or minutes or hours to recover from a malware infection or a mechanical/electrical failure. Business continuity plans (BCP) 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 requiring 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 deal with 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 it 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 describing 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 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 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 comprising 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 it is readily available during any type of disaster. The disaster could be natural, environmental, or caused by humans, either 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 and should consider leveraging existing plans when developing a response plan for cybersecurity events.

Supplemental guidance for the 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 Security Tip (ST13-003), *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 items:

- **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.** There are several responses that can be taken in the event of an incident. These 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 documenting 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 the various organizations. If there are reporting requirements, these should be documented along with contact information and reporting format to reduce confusion.

  Response actions should include steps for Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activity. Some considerations for OT may include:

  - Determining a priority: either returning to normal operations as quickly as possible, or performing an investigation and preserving forensic data
  - Communicating to 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 effect of both 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. As an example, the focus may be to recover the systems supporting critical utilities prior to the systems supporting manufacturing based on the order of start-up activities.

Testing recovery plan procedures for OT components could 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. Organizations at a minimum 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 maintenance tools (both local and remote) and 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, ensuring maintenance logs or changes performed 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.

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 hashes of installers).

Any maintenance performed on an OT device can inadvertently modify its configuration, resulting 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 only 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 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 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 the security capabilities as threats evolve and change; as such, organizations should manage the technical solutions securing 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 occurring 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. The typical types of 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 include identification of the device that generated the event, the timestamp of the event, and identification of the user or system account that generated the event. In general, each log entry should 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. Log size may grow quickly depending on the frequency of events being logged, resulting in increasing space utilization. Disk space and memory is limited on most OT devices, so adequate storage should be provided either locally or remotely 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 specific 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. For example, if an adversary gains access to media containing OT data, it could provide 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 organization personnel security program should be developed to include policy, position risk designations, personnel screening, terminations and transfers, access agreements, and third-party roles and responsibilities. OT personnel should be in communication with Human Resources, IT, and Physical Security as necessary to ensure personnel security requirements are being met.

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

Additionally, training programs should be developed to ensure that each employee has received training relevant and necessary to 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 Wireless Fidelity (WiFi) 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 (wired) communication capabilities. However, RF communications are also more susceptible to interference and may also allow eavesdropping by unauthorized personnel.

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 utilizing wireless communication should be placed in a separate network segment and only be deployed where the residual risks to health, safety, environmental, and financial implications are low.

Prior to installation, a wireless survey should be performed to determine antenna locations and signal strength to ensure adequate coverage and to minimize exposure of the wireless network to interference from OT environmental factors and eavesdropping. Organizations should consider that 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. The encryption must not degrade the operational performance of the end devices. Encryption at OSI Layer 2 should be considered, rather than at Layer 3, to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered.
- Wireless access points should establish independent network segments (not extend 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 supporting 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 encryption is used between field instruments and wireless access points
- Allowlisting devices into the wireless device manager so 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 appropriate for the application.

6.2.10 Remote Access

When accessing systems or data remotely, security controls should be implemented to prevent unauthorized access to the organization’s networks, systems, and data. A virtual private network (VPN) is a set of technologies and 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 implemented today are:

- **Internet Protocol Security (IPsec)**. IPsec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion (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 HTTP traffic; this protocol implementation is known as HTTP Secure (HTTPS). However, TLS is not limited to HTTP traffic; it can be used to secure many application-layer programs.
- **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. SSH 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 Guidance and Recommendations

Many OT security architectures are designed with multiple levels, such as in the Purdue Architecture. 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 only what is required to meet the business need. Remote access should not circumvent or negate safety or security controls.

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 secure connections are being utilized.

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

- Users/protocols (e.g., RDP, SSH) temporarily permitted through the OT/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/firmware to the latest versions
- Removing access when no longer required. Consider implementing automatic timers for removing access, or the management of change processes to manually confirm removal of access.
- Monitoring remote activities
- Ensuring 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. It should be noted that sometimes modem connections are part of the legal support service agreement with the vendor (e.g., 24x7 support with 15-minute response time). Personnel should be aware that disconnecting/removing the modems may require that contracts 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 onsite 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. Vulnerabilities are flaws that can be exploited, enabling unauthorized access to systems or enabling users to have access to greater privileges than authorized.

A systematic approach to managing and using software patches can help organizations to 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; in addition, they can save time and money that might be spent in responding to vulnerability-related incidents.

NIST SP 800-40 Revision 4 [SP800-40] 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 reduction of risk. The 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 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; consequently, 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 of known vulnerabilities within their OT environment. An organization is responsible for staying informed of its OT vulnerabilities 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, Cyber Security - System Security Management System Security Management; 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*
- NISTIR 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, 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 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 where 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 appropriate activities are developed and implemented.

6.3.1 Anomalies and Events (DE.AE)

Organizations should understand the different events and anomalies and their potential impact to the systems, organization, and 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 that 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 disabled security controls
- Requests for information about the system or architecture (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 follow-up investigation. Organizations should define incident alerting thresholds and response requirements for the events and anomalies affecting 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 and alarm on organization- or environment-specific events. 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. Also, organizations should 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 also 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 if additional controls, such as identifying the use of shared credentials using physical access monitoring, are required.

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 for supporting vulnerability or patch management or for validating device configurations. Solutions that perform active scanning or use local resources to support automation should be subjected to testing before deployment to 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. As an 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 if 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/layer 4 firewalls.

When using third parties for continuous monitoring of 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), or Intrusion Detection/Prevention systems (IDS/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)*
- NISTIR 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, thereby improving security. 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 the normal state.

Gaining access to network traffic is typically performed with switched port analyzer (SPAN) ports and network taps. SPAN ports are a feature in network devices that can logically duplicate and forward select network traffic to a network monitoring solution. Taps are bump-in-the-wire network devices that duplicate traffic from a single physical link. For both types of sensors, care should be taken as performance impacts to the OT system may result from their use.

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.

Regardless of the type of network sensor, all sensors should be subjected to extensive testing and be implemented in a test environment before being deployed to 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) occurring within a system. Monitoring users and systems helps to ensure 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 that no policy violations or cyber incidents have hindered its operation. Strong device monitoring, logging, and auditing is necessary to collect, correlate, and analyze security-related information, resulting in actionable communication of 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. It is generally suggested these solutions 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 is dependent 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 be implemented in a test environment before being deployed to devices in the OT system. Concerns include performance impacts of host-based agents on devices, impact of active scanning on devices, and 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 they consume from the host.

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 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 security practice 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 for testing 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, Linux systems, etc., used as engineering workstations, data historians, maintenance laptops, and backup servers can be secured like commercial IT equipment: install 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-good vendor sites to the OT antivirus servers to 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 it different from a standard PC. Perform testing of 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 requiring ongoing antivirus updates, such that signature updates can be performed without impact to 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 in an offline environment prior to implementing 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)

Detection process includes maintaining and testing processes, procedures, and tools to ensure anomalous events are identified in a prompt manner and responsible parties (individuals) are alerted and help accountable for adequate response. To ensure ongoing awareness of anomalous events: define roles and responsibilities to ensure 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 Response 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 details associated with executing the documented response plans. This may help organizations during the post-incident review process to identify gaps or potential opportunities for improvement in the response plan. Due to time sensitivity of response efforts, if capturing execution details impacts safety or increases the time to complete the response plan, organizations may want to consider other techniques such as reviewing logs, reviewing video footage captured during the response activities, or interviewing response personnel.

6.4.2 Response Communications (RS.CO)

Response to a cybersecurity incident includes coordination 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 that have been trained on incident response. The FEMA National Incident Management System (NIMS) can be used to standardize on 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 / 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.

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 a role or roles 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
- Public relations and legal personnel

External Industry Partners

- OT technical support (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 to 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 nondisclosure 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 are available to be held on retainer in case of an OT incident.

6.4.3 Response Analysis (RS.AN)

Analyses of cybersecurity incidents are conducted to ensure effective response and recovery activities, consistent with the detection process and the response plan. Analysis includes reviewing notifications and determining if further investigation is required, understanding the potential impact, 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 affecting 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)

Activities are performed to prevent expansion of the incident, mitigate its effects, and resolve the incident. Mitigation activity 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 onsite (e.g., remote shutdown or disconnects).

Cyber incident mitigation may involve process shutdowns or communication disconnects that have impact to 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. It is recommended to designate an individual(s) 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 resilience of systems 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 if any gaps or potential opportunities for improvement in the recovery plan should be considered. Due to time sensitivity of recovery efforts, if capturing execution details impacts safety or increases the time to complete the recovery plan, organizations may want to consider other techniques such as reviewing logs, reviewing video footage captured during the recovery activities, or interviewing recovery personnel.

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 develop 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/warehouse personnel

External Communications

- OT vendors
- Security companies that may be held on retainer for response and recovery efforts
- Storage/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://collaborate.mitre.org/attackics

[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.CSWP.04162018

[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 (2013) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 186-4. https://doi.org/10.6028/NIST.FIPS.186-4

[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) 197. https://doi.org/10.6028/NIST.FIPS.197

[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 (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-2. https://doi.org/10.6028/NIST.FIPS.201-2

[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] Industrial Internet 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://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6859.pdf

[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 Interagency or Internal 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, 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.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[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.01162020

[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, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[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

[SP800-53Ar4] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[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—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 Shut Down
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 & 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	Industrial Internet 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
NISTIR	National Institute of Standards and Technology Internal Report, 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 Systems, 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 & Development
RAS	IEEE Robotics & 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
WiFi	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 [RFC4949] (adapted)	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.
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 [ANSI-ISA-5-1]	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.
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 [FIPS200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization [RFC4949] (adapted)	The right or a permission that is granted to a system entity to access a system resource.
Backdoor	An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.
Buffer overflow [SP800-28]	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.
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 [USC44-3552] (adapted)	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration (of a system or device)	Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections. SOURCE: IEC/PAS 62409
Configuration control [CNSS4009] (adapted)	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.
Control	The part of the OT system used to perform the monitoring and control of the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.
Control algorithm [ISADICT]	A mathematical representation of the control action to be performed.
Control center [ANSI-ISA-51-1]	An equipment structure or group of structures from which a process is measured, controlled, and/or monitored.
Control loop	A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as 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. SOURCE: ISA99
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 [ISADICT]	The variable that the control system attempts to keep at the set point value. The set point may be constant or variable.
Controller [ANSI-ISA-51-1]	A device or program that operates automatically to regulate a controlled variable.
Cycle time [ISADICT]	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 the process resulting in new sensor signals.
Data diode	A network appliance or device allowing 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 supporting data analysis using statistical process control techniques.
Database [IR6859] (adapted)	A repository of information that usually holds plant-wide information including process data, recipes, personnel data, and financial data.
Demilitarized zone [SP800-41r1]	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.
Denial of service [RFC4949]	The prevention of authorized access to a system resource or the delaying of system operations and functions.
Diagnostics [ISADICT]	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.
Disaster recovery plan [SP800-34r1] (adapted)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
Discrete process [ISADICT]	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.
Distributed control system [ISADICT]	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.
Disturbance [ANSI-ISA-51-1]	An undesired change in a variable being applied to a system that tends to adversely affect the value of a controlled variable.

Domain [RFC4949] (adapted)	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.
Encryption [RFC4949] (adapted)	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.
Enterprise	An organization that coordinates the operation of one or more processing sites. SOURCE: ANSI/ISA-88.01-1995
Fault tolerant	Of 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 of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.
File Transfer Protocol	An Internet 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 which allows FTP access.
Firewall [RFC4949]	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).
Human-machine interface [IR6859]	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.
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 [FIPS200]	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.
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 such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. 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 [OMB-A130]	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.
Input/output [ISADICT]	A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications.
Insider	An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
Integrity [USC44_3552] (adapted)	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Intelligent electronic device [AGA12]	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).
Internet [RFC4949] (adapted)	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).
Intrusion detection system [RFC4949] (adapted)	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.
Intrusion prevention system	A system that can detect an intrusive activity and can 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 used 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 [IR6859]	A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.
Maintenance [ISADICT]	Any act that either prevents the failure or malfunction of equipment or restores its operating capability.
Malware [SP800-53r5] (adapted)	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.
Manipulated variable [ISADICT]	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.
Master terminal unit	See *Control Server*.
Modem [IR6859]	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.
Operating system [ISADICT]	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.
Operational controls [FIPS200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
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 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 [SP800-30r1]	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.
Pressure regulator [IR6859]	A device used to control the pressure of a gas or liquid.
Pressure sensor [IR6859] (adapted)	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.
Printer [IR6859] (adapted)	A device that converts digital data to human-readable text on a paper medium.
Process controller [IR6859] (adapted)	A type of computer system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs.
Programmable logic controller [ISADICT]	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.
Protocol [RFC4949]	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems.
Protocol analyzer [ISADICT]	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.

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 [IR6859]	A backup to the control server that maintains the current state of the control server at all times.
Relay [ISADICT]	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.
Remote access [SP800-53r5]	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network.
Remote diagnostics	Diagnostics activities conducted by individuals communicating external to an information system security perimeter.
Remote maintenance [SP800-53r5]	Maintenance activities conducted by individuals communicating through an external network.
Remote terminal unit [IR6859]	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.
Risk [FIPS200] (adapted)	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.
Risk assessment [SP800-39] (adapted)	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.
Risk management [FIPS200] (adapted)	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.
Router [RFC4949] (adapted)	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.

Safety instrumented system [ANSI-ISA-84]	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).
SCADA server	The device that acts as the master in a SCADA system.
Security audit [ISO7498-1]	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.
Security controls [FIPS199]	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.
Security plan [SP800-18r1]	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.
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. SOURCE: ISA99
Sensor [ISADICT]	A device that produces a voltage or current output that is representative of some physical property being measured (e.g., speed, temperature, flow).
Set point [ISADICT]	An input variable that sets the desired value of the controlled variable. This variable may be manually set, automatically set, or programmed.
Single loop controller [IR6859]	A controller that controls a very small process or a critical process.
Social engineering [SP800-61r2]	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.
Supervisory control [ISADICT]	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*.

Supervisory control and data acquisition [ISADICT]	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.
Technical controls [FIPS200]	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.
Threat [FIPS200] (adapted)	Any circumstance or event with the potential to adversely impact agency operations (including 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.
Threat event [SP800-30r1]	An event or situation that has the potential for causing undesirable consequences or impact.
Threat source [FIPS200]	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.*
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 delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.
Trojan horse [RFC4949]	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.
Unauthorized access [SP800-61]	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
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 into the source network. The software replicates databases and emulates protocol servers and devices.
Valve [ISADICT]	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.
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,

[RFC4949] (adapted)	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.
Virus [RFC4949] (adapted)	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.
Vulnerability [FIPS200]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Wide area network	A physical or logical network that provides data communications to a larger number of independent users than are usually 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 in some cases to modify control set points.
Workstation [IR6859]	A computer used for tasks such as programming, engineering, and design.
Worm [RFC4949] (adapted)	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.

Appendix C—Threat Sources, Vulnerabilities, and Incidents

Several terms are used to describe the inter-related 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 for causing undesirable consequences or impact. 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 impact. Each organization calculates risk based on the specific threats, vulnerabilities, and impact and likelihood of incidents within their environment.

C.1 Threat Sources

Threats to OT can come from numerous sources, which 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 their 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/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 which exceed expected operating parameters. Includes 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 which are outside 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 housing 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/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; it should also not be assumed that these issues are found within every OT environment.

The 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 assist in determining 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 unique to the particular technology or implementation that do not appear in this appendix. Specific current information on OT vulnerabilities can be researched at the CISA website. Many vendors publish notifications and patches to improve both reliability and security which are not always found on the CISA website. It is beneficial to maintain relationships with the 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; others are more expeditiously dealt with by instituting additional policies and procedures.

Vulnerabilities in products and services acquired from outside 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 its 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 partner to policy, encouraging 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 and 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. 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. This ensures 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 as well as 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's limited ability to ensure 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 for 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. Lack of a specific plan for the OT could lead to extended downtimes and production loss.
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 policy, systems might 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 & 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 of 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, we find large complex systems, systems-of-systems, and networks, all of which incorporate hardware architecture and software framework (including application frameworks), where the combination supports 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 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 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 allowing 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 which 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 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 collection and retention of sufficient data. Without proper and accurate data collection, it might 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 not under asset management	The organization doesn't know what it has (e.g., make, model), where they are, or what version it has, 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 not under configuration management	The organization doesn't know the patch management status, security settings, or configuration versions that it has, resulting in 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 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 significantly 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 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 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 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 impact. 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, and also 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 loss of data. Documented procedures should be developed for maintaining configuration settings.
Data unprotected on portable device	If sensitive data (e.g., passwords, dial-up numbers) is stored in cleartext on portable devices such as laptops and mobile devices and these devices are lost or stolen, system security could be compromised. 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.
Passwords generation, use, and protection not in accord 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 be matched to the way the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in giving an OT user 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 with 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 to others. Data linkage may create a vulnerability if it is not properly configured and may allow unauthorized data access or manipulation.
Malware protection not installed or up to date	Installation of malicious software, or malware, 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 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/prevention software 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 determine that it does not compromise normal operation of the OT.
Logs 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, taking into account safety requirements 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 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 (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 and electromagnetic pulses (EMP), static discharge, brownouts, and voltage spikes. The impact can range from 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	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; some may continue to operate but in a minimal capacity and may 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, keystroke loggers, etc.

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 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 not employed	Data flow controls, based on data characteristics, are needed to restrict which information is permitted between systems. These controls can prevent exfiltration of information and illegal operations.
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, 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 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 to spoof 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. Also, incorrect implementation of the protocols can lead to additional vulnerabilities.
Lack of integrity checking for communications	Integrity checks are not built into most OT protocols; 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 also to ensure 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, WiFi, WirelessHART). Wireless access should be securely configured or disabled using hardware write-protect where possible to protect unauthorized modification of the sensors and final elements which are connected both to the physical process and to the OT environment.

Vulnerability	Description
Inappropriate segmentation of 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. In 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, specifically addressing how the threat events can manipulate OT processes to cause physical damage. Table 21 provides an overview of potential OT threat events, leveraging 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, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling 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.
Loss of Safety	Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow for 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 Section 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 resulting in an accidental event). Provided below is a limited selection of reported incidents covering 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, sending a comical message in morse code referencing "rats." Maskelyne then published an explanation of his hack to 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 knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out 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 develops manufacturing software applied for a job with the local government but was rejected. Over a two-month period, the disgruntled rejected 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.

---

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

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/.

- **[M][I] Night Dragon.**[12] McAfee reported a series of attacks designed to steal sensitive data from the 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 "massive"—though unspecified—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 which controlled the SCADA system for the Bowman Dam located in Rye, New York. The adversary was able to view water levels, temperature, and 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 using primarily Havex malware. Havex is a remote access trojan that uses the Open Platform Communications (OPC) standard to gather information about connected ICS devices on a network. The campaigns were exploratory.
- **[M][D] Ukrainian Power Grid, BlackEnergy3.**[18] On December 23, 2015, Ukrainian power companies experienced a cyberattack causing power outages which 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 target 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.

---

[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 US 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.

[18] Additional information about the first Ukrainian Power Grid attack can be found at: https://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.

- **[M][D] Ukrainian Power Grid, Industroyer.**[19] On December 17, 2016, a cyber attack occurred at a substation outside of Kiev. The impact was an outage for customers of one substation for approximately one hour. This attack is 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 impact to Maersk, FedEx, Merck, and Saint-Gobain. Malware destroyed data and disrupted shipping operations for Maersk, costing the company over $300 million on repair and recovery.
- **[M][D] Saudi Petrochem, TRITON.**[20] A petrochemical facility in Saudi Arabia was attacked using malicious software targeted at 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 which 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][D] Honda, EKANS.** EKANS is ransomware that impacted operations at Honda automotive US production facilities in June 2020. EKANS has a hard-coded kill-list of processes, including some associated with common ICS software platforms (e.g., GE Proficy historian, Honeywell HMIWeb).
- **[M][D] Oldsmar Water Treatment Facility.**[22] In February 2021, hackers gained access to the City of Oldsmar's water treatment control system using TeamViewer, which was accessible via the internet. Dosing set points were modified, which temporarily increased the amount of sodium hydroxide (NaOH) being added to the water. The water treatment operator observed the hacker moving the mouse on the operating screen and was able to restore normal operations.
- **[M][I] Colonial Pipeline.**[23] In May 2021, over 5500 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 which encrypted their IT systems by exploiting a legacy VPN profile. The

---

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/ and 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 Oldsmar Water Treatment event can be found at: https://www.dragos.com/blog/industry,-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/.

23 Additional information on the Colonial Pipeline incident can be found in: https://www.c-span.org/video/?512247-1/senate-homeland-security-hearing-colonial-pipeline-cyber-attack "Senate Homeland Security Hearing on Colonial Pipeline Cyber Attack" Video. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf Transcript.

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 entire OT network 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 bring the pipeline system back online. The U.S. government was able to recover some of the ransom payment.[24]

- **[M][I] Ransomware Targeting Healthcare.**[25] A string of malware delivered via phishing attacks targeted the healthcare and public health sectors. The malware was used by adversaries to conduct ransomware attacks, disrupt services, and steal data. In fall 2020, 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.**[26] In June 1999, 900,000 liters (237,000 gallons) of gasoline leaked from a 40.64 cm (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 not able 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 October 2002 was to utilize an off-line development and testing system for implementing and testing changes to the SCADA database.

- **[M][I] CSX Train Signaling System.**[27] 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, shutting down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, ten Amtrak trains were affected in the morning. Trains between Pittsburgh 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.**[28] 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

---

[24] Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to Ransomware Extortionists Darkside. 7 June 2021. https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[25] Additional information on the series of malware targeting Healthcare can be found at Ransomware Activity Targeting the Healthcare and Public Health Sector | CISA.

[26] Additional information on the Bellingham, Washington Gasoline Pipeline Failure incident can be found at http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.

[27] Additional information on the CSX Train Signaling System incident can be found at: http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807.

[28] 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.

failed devices discovered that they would crash when they encountered excessive network traffic.

C.3.3 Environmental Events

- **[N][I] Fukushima Daiichi Nuclear Disaster.**[29] The Great East Japan Earthquake on March 11, 2011 struck off the coast of Japan, sending a massive tsunami inland towards 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.**[30] While a ping sweep was being performed on an active SCADA network that controlled 3-meter (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 all hosts that were attached to the network, for inventory purposes, and it caused a system controlling 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.**[31] 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. The outcome was the loss of service to its customer base for those four hours.

- **[N][I] NERC Enforcement Action.**[32] 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.

---

29 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.

30 Additional information on the vulnerability scanner incidents can be found at: https://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf.

31 Additional information on penetration testing incidents can be found at: https://energy.sandia.gov/wp-content/gallery/uploads/sand_2005_2846p.pdf.

32 For additional information about fines imposed on energy companies, see Enforcement Actions 2019 (nerc.com).

- **[N][D] NASA Fire.**[33] 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.

[33] For additional information on accidental OT losses from applying IT security controls in NASA, see Final Report - IG-17-011 (nasa.gov).

Appendix D—OT Security Organizations, Research, and Activities

This appendix contains abstracts of some of the many activities that are addressing OT cybersecurity. Please be aware that organization descriptions and related information provided in this appendix have been drawn primarily from the listed organizations' websites and from other reliable public sources but has not been verified. Readers are encouraged to contact the organizations directly for the most up-to-date and complete information.

D.1 Consortiums and Standards

D.1.1 Critical Infrastructure Partnership Advisory Council (CIPAC)

The U.S. Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators. CIPAC is aligned with and supports the implementation of the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience to provide a forum in which the government and private sector entities, organized as coordinating councils, can jointly engage in a broad spectrum of activities to support and collaborate critical infrastructure security and resilience efforts.

https://www.cisa.gov/critical-infrastructure-partnership-advisory-council

D.1.2 Institute for Information Infrastructure Protection (I3P)

The I3P is a consortium of leading national cybersecurity institutions, including academic research centers, government laboratories, and non-profit organizations. It was founded in September 2001 to help meet a well-documented need for improved research and development (R&D) to protect the nation's information infrastructure against catastrophic failures. The institute's main role is to coordinate a national cybersecurity R&D program and help build bridges between academia, industry, and government. The I3P continues to work toward identifying and addressing critical research problems in information infrastructure protection and opening information channels between researchers, policymakers, and infrastructure operators.

https://www.thei3p.org

D.1.3 International Electrotechnical Commission (IEC)

IEC is a standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These standards serve as a basis for creating national standards and as references for drafting international tenders and contracts. IEC's members include manufacturers, providers, distributors, vendors, consumers, and users, all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries. Below you will find relevant IEC Technical Committees (TC) that contribute to the field of OT security.

https://www.iec.ch

D.1.3.1 IEC Technical Committee 57

The scope of TC 57 is to prepare international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control and Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation, and maintenance of power systems. The list of current working groups (WGs) within TC 57 is below.

https://www.iec.ch/dyn/www/f?p=103:7:3323052731869::::FSP_ORG_ID,FSP_LANG_ID:1273,25

- WG 3: Telecontrol protocols
- WG 10: Power system IED communication and associated data models
- WG 13: Software interfaces for operation and planning of the electric grid
- WG 14: Enterprise business function interfaces for utility operations
- WG 15: Data and communication security
- WG 16: Deregulated energy market communications
- WG 17: Power system intelligent electronic device communication and associated data models for microgrids, distributed energy resources and distribution automation
- WG 18: Hydroelectric power plants - Communication for monitoring and control
- WG 19: Interoperability within TC 57 in the long term
- WG 20: Power Line Carrier Communication Systems
- WG 21: Interfaces and protocol profiles relevant to systems connected to the electrical grid

D.1.3.2 IEC Technical Committee 65

The scope of TC 65 is to prepare international standards for systems and elements used for industrial process measurement, control, and automation. To coordinate standardization activities which affect integration of components and functions into such systems including safety and security aspects. This work of standardization is to be carried out in the international fields for equipment and systems. The list of current working groups within TC 65 is included in the link below.

https://www.iec.ch/dyn/www/f?p=103:7:3323052731869::::FSP_ORG_ID,FSP_LANG_ID:1250,25

D.1.4 Institute of Electrical and Electronics Engineers, Inc. (IEEE)

IEEE and its members inspire a global community to innovate for a better tomorrow through its more than 400,000 members in more than 160 countries, and its highly cited publications, conferences, technology standards, and professional and educational activities. Below you will find relevant IEEE subsocieties that contribute to the field of OT security.

https://www.ieee.org/

D.1.4.1 IEEE Engineering in Medicine and Biology Society (EMBS)

EMBS is the world's largest international society of biomedical engineers who design the electrical circuits that make a pacemaker run, create the software that reads an MRI, and help develop the wireless technologies that allow patients and doctors to communicate over long distances.

https://www.embs.org/

D.1.4.2 IEEE Industrial Electronics Society (IES)

IES members focus on the theory and application of electronics, controls, communications, instrumentation, and computational intelligence to industrial and manufacturing systems and processes.

http://www.ieee-ies.org/

D.1.4.3 IEEE Power & Energy Society (PES)

IEEE PES is the world's largest forum for sharing the latest in technological developments in the electric power industry, for developing standards that guide the development and construction of equipment and systems, and for educating members of the industry and the general public.

https://www.ieee-pes.org/

D.1.4.4 IEEE Technical Committee on Power System Communications and Cybersecurity (PSCCC)

IEEE PSCCC Cybersecurity Subcommittee (SO) leads numerous working groups dedicated to maintaining standards within the field of OT security. For more information regarding each standard listed, please visit the link below.

https://site.ieee.org/pes-pscc/cybersecurity-subcommittee-s0/

- IEEE Std 1686, Standard for Intelligent Electronic Devices Cyber Security Capabilities
- IEEE Std 1711.1, Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links: Substation Serial Protection Protocol (SSPP)
- IEEE Std 2030.102.1-2020, Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems
- IEEE Std 1711.2-2019, Standard for Secure SCADA Communications Protocol (SSCP)

- IEEE Std C37.240, Standard Cybersecurity Requirements for Power System Automation, Protection and Control Systems
- IEEE Std 2808, Standard for Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity
- IEEE Std 2658, Guide for Cybersecurity Testing in Electric Power Systems
- IEEE Std 1547.3, Guide for Cybersecurity of DERs Interface with Electric Power Systems
- IEEE Std 1815-2012, Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)

D.1.4.5 IEEE Robotics and Automation Society (RAS)

RAS members foster the development and facilitate the exchange of scientific and technological knowledge in robotics and automation that benefits the profession and humanity.

https://www.ieee-ras.org/

D.1.4.6 IEEE Vehicular Technology Society (VTS)

The Vehicular Technology Society (VTS) is composed of engineers, scientists, students, and technicians interested in advancing the theory and practice of electrical engineering as it applies to mobile communications, land transportation, railroad/mass transit, vehicular electro-technology equipment and systems, and land/airborne/maritime mobile services.

https://vtsociety.org

D.1.5 International Society of Automation (ISA)

The International Society of Automation (ISA) is a non-profit professional association founded in 1945 to create a better world through automation. ISA advances technical competence by connecting the automation community to achieve operational excellence and is the trusted provider of standards-based foundational technical resources, driving the advancement of individual careers and the overall profession. ISA develops widely used global standards; certifies professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.

https://www.isa.org

D.1.5.1 ISA95, Enterprise-Control System Integration

The ISA95 standards development committee defines the interface between control functions and other enterprise functions based upon the Purdue Reference Model for Computer Integrated Manufacturing (CIM). The ISA95 standard grew from the Purdue Enterprise Reference Architecture (PERA), first published by ISA in 1992. Since then, it has served as a common reference for defining the interfaces between the enterprise and control networks across all OT sectors. The most up-to-date standards published by ISA95 can be found below:

https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

D.1.5.2 ISA99, Industrial Automation and Control Systems Security

The ISA99 standards development committee brings together industrial cybersecurity experts from across the globe to develop ISA standards on industrial automation and control systems security. This original and ongoing ISA99 work is being utilized by the International Electrotechnical Commission in producing the multi-standard ISA/IEC 62443 series. 62443 standards and technical reports are currently organized into four general categories called General, Policies and Procedures, System, and Component. The current state of the 62443 series can be found by following the link below.

https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

General

- ISA-62443-1-1, Concepts and models
- ISA-62443-1-2, Master glossary of terms and abbreviations
- ISA-62443-1-3, Security system conformance metrics
- ISA-62443-1-4, IACS security lifecycle and use cases

Policies and Procedures

- ISA-62443-2-1, Security program requirements for IACS asset owners
- ISA-62443-2-2, IACS Security Protection Ratings (Draft)
- ISA-62443-2-3, Patch management in the IACS environment
- ISA-62443-2-4, Security Program requirements for IACS service providers
- ISA-62443-2-5, Implementation guidance for IACS asset owners

System

- ISA-62443-3-1, Security technologies for IACS
- ISA-62443-3-2, Security risk assessment for system design
- ISA-62443-3-3, System security requirements and security levels

Component

- ISA-62443-4-1, Product security development life cycle requirements
- ISA-62443-4-2, Technical security requirements for IACS components

D.1.5.3 ISA-TR84.00.09, Cybersecurity Related to the Functional Safety Lifecycle

This document is intended to address and provide guidance on integrating the cybersecurity lifecycle with the safety lifecycle as they relate to Safety Controls, Alarms, and Interlocks (SCAI), inclusive of Safety Instrumented Systems (SIS). This scope includes the work processes and countermeasures used to reduce the risk involved due to cybersecurity threats to the Industrial Automation and Control System (IACS) network.

https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f

D.1.6 International Organization for Standardization (ISO)

ISO is an independent, non-governmental international organization with a membership of 165 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. While the 27001/27002 standards are defined for IT systems and environments, they still have many applications to OT security. The most recent versions of each standard were released in 2013.

https://www.iso.org

D.1.6.1 ISO 27001

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001 are generic and are intended to be applicable to all organizations, regardless of type, size, or nature.

https://www.iso.org/standard/54534.html

D.1.6.2 ISO 27002:2022

ISO/IEC 27002:2022 gives guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environment(s).

https://www.iso.org/standard/75652.html

D.1.7 National Council of Information Sharing and Analysis Centers (ISACs)

Formed in 2003, the NCI today comprises 25 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze, and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness. For a list of current member ISACs from various critical infrastructure sectors visit the link below.

https://www.nationalisacs.org/member-isacs-3

D.1.8 National Institute of Standards and Technology (NIST)

The mission of NIST is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology. NIST develops and maintains an extensive collection of computer security standards, guidelines, recommendations, and research which are released through SPs and other reporting mediums.

https://csrc.nist.gov/publications/

D.1.8.1 NIST SP 800 Series Cybersecurity Guidelines

The NIST SP 800 series of documents on information technology reports on the NIST Information Technology Laboratory (ITL) research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. In addition to NIST SP 800-82, the following is an abbreviated listing of additional 800 series documents that have broad applicability to the OT security community. All 800 series documents are available through the URL listed below.

https://csrc.nist.gov/publications/sp800

- 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 800-40 Rev. 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
- NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-53A Rev. 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*

- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*
- NIST SP 800-70 Rev. 4, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
- NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*
- NIST SP 800-116 Rev. 1, *Guidelines for the Use of PIV Credentials in Facility Access*
- NIST SP 800-123, *Guide to General Server Security*
- NIST SP 800-124 Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- NIST SP 800-125, *Guide to Security for Full Virtualization Technologies*
- 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*
- NIST SP 800-150, *Guide to Cyber Threat Information Sharing*
- NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
- NIST SP 800-160 Vol. 2 Rev. 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*

D.1.8.2 NIST SP 1800 Series Cybersecurity Practice Guides

NIST SP 1800 series documents present practical, usable, cybersecurity solutions to the cybersecurity community. These solutions demonstrate how to apply standards-based approaches and best practices. An 1800 document can map capabilities to the Cybersecurity Framework and outline steps needed for another entity or organization to recreate an example solution. Each SP 1800 series publication generally serves as a "how to" guide that demonstrates how to implement and apply standards-based cybersecurity technologies in the real world. The guides are designed to help organizations gain efficiencies in implementing cybersecurity technologies, while saving them research and proof of concept costs. The following is a listing of some 1800 series documents that have applicability to the OT security community. These as well as many others are available through the URL listed below.

https://csrc.nist.gov/publications/sp1800

- NIST SP 1800-2, *Identity and Access Management for Electric Utilities*
- NIST SP 1800-7, *Situational Awareness for Electric Utilities*
- NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*
- NIST SP 1800-10, *Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector*

- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*
- NIST SP 1800-23, *Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry*
- NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector*
- NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*
- NIST SP 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*
- NIST SP 1800-27, *Securing Property Management Systems*
- NIST SP 1800-30, *Securing Telehealth Remote Patient Monitoring Ecosystem*
- NIST SP 1800-32, *Securing Distributed Energy Resources: An Example of Industrial Internet of Things*

D.1.8.3 NIST Internal or Interagency Reports

NISTIR series documents are reports of research findings, including background information for FIPS and SPs. The following is a listing of some NISTIR series documents that have applicability to the OT security community. These as well as many others are available through the URL listed below.

https://csrc.nist.gov/publications/nistir

- NISTIR 7628 Rev. 1, *Guidelines for Smart Grid Cybersecurity*
- NISTIR 8011 Vol. 1, *Automation Support for Security Control Assessments: Volume 1: Overview*
- NISTIR 8011 Vol. 2, *Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management*
- NISTIR 8011 Vol. 3, *Automation Support for Security Control Assessments: Software Asset Management*
- NISTIR 8011 Vol. 4, *Automation Support for Security Control Assessments: Software Vulnerability Management*
- NISTIR 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*
- NISTIR 8183 Rev. 1, *Cybersecurity Framework Version 1.1 Manufacturing Profile*
- NISTIR 8183A Vol. 1, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance*
- NISTIR 8183A Vol. 2, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case*

- NISTIR 8183A Vol. 3, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case*
- NISTIR 8212, *ISCMA: An Information Security Continuous Monitoring Program Assessment*
- NISTIR 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*

D.1.9 North American Electric Reliability Corporation (NERC)

NERC's mission is to improve the reliability and security of the bulk power system in North America. To achieve that, NERC develops and enforces reliability standards; monitors the bulk power system; assesses future adequacy; audits owners, operators, and users for preparedness; and educates and trains industry personnel. NERC is a self-regulatory organization that relies on the diverse and collective expertise of industry participants. As the Electric Reliability Organization, NERC is subject to audit by the US Federal Energy Regulatory Commission and governmental authorities in Canada.

https://www.nerc.com

NERC Critical Infrastructure Protection (CIP) Standards

NERC has issued a set of cybersecurity standards to reduce the risk of compromise to electrical generation resources and high-voltage transmission systems above 100 kV, also referred to as bulk electric systems. Bulk electric systems include Balancing Authorities, Reliability Coordinators, Interchange Authorities, Transmission Providers, Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, and Load Serving Entities. The cybersecurity standards include audit measures and levels of non-compliance that can be tied to penalties. NERC currently maintains 12 Critical Infrastructure Protection (CIP) standards subject to enforcement, with 2 additional standards which are filed and pending regulatory approval.

https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

- CIP-002, Cyber Security - BES Cyber System Categorization
- CIP-003, Cyber Security - Security Management Controls
- CIP-004, Cyber Security - Personnel & Training
- CIP-005, Cyber Security - Electronic Security Perimeter(s)
- CIP-006, Cyber Security - Physical Security of BES Cyber Systems
- CIP-007, Cyber Security - System Security Management
- CIP-008, Cyber Security - Incident Reporting and Response Planning
- CIP-009, Cyber Security - Recovery Plans for BES Cyber Systems
- CIP-010, Cyber Security - Configuration Change Management and Vulnerability Assessments

- CIP-011, Cyber Security - Information Protection
- CIP-013, Cyber Security - Supply Chain Risk Management
- CIP-014, Cyber Security - Physical Security

D.1.10 Operational Technology Cybersecurity Coalition

The Operational Technology Cybersecurity Coalition's mission is to promote open, vendor-neutral, interoperable, standards-based cybersecurity solutions for OT.

https://www.otcybercoalition.org/

D.2 Research Initiatives and Programs

D.2.1 Clean Energy Cybersecurity Accelerator Initiative

This initiative which is led by the U.S. Department of Energy (DOE) and the National Renewable Energy Laboratory (NREL), brings together federal infrastructure and expertise, asset owners in the energy sector, and technology innovators in a unified effort to catalyze the development of new cybersecurity solutions for the nation's future clean energy grid.

The Cybersecurity Accelerator offers a world-class facility for asset owners of all sizes and types to work jointly to develop and deploy renewable, modern, and secure grid technologies that are cost competitive. The innovative technologies will also advance the state of the practice in demonstrating "security by design"—ensuring cybersecurity is built into renewable technologies and architectures at the start at the start of the design and development process, not bolted on after deployment.

https://www.energy.gov/ceser/department-energy-clean-energy-accelerator-initiative

D.2.2 Cybersecurity for Energy Delivery Systems (CEDS) R&D Program

The Department of Energy (DOE) Cybersecurity, Energy Security, and Emergency Response (CESER) Office designed the CEDS R&D program starting in 2010 to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused research and development effort. Since then, DOE CESER has invested more than $240 million with industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber-incident for current and future energy delivery systems.

https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

D.2.3 Cybersecurity for the Operational Technology Environment (CyOTE)

DOE CESER has partnered with Idaho National Laboratory and energy companies on a research initiative to enhance energy sector threat detection of anomalous behavior potentially indicating malicious cyber activity in OT networks.

https://inl.gov/cyote/

D.2.4 Cybersecurity Risk Information Sharing Program (CRISP)

A public-private partnership, co-funded by DOE and industry and managed by the Electricity Information Sharing and Analysis Center (E-ISAC) at NERC. The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the nation's Intelligence Community to better inform the energy sector of the high-level cyber risks. Pacific Northwest National Laboratory (PNNL) plays a lead role in CRISP, which uses advanced sensors and data analysis to identify new and ongoing cyber threats. This information is shared with voluntary utility participants that collectively deliver more than 80 percent of the nation's electricity.

https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf

D.2.5 Cyber Testing for Resilient Industrial Control Systems (CyTRICS)

DOE CESER has partnered with Idaho National Laboratory and stakeholders to identify high priority OT components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing.

https://inl.gov/cytrics/

D.2.6 Homeland Security Information Network - Critical Infrastructure (HSIN-CI)

The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified (SBU) information. The Critical Infrastructure community on HSIN (HSIN-CI) is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure. HSIN-CI provides real-time collaboration tools including a virtual meeting space, document sharing, alerts, and instant messaging at no charge.

https://www.dhs.gov/hsin-critical-infrastructure

D.2.7 INL Cyber-Informed Engineering (CIE) / Consequence-Driven CIE (CCE)

The Department of Energy (DOE) and Idaho National Laboratory (INL) have developed a framework to guide the application of cybersecurity principles across the engineering design life cycle. The Cyber-Informed Engineering (CIE) framework and body of knowledge drives the inclusion of cybersecurity as a foundational element of risk management for engineering of functions aided by digital technology. Consequence-Driven Cyber-Informed Engineering (CCE) is a rigorous process for applying CIE's core principles to a specific organization, facility, or mission by identifying their most critical functions, methods and means an adversary would likely use to manipulate or compromise them and determining the most effective means of removing or mitigating those risks.

CIE emphasizes “engineering out” potential risk in key areas, as well as ensuring resiliency and response maturity within the design of the engineered system. The following CIE framework shows some of the key focus areas and how the relate to the CCE Methodology. CCE walks an organization through core components of CIE in CCE’s 4-phase process to evaluate and remove or mitigate weaknesses in their critical functions.

https://inl.gov/cie/

D.2.8 LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity

The LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) program is a collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate. LOGIIC undertakes collaborative research and development projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector. The objective is to promote the cybersecurity of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality.

The Automation Federation serves as the LOGIIC host organization and has entered into agreements with the LOGIIC member companies and all other LOGIIC project participants. The US Department of Homeland Security Science and Technology Directorate previously contracted with scientific research organization SRI International to provide scientific and technical guidance for LOGIIC.

https://www.logiic.org/

D.2.9 NIST Cyber Physical Systems and Internet of Things Program

The definitions of cyber-physical systems (CPS) and the Internet of Things (IoT) are converging over time to include a common emphasis on hybrid systems of interacting digital, analog, physical, and human components in systems engineered for function through integrated physics and logic. CPS and IoT enable innovative applications in important economic sectors such as smart cities, energy, manufacturing, transportation, and emergency response. The CPS/IoT Program develops and demonstrates new measurement science and promotes the emergence of consensus standards and protocols for advanced cyber-physical systems and IoT that are scalable, effective, measurable, interoperable, trustworthy, and assured. The Engineering Laboratory (Smart Grid and Cyber-Physical Systems Program Office) also provides leadership to support NIST-wide CPS/IoT program coordination with the Information Technology, Communications Technology, and Physical Measurement Laboratories.

https://www.nist.gov/programs-projects/cyber-physical-systems-and-internet-things-program

D.2.10 NIST Cybersecurity for Smart Grid Systems Project

Smart grid cybersecurity must address both inadvertent compromises of the electric infrastructure, due to user errors, equipment failures, and natural disasters, and deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists. NIST will address these challenges through research conducted in the NIST Smart Grid Testbed facility and leadership within the Smart Electric Power Alliance (SEPA) Cybersecurity Committee (SGCC) to evaluate of cybersecurity policies and measures in industry standards, and development of relevant guidance documents for the smart grid cybersecurity community. The primary goal is to develop a cybersecurity risk management strategy for the smart grid to enable secure interoperability of solutions across different domains and components. The Cybersecurity for Smart Grid Systems Project is moving forward to address the critical cybersecurity needs by promoting technology transfer of best practices, standards and voluntary guidance, and research in the areas of applied cryptography and cybersecurity for microgrids. This project will provide foundational cybersecurity guidance, cybersecurity reviews and recommendations for standards and requirements, outreach, and foster collaborations in the cross-cutting issue of cybersecurity in the smart grid.

https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems

D.2.11 NIST Cybersecurity for Smart Manufacturing Systems Project

The Cybersecurity for Smart Manufacturing Systems project develops cybersecurity implementation methods, metrics and tools to enable manufacturers to implement cybersecurity capabilities in smart manufacturing systems while addressing the demanding performance, reliability, and safety requirements of these systems.

https://www.nist.gov/programs-projects/cybersecurity-smart-manufacturing-systems

D.2.12 NIST Reliable, High Performance Wireless Systems for Factory Automation

The Reliable, High Performance Wireless Systems for Factory Automation project develops robust requirements, system models, recommended architectures, and guidelines for the integration of trustworthy wireless systems within a factory workcell where wireless is the primary mode of communication enabling robot mobility and ease of installation of edge devices.

https://www.nist.gov/programs-projects/reliable-high-performance-wireless-systems-factory-automation

D.2.13 NIST Prognostics and Health Management for Reliable Operations in Smart Manufacturing (PHM4SM)

The NIST Prognostics and Health Management for Reliable Operations in Smart Manufacturing (PHM4SM) project develop and deploys measurement science to promote the implementation, verification, and validation of advanced monitoring, diagnostic, and prognostic technologies to increase reliability and decrease downtime in smart manufacturing systems.

https://www.nist.gov/programs-projects/prognostics-and-health-management-reliable-operations-smart-manufacturing-phm4sm

D.2.14 NIST Supply Chain Traceability for Agri-Food Manufacturing

The NIST Supply Chain Traceability for Agri-Food Manufacturing project develops and deploys new standards, tools, and guidelines for traceability and cybersecurity that increase trust among participants and customers of agri-food manufacturing supply chains.

https://www.nist.gov/programs-projects/supply-chain-traceability-agri-food-manufacturing

D.3 Tools and Training

D.3.1 CISA Cyber Security Evaluation Tool (CSET®)

The Cyber Security Evaluation Tool (CSET®) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate ICS and IT network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.

https://github.com/cisagov/cset/releases

D.3.2 CISA Cybersecurity Framework Guidance

Sector-specific guidance has been completed by all six critical infrastructure sectors for which the Department of Homeland Security, Office of Infrastructure Protection is the Sector-Specific Agency (SSA): Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear. Guidance is developed in close collaboration with the SSA, alongside the Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC), to provide a holistic view of a sector's cybersecurity risk environment.

https://us-cert.cisa.gov/resources/cybersecurity-framework

D.3.3 CISA ICS Alerts, Advisories and Reports

CISA Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

https://www.cisa.gov/uscert/ics/alerts

Advisories provide timely information about current security issues, vulnerabilities, and exploits.

https://www.cisa.gov/uscert/ics/advisories

ICS-related Technical Information Papers (TIPs), Annual Reports (Year in Review), and 3rd-party products that CISA considers of interest to persons engaged in protecting ICS:

https://www.cisa.gov/uscert/ics/Other-Reports

D.3.4 CISA ICS Training Courses

CISA offers both self-paced virtual online training courses via a virtual learning portal as well as instructor-led classes provided at various venues. All CISA training courses are presented with no tuition cost to the attendee.

https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA

D.3.5 MITRE ATT&CK for ICS

MITRE ATT&CK for ICS is a curated knowledge base for cyber adversary behavior in the ICS technology domain. It reflects the various phases of an adversary's attack life cycle and the assets and systems they are known to target. ATT&CK for ICS originated from MITRE internal research focused on applying the ATT&CK methodology to the ICS technology domain.

https://collaborate.mitre.org/attackics/index.php/Main_Page

D.3.6 NIST Cybersecurity Framework

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013 [EO13636]. It directed NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure.

NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

In April of 2018, NIST published Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity. Edits were driven by dialog with over 1,200 participants at the 2016 and 2017 annual framework workshops in addition to over 200 written comments regarding draft publications. Both versions can be found at the link below.

https://www.nist.gov/cyberframework/framework

D.3.7 SANS ICS Security Courses

SANS offers several courses that provide hands-on training focused on the cybersecurity of OT environments. These courses equip both security professionals and control system engineers with the knowledge and skills they need to safeguard critical infrastructure. Current course offerings and their corresponding certification are listed below.

https://www.sans.org/industrial-control-systems-security/

- ICS410: ICS/SCADA Security Essentials, Global Industrial Cyber Security Professional (GICSP)
- ICS456: Essentials for NERC CIP, GIAC Critical Infrastructure Protection (GCIP)
- ICS515: ICS Visibility Detection, and Response, GIAC Response and Industrial Defense (GRID)

D.4 Sector-Specific Resources

D.4.1 Chemical

Chemical Facility Anti-Terrorism Standards (CFATS) - https://www.cisa.gov/chemical-facility-anti-terrorism-standards

ChemLock - https://www.cisa.gov/chemlock

American Chemistry Council (ACC) - https://www.americanchemistry.com

American Petroleum Institute (API) - https://www.api.org

American Gas Association (AGA) - https://www.aga.org

American Fuel and Petrochemical Manufacturers (AFPM) - https://www.afpm.org

Society of Chemical Manufacturers and Affiliates (SOCMA) - https://www.socma.org

D.4.2 Communications

Federal Communications Commission (FCC) - https://www.fcc.gov

> Cybersecurity and Communications Reliability Division

> Communications Security, Reliability, and Interoperability Council (CSRIC)

D.4.3 Critical Manufacturing

National Association of Manufacturers (NAM) - https://www.nam.org

> NAM Cyber Cover

Association for Advancing Automation (A3) - https://www.automate.org

Measurement, Control, & Automation Association (MCAA) - https://www.themcaa.org

International Association for Automation and Robotics in Construction (IAARC) - https://www.iaarc.org

ODVA - https://www.odva.org

D.4.4 Dams

Association of State Dam Safety Officials (ASDSO) - http://www.damsafety.org

D.4.5 Energy

US Department of Energy (DOE) - https://www.energy.gov

> The Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

International council on Large Electric Systems (CIGRE) - https://www.cigre.org

American Public Power Association (APPA) - https://www.publicpower.org

> Cybersecurity Defense Community (CDC)

Electric Power Research Institute (EPRI) - https://www.epri.com

> National Electric Sector Cybersecurity Resource (NESCOR)

D.4.6 Food and Agriculture

US Department of Agriculture (USDA) - https://www.usda.gov

US Food and Drug Administration (FDA) - https://www.fda.gov

National Farmers Union (NFU) - https://www.nfu.org

> Farm Crisis Center

D.4.7 Healthcare and Public Health

US Food and Drug Administration (FDA) – https://www.fda.gov

> Digital Health Center of Excellence

Department of Health and Human Services (HHS) - https://www.hhs.gov

> Health Sector Cybersecurity Coordination Center (HC3)

American Hospital Association (AHA) - https://www.aha.org/

> AHA Preferred Cybersecurity Provider (APCP) Program

National Institutes of Health (NIH) - https://www.nih.gov

> NIH Information Technology Acquisition and Assessment Center (NITAAC)

American Medical Association (AMA) - https://www.ama-assn.org

D.4.8 Nuclear Reactors, Materials, and Waste

US Nuclear Regulatory Commission (NRC) - https://www.nrc.gov

> Office of Nuclear Security and Incident Response Cyber Security Branch (CSB)

International Atomic Energy Agency (IAEA) - https://www.iaea.org

Nuclear Energy Agency (NEA) - https://www.oecd-nea.org

> Digital Instrumentation and Control Working Group (DICWG)

Nuclear Energy Institute (NEI) - https://www.nei.org

World Institute of Nuclear Security (WINS) - https://www.wins.org

D.4.9 Transportation Systems

US Department of Transportation (DOT) - https://www.transportation.gov

> Intelligent Transportation Systems Joint Program Office

Federal Aviation Administration (FAA) - https://www.faa.gov

> Aviation Cyber Initiative (ACI)

> Air Traffic Organization (ATO) Cybersecurity Group

Federal Highway Administration (FHWA) - https://highways.dot.gov

> FHWA Office of Operations Research, Development, and Technology

Federal Motor Carrier Safety Administration (FMCSA) - https://www.fmcsa.dot.gov

Federal Railroad Administration (FRA) - https://railroads.dot.gov

> FRA Office of Research, Development, and Technology

Federal Transit Administration (FTA) - https://www.transit.dot.gov

Maritime Administration (MARAD) - https://www.maritime.dot.gov

> Office of Maritime Security

Pipeline and Hazardous Materials Safety Administration (PHMSA) - https://www.phmsa.dot.gov

National Highway Traffic Safety Administration (NHTSA) - https://www.nhtsa.gov

Transportation Security Administration (TSA) - https://www.tsa.gov/for-industry

> Surface Transportation Cybersecurity Resource Toolkit

Association of American Railroads - https://www.aar.org

D.4.10 Water and Wastewater

US Environmental Protection Agency (EPA) - https://www.epa.gov

> Drinking Water and Wastewater Resilience

American Water Works Association (AWWA) - https://www.awwa.org

> AWWA Cybersecurity Tool

Association of Metropolitan Water Agencies (AMWA) - https://www.amwa.net

National Association of Water Companies (NAWC) - https://www.nawc.org

D.5 Conferences and Working Groups

D.5.1 Digital Bond's SCADA Security Scientific Symposium (S4)

Since 2007, S4 has hosted an ICS security conference. The conference initially was founded for a need to showcase advanced and highly technical content to the ICS audience. S4 has since grown to also accommodate other ICS security content but remains a premier venue to present technical findings within OT security.

https://s4xevents.com/

D.5.2 Industrial Control Systems Joint Working Group (ICSJWG)

CISA hosts a bi-annual working group which provides a vehicle for communicating and partnering across all Critical Infrastructure (CI) Sectors between federal agencies and departments, as well as private asset owners/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the collaborative efforts of the industrial control systems stakeholder community in securing CI by accelerating the design, development, and deployment of secure industrial control systems.

https://www.cisa.gov/uscert/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

D.5.3 IFIP Working Group 11.10 on Critical Infrastructure Protection

An active international community of scientists, engineers and practitioners dedicated to advancing the state-of-the-art of research and practice in the emerging field of critical infrastructure protection.

http://ifip1110.org/Conferences/

D.5.4 SecurityWeek's ICS Cyber Security Conference

Since 2002, SecurityWeek has held an annual conference focused on cybersecurity for the industrial control systems sector. An event where ICS users, ICS vendors, system security providers and government representatives meet to discuss the latest cyber-incidents, analyze their causes, and cooperate on solutions.

https://www.icscybersecurityconference.com/

D.5.5 Stockholm International Summit on Cyber Security in SCADA and ICS (CS3STHLM)

Organized beginning in 2014, CS3STHLM has quickly become the premier ICS Security Summit in Northern Europe. CS3STHLM is a summit that offers generous time for lectures, networking, and knowledge sharing in regard to today's ICS security challenges.

https://cs3sthlm.se/

Appendix E—OT Security Capabilities and Tools

This appendix provides an overview of key security technologies that are available to or being developed to support the OT community. There are several security products that are marketed specifically for OT, while others are general IT security products that are also applicable to OT. Many cybersecurity products are marketed today as a single platform that combines many of the capabilities and tools listed here. Each organization should make a risk-based determination on whether to employ the security technologies and tools mentioned in this appendix.

E.1 Network Segmentation and Isolation

Network segmentation and separation technologies allow OT network owners to implement cybersecurity strategies that isolate devices and network traffic by both physical and logical means. Popular tooling for this capability area is described below.

E.1.1 Firewalls

Firewalls can be used to logically enforce user-defined rule sets on network traffic. Commonly placed at network boundaries, firewalls can limit both incoming and outgoing traffic based on a variety of data characteristics.

There are several types of general IT firewalls. Basic *packet filtering firewalls* directly inspect current network traffic at OSI layers 3 and 4 to inform decisions on whether to drop or forward packets to their destination. Conversely, *stateful inspection firewalls* draw upon memory of both past and present network connections when making filtering decisions, thereby offering more capability at an increased computational cost. *Next generation firewalls (NGFWs)* expand upon stateful inspection firewalls by adding features such as application filtering, deep packet inspection, VPN traffic awareness, adaptive rules, and threat detection.

Several vendors also offer OT-specific firewalls. The OT-specific implementations are often preferred over their generic IT counterparts due to their unique feature sets specific to OT networks. For example, they often provide built-in parsers for common OT protocols such as DNP3, CIP, and Modbus, allowing for deep packet inspection of OT traffic.

E.1.2 Unidirectional Gateways

Unidirectional gateways, also referred to as data diodes, are designed to only allow data transmission in a single direction. Unlike a firewall, data diodes cannot be programmed to allow data to flow in both directions; the hardware is incapable. A common use case is placing a data diode at the boundary between the operational network and the enterprise network. The data diode would allow network traffic to leave the operational network, but not enter, preventing a potential avenue of cyber attack.

E.1.3 Virtual Local Area Networks (VLAN)

A VLAN can be used to logically separate areas within a network when physical separation may not be feasible due to cost or other prohibitive measures. VLANs are implemented on modern network switching equipment that logically separates network traffic based on switch port. For example, an 8-port switch can be configured to separate traffic into two VLANs. One VLAN would be provided for ports 1-4, while another would be provided for ports 5-8. While all 8 ports are physically connected to a single device, each port is only logically connected to the other ports within its VLAN.

E.1.4 Software-Defined Networking (SDN)

Traditional networking switches are responsible for both forwarding packets (data plane) and running the distributed algorithms that determine routing (control plane). SDN is a technology that evolves this concept by keeping the data plane at the switch and moving the control plane to a centralized controller. The centralized controller acts as an abstraction layer for network programmability, eliminating the need to individually manage each switch within the network. SDN allows for easy dynamic reconfiguration of the data plane, which can allow for quick isolation of devices or redirection and duplication of traffic for monitoring and data capture. Utilizing SDN technology within an OT environment allows asset owners greater flexibility when initially designing their network architectures and when updating them in the future.

E.2 Network Monitoring/Security Information and Event Management (SIEM)

Network monitoring technologies allow OT network owners to maintain situational awareness of their controlled processes and support cybersecurity objectives such as event or anomaly detection. OT vendors often market their network monitoring technology as capable of integration with SIEM technologies. These systems collect data through log aggregation and network scanning tools, detect threats through analytics, and can provide automated incident response. Capabilities continue to be added, including use of machine learning and artificial intelligence to improve detection and reduce unnecessary alerts. OT owners must exercise caution when implementing these technologies as they can directly impact the availability of the controlled process.

E.2.1 Centralized Logging

System and network logs from all sources in an environment are the foundation of SIEM. Logs act as the primary historical artifact for incident response. When aggregated at a central location, logs can be analyzed together to provide a holistic view of the network state. A SIEM will utilize a variety of sensors strategically placed within a target network to collect logs from endpoints, as well as network traffic information, which is then stored in a database for real-time analysis. Specific to OT networks, data historians can serve as a supplemental source of event data providing greater context surrounding a cyber incident.

E.2.2 Passive Scanning

Passive network scans are a form of network discovery that inspects existing network traffic by watching traffic passing through network switches or other dedicated network capture devices. Systems that implement passive network scans do not introduce any additional traffic to the network, which is ideal for sensitive devices found on OT networks that may exhibit unexpected behavior when directly probed. Passive scanning can identify all devices actively communicating on network segments being monitored. Through inspection of network data, passive scanning can identify significant amounts of information about devices, potentially including, but not limited to, manufacturer, part number, and firmware version. Passive scanning cannot identify devices that are not actively communicating, nor can it inspect encrypted traffic (without special provisioning). Additionally, a passive scan will often take days to complete due to its dependence on existing network traffic.

E.2.3 Active Scanning

Active network scans are a form of network discovery that directly probe the network for attached devices. Systems employing active scanning introduce traffic to the network and will directly interact with the devices within the scan's scope. OT network owners should exercise extreme caution when permitting active scanning on an operational network due to device sensitivity on the target network.

Some OT-specific scanning devices combine passive and active scanning to enable a safer version of active scanning. Safe active scanning first learns about connected equipment through passive means and then uses device-specific communication to actively gain additional information about connected equipment without risks to OT operations.

E.2.4 Malware Detection

Endpoint malware detection can be bolstered with antivirus software. Antivirus software monitors activity on the host device and will alert the user to possible malicious activities. Older detection techniques rely on file signatures to detect known threats. Over time, malware developers have found ways to bypass this mechanism such as with polymorphic code. Modern antivirus software uses behavioral analysis of running processes and advanced file analysis to detect potentially malicious activity.

Host-based malware detection with antivirus software may not be advisable for some OT endpoints due to OS incompatibility, software incompatibility, or runtime requirements. However, network-based malware detection can still be utilized. Unlike host-based antivirus software, network-based malware detection runs on an independent system that aggregates and inspects network traffic for anomalies. Network-based malware detection offers similar capabilities to host-based detection without the computational overhead being placed on the defended component. Network-based detection is a primary component of SIEM packages.

E.2.5 Behavioral Anomaly Detection

Behavioral anomaly detection (BAD) systems compare the current state of an environment with a baseline to detect abnormal activity. This baseline is used to detect anomalous events to be investigated further. This could be unusual network traffic such as large amounts of data transferred, new ports/protocols, or new connections between devices. Unusual activity on an endpoint may include excessive processor usage, logins outside of work hours, or new processes. The detectable events are dependent on the sensor capabilities of the specific implementation. Some BAD systems utilize artificial intelligence (AI) and machine learning (ML) algorithms to automatically update the baseline model. By automating the process of updating the baseline, the

BAD system is able to maintain knowledge of normal activity even as the environment evolves over time. This ultimately reduces false positive detections, improving incident response capability.

E.2.6 Data Loss Prevention (DLP)

DLP is a collection of tools built to improve the confidentiality of sensitive data on a network. DLP is often marketed as a feature set within SIEM that actively monitors both data at rest to prevent unauthorized access and data in transit to prevent unauthorized extraction. In cases where DLP is unable to prevent the data loss, it can still alert the organization to a breach.

E.2.7 Deception Technology

A deception technology uses decoy data and/or devices placed across the network to lure attackers away from legitimate assets. Decoys can range from access credentials and files to complete endpoints. When a threat actor interacts with a decoy, it triggers an alarm to alert cyber defenders to its presence. Defenders can then choose to further monitor the adversary for intelligence or immediately mitigate the threat. Because decoys do not actively interact with other network components, deception technologies can support malicious activity monitoring and detection without jeopardizing the controlled process.

E.2.8 Digital Twins

A digital twin is a digital replica of a physical system or component. They can be deployed within OT environments as a tool for anomaly detection. The digital twin utilizes real-time sensor inputs and compares them using heuristics and algorithms (including machine learning) against a baseline model. Operational anomalies detected by digital twins most often indicate a maintenance or failure situation. However, a detected operational anomaly could indicate an advanced cyber attack which has bypassed other security mechanisms and otherwise would have gone undetected.

E.3 Data Security

Various data security technologies assist information owners in protecting the confidentiality, integrity, and availability of their data. OT network owners are encouraged to identify the critical files and data residing in their networks and implement data security technologies to mitigate risk.

E.3.1 Backup Storage

Backup storage is an alternative file storage location where copies of critical files are stored and protected to assist with recovery should the originals be lost, compromised, or unusable. Using backup tools and procedures is fundamental to ensuring the availability of critical data within an OT network environment. Based on risk, backup plans should specify which files require backup, how often they should be backed up, the number of copies to be made, the location of the backup (e.g., offline, offsite) and how long backup copies should be kept. Various solutions exist that automate backup storage of critical data on a regular basis.

E.3.2 Immutable Storage

Immutable storage is a special type of backup storage that provides additional data integrity through data storage in a read-only format. Immutable storage can be used to store backups of programs or device configurations. It can also be used as a read-only drive in a maintenance workstation for added protection against installation of new software.

E.3.3 File Hashing

Integrity of critical files such as program logic can be validated by using hashes. A hashing algorithm calculates a fixed-size string from a file's contents. If a hash is calculated and stored for a critical file when it is first created, the integrity of the file can be checked later by calculating the hash again. For example, if an end user needs to restore functionality to a device by returning it to a baseline, the integrity of the baseline files can first be validated by recomputing the file hash. If a different hash is calculated for a target file, the data owner can assume the backup files have been compromised. Many data backup software systems include hashing within their feature set. NIST-approved hash algorithms are specified in FIPS 180-4, *Secure Hash Standard* [FIPS180] and FIPS 202, *SHA-3 Standard* [FIPS202].

E.3.4 Digital Signatures

Digital signatures are an additional data integrity measure. They are the electronic analogue of a written signature providing assurance that the claimed signatory signed the information, and that the information was not modified following signature. FIPS 186-4, *Digital Signature Standard (DSS)* [FIPS186] specifies three NIST-approved digital signature algorithms: DSA, RSA, and ECDSA.

E.3.5 Block Ciphers

Asset owners can protect the confidentiality of data at rest using block ciphers. Block ciphers are algorithms that encrypt data in block-sized chunks rather than one bit at a time. This is beneficial when encrypting large amounts of data at once. NIST-approved block ciphers are Advanced Encryption Standard (AES) and Triple Data Encryption Standard (DES). AES is specified in FIPS 197, *Advanced Encryption Standard* [FIPS197]. Triple DES is specified in NIST SP 800-67 Rev. 2, *Recommendation for the Triple Data Encryption Algorithm Block Cipher* [SP800-67].

E.3.6 Remote Access

When accessing systems or data remotely, security controls should be implemented to prevent unauthorized access to the organization's networks, systems, and data. A virtual private network (VPN) is a set of technologies and 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 implemented today are:

- **Internet Protocol Security (IPsec).** IPsec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion (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. See NIST SP 800-77 Rev. 1, *Guide to IPsec VPNs* for more information.

- **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 HTTP traffic; this protocol implementation is known as HTTP Secure (HTTPS). However, TLS is not limited to HTTP traffic; it can be used to secure many application-layer programs. For more information, see NIST SP 800-52 Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.
- **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. SSH is included in most UNIX distributions and is typically added to other platforms through a third-party package.

When implemented with diligence, remote access technologies can improve an organization's capability. There are several options for remote access and desktop control including Remote Desktop Protocol (RDP), screens, and other standalone packages. If remote technologies are not managed properly using vulnerability and patch management, these connections serve as another channel for an adversary to exploit.

Appendix F—OT Overlay

Note to Readers

The OT overlay is a partial tailoring of the controls and control baselines in SP 800-53 Rev. 5 and adds supplementary guidance specific to OT. The concept of overlays is discussed in Appendix C of SP 800-53B. The OT overlay is intended to be applicable to all OT systems in all industrial sectors. Further tailoring can be performed to add specificity to a particular sector (e.g., pipeline, energy). Ultimately, an overlay may be produced for a specific system (e.g., the XYZ company).

This OT overlay constitutes supplemental guidance and tailoring for SP 800-53 Revision 5. Please be sure you are looking at the correct version of SP 800-53. Duplicating Appendix F of SP 800-53 would increase the size of this publication significantly. Therefore, the drafting committee has decided to not duplicate Appendix F here. The reader should have SP 800-53 Revision 5 available.

The authoring team also considered that this OT overlay may serve as a model for other overlays. Feedback on this Appendix's structure would be appreciated, especially on the level of abstraction and whether the examples provided in the supplemental guidance are sufficient/beneficial for implementation.

Overlays provide a structured approach to help organizations tailor control baselines and develop specialized security plans that can be applied to specific mission/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

A repository of overlays may be found at https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/overlay-repository. This overlay may be referenced as the NIST SP 800-82 Revision 3 Operational Technology Overlay ("NIST SP 800-82 Rev 3 OT Overlay"). It is based on NIST SP 800-53 Revision 5 [SP800-53r5].

NIST developed this overlay in furtherance of its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283) [FISMA], Presidential Policy Directive 21 (PPD-21) [PPD-21], and Executive Order 13636 [EO13636]. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

F.1 Overlay Characteristics

OT 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/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.

ICS consists 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 control part of the system includes the specification of the desired output or performance. Control can be fully automated or may include a human in the loop.

Section 2 provides an overview of various OT systems such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Building Automation Systems (BAS), Physical Access Control Systems (PACS), and the Industrial Internet of Things (IIoT).

F.2 Applicability

The purpose of this overlay is to provide guidance for securing OT systems. This overlay has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis.

Privacy is a risk consideration for OT systems. For additional guidance, refer to the NIST Privacy Framework [PF]. The application of privacy in OT will depend on sector and organizational risks; therefore, controls exclusively related to privacy have not been included in this OT overlay. Each organization will need to independently determine applicability. All controls and control enhancements that only appear in the privacy baseline have been removed from this OT overlay according to this rationale.

F.3 Overlay Summary

Table 22 provides a summary of the controls and control enhancements from NIST SP 800-53 Rev. 5, Appendix F [SP800-53r5] that have been allocated to the initial control baselines (i.e., Low, Moderate, and High) along with indications of OT Discussion and OT tailoring. The table uses the following conventions:

- **Bold** indicates controls and control enhancements with OT Discussions.
- Underline indicates that this overlay has added a control to the baseline, supplemental to the baselines provided in NIST SP 800-53B.
- ~~Strikethrough~~ indicates that a control or control enhancement has been removed from this baseline, compared to the baselines provided in NIST SP 800-53B.

In the following example, OT Discussion was added to Control Enhancement 1 of AU-4 (bolded). In addition, Control Enhancement 1 of AU-4 was added to the Low, Moderate (Mod), and High baselines (underlined), compared with the NIST 800-53B baseline which did not include AU-4 Control Enhancement 1.

AU-4	Audit Storage Capacity	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**

Some controls and control enhancements are useful to many OT environments but are not applicable across all OT sectors or architectures. Such controls may have additional OT discussion. These will appear in the individual control tables. Controls and control enhancements without baselines are not included in Table 22.

Table 22: Control Baselines

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Policy and Procedures	**AC-1**	**AC-1**	**AC-1**
AC-2	Account Management	**AC-2**	**AC-2** (1) **(2)** (3) (4) **(5)** **(13)**	**AC-2** (1) **(2)** (3) (4) **(5)** (11) (12) **(13)**
AC-3	Access Enforcement	**AC-3**	**AC-3**	**AC-3** **(11)**
AC-4	Information Flow Enforcement		**AC-4**	**AC-4** (4)
AC-5	Separation of Duties		**AC-5**	**AC-5**
AC-6	Least Privilege		**AC-6 (1) (2) (5)** (7) **(9) (10)**	**AC-6 (1) (2) (3) (5)** (7) **(9) (10)**
AC-7	Unsuccessful Logon Attempts	**AC-7**	**AC-7**	**AC-7**
AC-8	System Use Notification	**AC-8**	**AC-8**	**AC-8**
AC-10	Concurrent Session Control			**AC-10**
AC-11	Device Lock		**AC-11 (1)**	**AC-11 (1)**
AC-12	Session Termination		**AC-12**	**AC-12**
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	**AC-17** **(9)**	**AC-17 (1) (2) (3)** (4) **(9)** (10)	**AC-17 (1) (2) (3)** (4) **(9)** (10)
AC-18	Wireless Access	**AC-18**	**AC-18 (1)** (3)	**AC-18 (1)** (3) (4) **(5)**
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Systems	**AC-20**	**AC-20** (1) (2)	**AC-20** (1) (2)
AC-21	Information Sharing		AC-21	AC-21
AC-22	Publicly Accessible Content	**AC-22**	**AC-22**	**AC-22**
AT-1	Policy and Procedures	**AT-1**	**AT-1**	**AT-1**
AT-2	Literacy Training and Awareness	**AT-2** (2)	**AT-2** (2) (3) **(4)**	**AT-2** (2) (3) **(4)**

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AT-3	Role-Based Training	**AT-3**	**AT-3**	**AT-3**
AT-4	Training Records	AT-4	AT-4	AT-4
AU-1	Policy and Procedures	**AU-1**	**AU-1**	**AU-1**
AU-2	Event Logging	**AU-2**	**AU-2**	**AU-2**
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1)
AU-4	Audit Log Storage Capacity	AU-4 (1)	AU-4 (1)	AU-4 (1)
AU-5	Response to Audit Logging Process Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Record Review, Analysis, and Reporting	AU-6	AU-6 **(1)** (3)	AU-6 **(1)** (3) (5) (6)
AU-7	Audit Record Reduction and Report Generation		AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	**AU-8**	**AU-8**	**AU-8**
AU-9	Protection of Audit Information	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation			**AU-10**
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12 **(1) (3)**
CA-1	Policy and Procedures	**CA-1**	**CA-1**	**CA-1**
CA-2	Control Assessments	**CA-2**	**CA-2** (1)	**CA-2** (1) **(2)**
CA-3	Information Exchange	**CA-3**	**CA-3**	**CA-3** (6)
CA-5	Plan of Action and Milestones	**CA-5**	**CA-5**	**CA-5**
CA-6	Authorization	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	**CA-7** (4)	**CA-7** (1) (4)	**CA-7** (1) (4)
CA-8	Penetration Testing			**CA-8** ~~(1)~~
CA-9	Internal System Connections	**CA-9**	**CA-9**	**CA-9**
CM-1	Policy and Procedures	**CM-1**	**CM-1**	**CM-1**
CM-2	Baseline Configuration	CM-2	CM-2 (2) (3) (7)	CM-2 (2) (3) (7)
CM-3	Configuration Change Control		**CM-3** (2) (4)	**CM-3** (1) (2) (4) (6)
CM-4	Impact Analysis	**CM-4**	**CM-4** (2)	**CM-4** (1) (2)

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
CM-5	Access Restrictions for Change	**CM-5**	**CM-5**	**CM-5** (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	**CM-7**	**CM-7** (1) (2) **(5)**	**CM-7** (1) (2) **(5)**
CM-8	System Component Inventory	CM-8	CM-8 (1) (3)	CM-8 (1) (2) (3) (4)
CM-9	Configuration Management Plan		**CM-9**	**CM-9**
CM-10	Software Usage Restrictions	CM-10	CM-10	CM-10
CM-11	User-Installed Software	CM-11	CM-11	CM-11
CM-12	Information Location		**CM-12** (1)	**CM-12** (1)
CP-1	Policy and Procedures	**CP-1**	**CP-1**	**CP-1**
CP-2	Contingency Plan	**CP-2**	**CP-2** (1) (3) (8)	**CP-2** (1) (2) (3) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) **(2)**
CP-6	Alternate Storage Site		CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site		**CP-7** (1) (2) (3)	**CP-7** (1) (2) (3) (4)
CP-8	Telecommunications Services		**CP-8** (1) (2)	**CP-8** (1) (2) (3) (4)
CP-9	System Backup	CP-9	CP-9 **(1)** (8)	CP-9 **(1)** **(2)** (3) (5) (8)
CP-10	System Recovery and Reconstitution	**CP-10**	**CP-10** (2) **(6)**	**CP-10** (2) (4) **(6)**
CP-12	Safe Mode	CP-12	CP-12	CP-12
IA-1	Policy and Procedures	**IA-1**	**IA-1**	**IA-1**
IA-2	Identification and Authentication (Organizational Users)	**IA-2** **(1)** **(2)** (8) **(12)**	**IA-2** **(1)** **(2)** (8) **(12)**	**IA-2** **(1)** **(2)** **(5)** (8) **(12)**
IA-3	Device Identification and Authentication	IA-3	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4 **(4)**	IA-4 **(4)**
IA-5	Authenticator Management	**IA-5** (1)	**IA-5** (1) (2) (6)	**IA-5** (1) (2) (6)
IA-6	Authentication Feedback	**IA-6**	**IA-6**	**IA-6**
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	**IA-8** **(1)** **(2)** **(4)**	**IA-8** **(1)** **(2)** **(4)**	**IA-8** **(1)** **(2)** **(4)**

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
IA-11	Re-authentication	IR-11	IR-11	IR-11
IA-12	Identity Proofing		**IA-12 (2) (3) (5)**	**IA-12 (1) (2) (3) (4) (5)**
IR-1	Policy and Procedures	**IR-1**	**IR-1**	**IR-1**
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing		IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	**IR-4**	**IR-4** (1)	**IR-4** (1) (4) (11)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5
IR-6	Incident Reporting	**IR-6**	**IR-6 (1)** (3)	**IR-6 (1)** (3)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8
MA-1	Policy and Procedures	**MA-1**	**MA-1**	**MA-1**
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools		MA-3 (1) (2) (3)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (1)	MA-4 (1) **(3)**
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance		MA-6	MA-6
MA-7	Field Maintenance	**MA-7**	**MA-7**	**MA-7**
MP-1	Policy and Procedures	**MP-1**	**MP-1**	**MP-1**
MP-2	Media Access	MP-2	MP-2	MP-2
MP-3	Media Marking		MP-3	MP-3
MP-4	Media Storage		MP-4	MP-4
MP-5	Media Transport		MP-5	MP-5
MP-6	Media Sanitization	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	MP-7	MP-7	MP-7
PE-1	Policy and Procedures	**PE-1**	**PE-1**	**PE-1**
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
PE-3	Physical Access Control	**PE-3**	**PE-3**	**PE-3** (1)
PE-4	Access Control for Transmission		PE-4	PE-4
PE-5	Access Control for Output Devices		PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1) (4)	PE-6 (1) (4)
PE-8	Visitor Access Records	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling		PE-9	PE-9
PE-10	Emergency Shutoff		**PE-10**	**PE-10**
PE-11	Emergency Power		PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	**PE-13**	**PE-13** (1)	**PE-13** (1) (2)
PE-14	Environmental Controls	**PE-14**	**PE-14**	**PE-14**
PE-15	Water Damage Protection	**PE-15**	**PE-15**	**PE-15** (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site		PE-17	PE-17
PE-18	Location of System Components			PE-18
PE-22	Component Marking		**PE-22**	**PE-22**
PL-1	Policy and Procedures	**PL-1**	**PL-1**	**PL-1**
PL-2	System Security and Privacy Plans	**PL-2**	**PL-2**	**PL-2**
PL-4	Rules of Behavior	PL-4 (1)	PL-4 (1)	PL-4 (1)
PL-8	Security and Privacy Architecture		PL-8	PL-8
PL-10	Baseline Selection	PL-10	PL-10	PL-10
PL-11	Baseline Tailoring	PL-11	PL-11	PL-11
PM-1	Information Security Program Plan	PM-1		
PM-2	Information Security Program Leadership Role	PM-2		
PM-3	Information Security and Privacy Resources	PM-3		
PM-4	Plan of Action and Milestones Process	PM-4		

<table>
<tr><th rowspan="2">CNTL NO.</th><th rowspan="2">CONTROL NAME</th><th colspan="3">INITIAL CONTROL BASELINES</th></tr>
<tr><th>LOW</th><th>MOD</th><th>HIGH</th></tr>
<tr><td>PM-5</td><td>System Inventory</td><td colspan="3">PM-5</td></tr>
<tr><td>PM-6</td><td>Measures of Performance</td><td colspan="3">PM-6</td></tr>
<tr><td>PM-7</td><td>Enterprise Architecture</td><td colspan="3">PM-7</td></tr>
<tr><td>PM-8</td><td>Critical Infrastructure Plan</td><td colspan="3">PM-8</td></tr>
<tr><td>PM-9</td><td>Risk Management Strategy</td><td colspan="3">PM-9</td></tr>
<tr><td>PM-10</td><td>Authorization Process</td><td colspan="3">PM-10</td></tr>
<tr><td>PM-11</td><td>Mission and Business Process Definition</td><td colspan="3">PM-11</td></tr>
<tr><td>PM-12</td><td>Insider Threat Program</td><td colspan="3">PM-12</td></tr>
<tr><td>PM-13</td><td>Security and Privacy Workforce</td><td colspan="3">PM-13</td></tr>
<tr><td>PM-14</td><td>Testing, Training, and Monitoring</td><td colspan="3">PM-14</td></tr>
<tr><td>PM-15</td><td>Security and Privacy Groups and Associations</td><td colspan="3">PM-15</td></tr>
<tr><td>PM-16</td><td>Threat Awareness Program</td><td colspan="3">PM-16</td></tr>
<tr><td>PM-17</td><td>Protecting Controlled Unclassified Information on External Systems</td><td colspan="3">PM-17</td></tr>
<tr><td>PM-18</td><td>Privacy Program Plan</td><td colspan="3">PM-18</td></tr>
<tr><td>PM-19</td><td>Privacy Program Leadership Role</td><td colspan="3">PM-19</td></tr>
<tr><td>PM-20</td><td>Dissemination of Privacy Program Information</td><td colspan="3">PM-20 (1)</td></tr>
<tr><td>PM-21</td><td>Accounting of Disclosures</td><td colspan="3">PM-21</td></tr>
<tr><td>PM-22</td><td>Personally Identifiable Information Quality Management</td><td colspan="3">PM-22</td></tr>
<tr><td>PM-23</td><td>Data Governance Body</td><td colspan="3">PM-23</td></tr>
<tr><td>PM-24</td><td>Data Integrity Board</td><td colspan="3">PM-24</td></tr>
<tr><td>PM-25</td><td>Minimization of Personally Identifiable Information Used in Testing, Training, and Research</td><td colspan="3">PM-25</td></tr>
<tr><td>PM-26</td><td>Complaint Management</td><td colspan="3">PM-26</td></tr>
<tr><td>PM-27</td><td>Privacy Reporting</td><td colspan="3">PM-27</td></tr>
<tr><td>PM-28</td><td>Risk Framing</td><td colspan="3">PM-28</td></tr>
<tr><td>PM-29</td><td>Risk Management Program Leadership Roles</td><td colspan="3">PM-29</td></tr>
<tr><td>PM-30</td><td>Supply Chain Risk Management Strategy</td><td colspan="3">PM-30 (1)</td></tr>
</table>

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
PM-31	Continuous Monitoring Strategy	PM-31		
PM-32	Purposing	PM-32		
PS-1	Policy and Procedures	**PS-1**	**PS-1**	**PS-1**
PS-2	Position Risk Designation	**PS-2**	**PS-2**	**PS-2**
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	External Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
PS-9	Position Descriptions	PS-9	PS-9	PS-9
RA-1	Policy and Procedures	**RA-1**	**RA-1**	**RA-1**
RA-2	Security Categorization	**RA-2**	**RA-2**	**RA-2**
RA-3	Risk Assessment	RA-3 (1)	RA-3 (1)	RA-3 (1)
RA-5	Vulnerability Monitoring and Scanning	**RA-5** (2) **(11)**	**RA-5** (2) (5) **(11)**	**RA-5** (2) **(4)** (5) **(11)**
RA-7	Risk Response	RA-7	RA-7	RA-7
RA-9	Criticality Analysis		RA-9	RA-9
SA-1	Policy and Procedures	**SA-1**	**SA-1**	**SA-1**
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3
SA-4	Acquisition Process	**SA-4 (10)** (12)	**SA-4 (1) (2) (9) (10)** (12)	**SA-4 (1) (2)** (5) **(9) (10)** (12)
SA-5	System Documentation	SA-5	SA-5	SA-5
SA-8	Security and Privacy Engineering Principles	SA-8	SA-8	SA-8
SA-9	External System Services	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management		**SA-10**	**SA-10**
SA-11	Developer Testing and Evaluation		SA-11	SA-11

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
SA-15	Development Process, Standards, and Tools		SA-15 (3)	SA-15 (3)
SA-16	Developer-Provided Training			SA-16
SA-17	Developer Security Architecture and Design			SA-17
SA-21	Developer Screening			SA-21
SA-22	Unsupported System Components	**SA-22**	**SA-22**	**SA-22**
SC-1	Policy and Procedures	**SC-1**	**SC-1**	**SC-1**
SC-2	Separation of System and User Functionality		**SC-2**	**SC-2**
SC-3	Security Function Isolation			**SC-3**
SC-4	Information in System Shared Resources		**SC-4**	**SC-4**
SC-5	Denial-of-Service Protection	**SC-5**	**SC-5**	**SC-5**
SC-7	Boundary Protection	SC-7 **(28)** **(29)**	SC-7 (3) (4) (5) (7) (8) **(18)** **(28)** **(29)**	SC-7 (3) (4) (5) (7) (8) **(18)** (21) **(28)** **(29)**
SC-8	Transmission Confidentiality and Integrity		SC-8 **(1)**	SC-8 **(1)**
SC-10	Network Disconnect		~~SC-10~~	~~SC-10~~
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices and Applications	SC-15	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates		SC-17	SC-17
SC-18	Mobile Code		SC-18	SC-18
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	**SC-20**	**SC-20**	**SC-20**
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	**SC-21**	**SC-21**	**SC-21**
SC-22	Architecture and Provisioning for Name/Address Resolution Service	**SC-22**	**SC-22**	**SC-22**
SC-23	Session Authenticity		**SC-23**	**SC-23**
SC-24	Fail in Known State		**SC-24**	**SC-24**
SC-28	Protection of Information at Rest		**SC-28** (1)	**SC-28** (1)
SC-39	Process Isolation	**SC-39**	**SC-39**	**SC-39**
SC-41	Port and I/O Device Access	SC-41	SC-41	SC-41

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
SC-45	System Time Synchronization	**SC-45**	**SC-45**	**SC-45**
SC-47	Alternate Communications Path			**SC-47**
SI-1	Policy and Procedures	**SI-1**	**SI-1**	**SI-1**
SI-2	Flaw Remediation	**SI-2**	**SI-2** (2)	**SI-2** (2)
SI-3	Malicious Code Protection	**SI-3**	**SI-3**	**SI-3**
SI-4	System Monitoring	**SI-4**	**SI-4 (2)** (4) **(5)**	**SI-4 (2)** (4) **(5)** (10) (12) (14) (20) (22)
SI-5	Security Alerts, Advisories, and Directives	**SI-5**	**SI-5**	**SI-5** (1)
SI-6	Security and Privacy Function Verification			**SI-6**
SI-7	Software, Firmware, and Information Integrity		**SI-7 (1) (7)**	**SI-7 (1) (2) (5) (7) (15)**
SI-8	Spam Protection		**SI-8** ~~(2)~~	**SI-8** ~~(2)~~
SI-10	Information Input Validation		SI-10	SI-10
SI-11	Error Handling		SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention			SI-13
SI-16	Memory Protection		SI-16	SI-16
SI-17	Fail-Safe Procedures	**SI-17**	**SI-17**	**SI-17**
SR-1	Policy and Procedures	**SR-1**	**SR-1**	**SR-1**
SR-2	Supply Chain Risk Management Plan	SR-2 (1)	SR-2 (1)	SR-2 (1)
SR-3	Supply Chain Controls and Processes	SR-3	SR-3	SR-3
SR-5	Acquisition Strategies, Tools, and Methods	SR-5	SR-5 **(1)**	SR-5 **(1)**
SR-6	Supplier Assessments and Reviews		SR-6	SR-6
SR-8	Notification Agreements	SR-8	SR-8	SR-8
SR-9	Tamper Resistance and Detection			SR-9 (1)
SR-10	Inspection of Systems or Components	SR-10	SR-10	SR-10
SR-11	Component Authenticity	SR-11 (1) (2)	SR-11 (1) (2)	SR-11 (1) (2)
SR-12	Component Disposal	SR-12	SR-12	SR-12

F.4 Tailoring Considerations

The OT overlay in this publication leverages the SP 800-53B control baselines accounting for the unique characteristics of OT systems, such as an increased need for availability, safety, and environmental/operating environment considerations. Additionally, OT systems vary widely in their architecture and technology selection. The SP 800-53B control baselines were tailored for these general considerations, including addition of controls relevant for OT environments. Organizations can use this overlay as a starting point and further tailor controls to meet specific operational needs to address variability of OT systems.

As organizations further tailor controls to meet their internal security requirements, limitations (e.g., technology, operational constraints, environmental considerations) may necessitate selecting compensating controls. Compensating controls in the OT environment may be required in situations where the OT cannot support certain controls or control enhancements, or the organization determines it is not advisable to implement controls or control enhancements due to potential adverse impacts to performance, safety, or reliability. Compensating controls are alternatives to a specific baseline control or enhancement that provide equivalent or comparable protection. For example, if controls or control enhancements require automated mechanisms which are not readily available, cost effective, or technically feasible in OT environments, compensating controls implemented through nonautomated mechanisms or procedures may be acceptable to meet the intent of the control.

Compensating controls implemented in accordance with PL-11 from SP 800-53 Rev. 5 are not considered exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the OT environment that accomplish the intent of the original controls that could not be effectively employed. See "Control Tailoring" in Section 3.3 of SP 800-37 Rev. 2 [SP800-37r2].

Using compensating controls may also include control enhancements that supplement the baseline. Using compensating controls typically involves a trade-off between additional risk and reduced functionality. Every use of compensating controls should involve a risk-based determination of how much residual risk to accept and how much functionality to reduce. Additionally, when compensating controls are employed, organizations should document the rationale describing:

- why the baseline control could not be implemented;
- how the compensating control(s) provide equivalent security capabilities for OT systems; and
- the risk acceptance for any residual risk resulting from using the compensating control(s) instead of the baseline control.

Organizational decisions on the use of compensating controls are documented in the security plan for the OT.

Controls that contain assignments (e.g., *Assignment: organization-defined conditions or trigger events*) may be tailored out of the baseline. This is equivalent to assigning a value of "none." The assignment may take on different values for different impact baselines.

F.5 OT Communication Protocols

The unique network properties within OT may warrant specific attention when applying certain controls. Many of the controls in NIST SP 800-53 Rev. 5 that pertain to communication, devices, and interfaces implicitly assume the applicability of network routing or communication between network segments or zones. Some devices, or subsystems, used in OT may be configured or architected in a way that may create an exception to this assumption. As a result, controls for devices that communicate using standards and protocols that do not include network addressing generally require tailoring. An RS-232 (serial) interface is an example of a non-network addressable or routable communication method that is commonly employed in OT equipment.

F.6 Definitions

Terms used in this overlay are defined in the CSRC glossary.

F.7 Detailed Overlay Control Specifications

This overlay is based on NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* [SP800-53r5], which provides a catalog of security and privacy controls, and NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* [SP800-53B]. The controls are customizable and implemented as part of an organization-wide process that manages security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, and are derived from legislation, Executive Orders, policies, directives, regulations, standards, and mission/business needs. The documents also describe how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog controls address security from both a functionality perspective (the strength of security and privacy functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented capability). Addressing both functionality and assurance helps to ensure that component products and the systems built from those products using sound system and security engineering principles are sufficiently trustworthy.

In preparation for selecting and specifying the appropriate controls for organizational systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. This process is known as security categorization. FIPS 199 [FIPS199] enables federal agencies to establish security categories for both information and information systems. Other documents, such as those produced by ISA and CNSS, also provide guidance for defining low, moderate, and high levels of security based on impact. The security categories are based on the potential impact on an organization or on people (employees and/or the public) should certain events occur which jeopardize the information and systems needed by the organization to accomplish its assigned mission, such as protecting its assets, fulfilling its legal responsibilities, maintaining its day-to-day functions, and protecting individuals' safety, health, and life. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

This overlay provides OT Discussion for the controls and control enhancements prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its data and to meet a set of defined security requirements. Discussions for all controls and control enhancements in SP 800-53 Rev. 5, Chapter 3 should be used in conjunction with the OT Discussions in this overlay. This overlay contains a tailoring of the control baselines; its specification may be more stringent or less stringent than the original control baseline specification. It can be applied to multiple systems. This overlay is high-level, applicable to all OT environments; it may be used as the basis for more specific overlays. Use cases for specific systems in specific environments may be separately published (e.g., as a NISTIR).

Figure 22 uses the AU-4 control as an example of the format and content of the detailed overlay control specifications.

❶ Control number and title

❷ Column for control and control enhancement number

❸ Column for control and control enhancement name

❹ Columns for baselines. If the baselines have been supplemented, then SUPPLEMENTED appears.

❺ A row for each control or control enhancement

❻ Columns for LOW, MODERATE, and HIGH baselines

❼ "Select" indicates the control is selected in NIST SP 800-53 Rev. 5. "Add" indicates the control is added to a baseline in the OT overlay. A blank cell indicates the control is not selected. "~~Remove~~" indicates the control is removed from the baseline.

❽ The OT Discussion. If there is none, that is stated.

❾ The control enhancement OT Discussion. If there is none, that is stated.

❿ The rationale for changing the presence of a control or control enhancement in the baseline

❶**AC-3 ACCESS ENFORCEMENT**

❷CNTL NO.	❸CONTROL NAME *Control Enhancement Name*	❹SUPPLEMENTED ❻CONTROL BASELINES		
		LOW	MOD	HIGH
❺**AC-3**	**Access Enforcement**	**Select**	**Select**	❼ **Select**
AC-3 (11)	*ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES*			**Add**

❽ OT Discussion: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the OT. Example compensating controls include encapsulation. Policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control; however, it may not provide sufficient granularity in situations where users require access to different functions.

❾ Control Enhancement: (11) OT Discussion: The organization identifies and restricts access to information that could impact the OT environment, accounting for information types that are sensitive, proprietary, contain trade secrets, or support safety functions.

❿ Rationale for adding AC-3 (11) to HIGH baseline: The loss of availability, integrity, and confidentiality of certain types of information residing on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals that include severe degradation or loss of mission capability, major damage to organizational assets, or result in harm to individuals involving loss of life or life-threatening injuries.

Figure 22: Detailed Overlay Control Specifications Illustrated

F.7.1 ACCESS CONTROL – AC

Tailoring Considerations for the Access Control Family

Before implementing controls in the AC family, consider the tradeoffs among security, privacy, latency, performance, throughput, and reliability. For example, the organization considers whether latency induced from the use of confidentiality and integrity mechanisms employing cryptographic mechanisms would adversely impact the operational performance of the OT.

In situations where the OT cannot support the specific Access Control requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems. OT access by vendors and maintenance staff can occur over a very large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.

AC-2 ACCOUNT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	**Select**	**Select**	**Select**
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Select	Select
AC-2 (2)	*ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT*		**Select**	**Select**
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS*		Select	Select
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Select	Select
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*		**Select**	**Select**
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Select
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE*			Select
AC-2 (13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*		**Select**	**Select**

OT Discussion: In OT systems, physical security, personnel security, intrusion detection, or auditing measures may assist in supporting this control objective.

Control Enhancement: (1) (3) (4) No OT Discussion for this control.

Control Enhancement: (2) OT Discussion: In situations where the OT (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (5) OT Discussion: This control enhancement defines situations or timeframes in which users log out of accounts in policy; automatic enforcement is not addressed by this control enhancement. Organizations determine if this control enhancement is appropriate for the mission and/or functions of the OT system and define the timeframe or scenarios. If no timeframe or scenario(s) apply, the organization-defined parameter reflects as such.

Control Enhancement: (11) (12) No OT Discussion for this control.

Control Enhancement: (13) OT Discussion: Close coordination occurs between OT, Human Resources (HR), IT, and Physical Security personnel to ensure the timely removal of high-risk individuals.

AC-3 ACCESS ENFORCEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AC-3	**Access Enforcement**	**Select**	**Select**	**Select**
AC-3 (11)	*ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES*			**Add**

OT Discussion: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the OT. Example compensating controls include encapsulation. Policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control; however, it may not provide sufficient granularity in situations where users require access to different functions.

Control Enhancement: (11) OT Discussion: The organization identifies and restricts access to information that could impact the OT environment, accounting for information types that are sensitive, proprietary, contain trade secrets, or support safety functions.

Rationale for adding AC-3 (11) to HIGH baseline: The loss of availability, integrity, and confidentiality of certain types of information residing on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals that include severe degradation or loss of mission capability, major damage to organizational assets, or result in harm to individuals involving loss of life or life-threatening injuries.

AC-4 INFORMATION FLOW ENFORCEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-4	**Information Flow Enforcement**		**Select**	**Select**
AC-4 (4)	*INFORMATION FLOW ENFORCEMENT | FLOW CONTROL OF ENCRYPTED INFORMATION*			Select

OT Discussion: Information flow policy may be achieved using a combination of logical and physical flow restriction techniques. Inspection of message content may enforce information flow policy. For example, industrial OT protocols may be restricted using inbound and outbound traffic rules on a network control device between OT and IT networks. For non-routable communication such as serial connections, devices may be configured to limit commands to and from specific tags within the OT device. Information flow policy may be supported by labeling or coloring physical connectors to aid in connecting networks. Devices that do not have a business need to communicate should not be connected (i.e., air gapped).

Control Enhancement: (4) No OT discussion for this control.

AC-5 SEPARATION OF DUTIES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-5	**Separation of Duties**		**Select**	**Select**

OT Discussion: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6 LEAST PRIVILEGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-6	**Least Privilege**		**Select**	**Select**
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*		**Select**	**Select**
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*		**Select**	**Select**
AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*			**Select**
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*		**Select**	**Select**
AC-6 (7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*		Select	Select
AC-6 (9)	*LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS*		**Select**	**Select**
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*		**Select**	**Select**

OT Discussion: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual having multiple critical privileges. System privilege models may be tailored to enforce integrity and availability (e.g., lower privileges include read access and higher privileges include write access).

Control Enhancement: (1) (2) (3) (5) (9) OT Discussion: In situations where the OT components (e.g., PLCs) cannot support logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

Control Enhancement: (7) No OT Discussion for this control.

Control Enhancement: (10) OT Discussion: Example compensating controls include enhanced auditing.

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-7	Unsuccessful Logon Attempts	Select	Select	Select

OT Discussion: Many OT systems remain in continuous operation and operators remain logged onto the system at all times. A "log-over" capability may be employed. Example compensating controls include logging or recording all unsuccessful login attempts and alerting OT security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded. Unsuccessful logon attempt limits are enforced for accounts (e.g., administrator) or systems (e.g., engineering workstations) not required for continuous operation.

AC-8 SYSTEM USE NOTIFICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-8	System Use Notification	Select	Select	Select

OT Discussion: Many OT systems must remain in continuous operation and system use notification may not be supported or effective. Example compensating controls include posting physical notices in OT facilities or providing recurring training on system use prior to permitting access.

AC-10 CONCURRENT SESSION CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-10	Concurrent Session Control			Select

OT Discussion: The number, account type, and privileges of concurrent sessions considers the roles and responsibilities of the affected individuals. Example compensating controls include providing increased auditing measures.

AC-11 DEVICE LOCK

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-11	**Device Lock**		**Select**	**Select**
AC-11 (1)	*DEVICE LOCK | PATTERN-HIDING DISPLAYS*		**Select**	**Select**

OT Discussion: This control assumes a staffed environment where users interact with system displays. This control may be tailored appropriately where systems do not have displays configured, systems are placed in an access-controlled facility or locked enclosure, or immediate operator response is required in emergency situations. Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

Control Enhancement: (1) OT Discussion: Physical protection may be employed to prevent access to a display or prevent attachment of a display. In situations where the OT cannot conceal displayed information, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-12 SESSION TERMINATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-12	**Session Termination**		**Select**	**Select**

OT Discussion: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-14	**Permitted Actions without Identification or Authentication**	Select	Select	Select

No OT Discussion for this control.

AC-17 REMOTE ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AC-17	**Remote Access**	**Select**	**Select**	**Select**
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*		**Select**	**Select**
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*		**Select**	**Select**
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*		**Select**	**Select**
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*		Select	Select
AC-17 (9)	*REMOTE ACCESS | DISCONNECT OR DISABLE ACCESS*	**Add**	**Add**	**Add**
AC-17 (10)	*REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS*		Add	Add

OT Discussion: In situations where the OT cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1) OT Discussion: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls. Compensating controls could include limiting remote access to a specified period of time or placing a call from the OT site to the authenticated remote entity.

Control Enhancement: (2) OT Discussion: Encryption-based technologies should be used to support the confidentiality and integrity of remote access sessions. While OT devices often lack the ability to support modern encryption, additional devices (e.g., VPNs) can be added to support these features. This control should not be confused with SC-8 – Transmission Confidentiality and Integrity, which discusses confidentiality and integrity requirements for general communications, including between OT devices.

Control Enhancement: (3) OT Discussion: Example compensating controls include connection-specific manual authentication of the remote entity.

Control Enhancement: (4) (10) No OT Discussion for this control.

Control Enhancement: (9) OT Discussion: Implementation of the remote access disconnect should not impact OT operations. OT personnel should be trained on how to use the remote access disconnect.

Rationale for adding AC-17 (9) to LOW, MOD and HIGH baselines: As more OT systems become accessible remotely, the capability to disconnect or disable remote access is critical to manage risk. Disconnect of remote access may be required to provide stable and safe operations.

Rationale for adding AC-17 (10) to MOD and HIGH baselines: The ability to authenticate remote commands is important to prevent unauthorized commands that may have immediate or serious consequences such as injury, death, property damage, loss of high-value assets, failure of mission or business functions, or compromise of sensitive information.

AC-18 WIRELESS ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-18	**Wireless Access**	**Select**	**Select**	**Select**
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*		**Select**	**Select**
AC-18 (3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*		Select	Select
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*			Select
AC-18 (5)	*WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS*			**Select**

OT Discussion: In situations where OT cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1) OT Discussion: Implementation of authentication and encryption is driven by the OT environment. There are some scenarios where devices and users cannot all be authenticated and encrypted due to operational or technology constraints. In such scenarios, compensating controls include providing increased auditing for wireless access, limiting wireless access privileges to key personnel, or using AC-18 (5) to reduce the boundary of wireless access.

Control Enhancement: (3) (4) No OT Discussion for this control.

Control Enhancement: (5) Availability and interference for wireless signals may be a concern within OT environments. Antennas and power levels should be designed to overcome and achieve availability goals. Where confidentiality is concerned, antennas and power levels can also be designed to minimize signal exposure outside of the facility.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-19	**Access Control for Mobile Devices**	Select	Select	Select
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*		Select	Select

No OT Discussion for this control.

AC-20 USE OF EXTERNAL SYSTEMS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-20	**Use of External Systems**	**Select**	**Select**	**Select**
AC-20 (1)	*USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE*		Select	Select
AC-20 (2)	*USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE MEDIA*		Select	Select

OT Discussion: Organizations refine the definition of "external" to reflect lines of authority and responsibility; granularity of organization entity; and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, falls under different management authorities, or does not provide sufficient visibility into the implementation of controls to allow the establishment of a satisfactory trust relationship. For example, an OT system and a business data processing system may be considered external to each other depending on the organization's system boundaries.

Access to an OT for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external systems is reexamined with respect to OT functions, purposes, technology, and limitations to establish a clearly documented technical or business case for use and an acceptance of the risk inherent in the use of an external system.

Control Enhancement: (1) (2) No OT Discussion for this control.

AC-21 INFORMATION SHARING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-21	**Information Sharing**		Select	Select

No OT Discussion for this control.

AC-22 PUBLICLY ACCESSIBLE CONTENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-22	**Publicly Accessible Content**	**Select**	**Select**	**Select**

OT Discussion: Generally, public access to OT systems is not permitted. Select information may be transferred to a publicly accessible system, possibly with added controls. The organization should review what information is being made accessible prior to publication.

F.7.2 AWARENESS AND TRAINING – AT

AT-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

AT-2 LITERACY TRAINING AND AWARENESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AT-2	**Literacy Training and Awareness**	**Select**	**Select**	**Select**
AT-2 (2)	*LITERACY TRAINING AND AWARENESS | INSIDER THREAT*	Select	Select	Select
AT-2 (3)	*LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING*		Select	Select
AT-2 (4)	*LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*		**Add**	**Add**

OT Discussion: Security awareness training includes initial and periodic review of OT-specific policies, standard operating procedures, security trends, and vulnerabilities. The OT security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

Control Enhancement: (2) (3) No OT Discussion for this control.

Control Enhancement: (4) OT Discussion: Identify and communicate suspicious and anomalous behaviors within the OT environment. Some examples of OT suspicious or anomalous behavior may include a PLC still in programming mode when it is expected to be in run mode, process trips with undetermined root cause, malware on an HMI, unexpected mouse movement, or process changes that are not being performed by the operator.

Rationale for adding AT-2 (4) to MOD and HIGH baselines: Training OT personnel on potentially suspicious communications/anomalous behaviors, and actions to take if anomalous system behavior occurs, can supplement system detection and protection mechanisms for improved response.

AT-3 ROLE-BASED TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-3	**Role-Based Training**	**Select**	**Select**	**Select**

OT Discussion: Security training includes initial and periodic review of OT-specific policies, standard operating procedures, security trends, and vulnerabilities. The OT security training program is consistent with the requirements of the security awareness and training policy established by the organization. The training may be customized for specific OT roles, which could include operators, maintainers, engineers, supervisors, and administrators.

AT-4 TRAINING RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-4	**Training Records**	Select	Select	Select

No OT Discussion for this control.

F.7.3 AUDITING AND ACCOUNTABILITY – AU

Tailoring Considerations for the Audit Family

In general, security audit information and audit tools are not available on legacy OT. In situations where OT cannot support the specific audit and accountability requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. For example, organizations may want to consider if security audit information is available from separate systems or system components (e.g., the historian, firewall logs, physical security systems). Additional examples of compensating controls are given with each control as appropriate.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

AU-2 EVENT LOGGING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-2	**Event Logging**	**Select**	**Select**	**Select**

OT Discussion: Organizations may want to include relevant OT events (e.g., alerts, alarms, configuration and status changes, operator actions) in their event logging, which may be designated as audit events.

AU-3 CONTENT OF AUDIT RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-3	**Content of Audit Records**	Select	Select	Select
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*		Select	Select

No OT Discussion for this control.

AU-4 AUDIT LOG STORAGE CAPACITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AU-4	**Audit Log Storage Capacity**	Select	Select	Select
AU-4 (1)	*AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Add	Add	Add

No OT Discussion for this control.

Rationale for adding AU-4 (1) to LOW, MOD and HIGH baselines: Organizational requirements may require storage of very large amounts of data, which OT components may not be able to support directly.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-5	**Response to Audit Logging Process Failures**	Select	Select	Select
AU-5 (1)	*RESPONSE TO AUDIT LOGGING PROCESS FAILURES | AUDIT STORAGE CAPACITY*			Select
AU-5 (2)	*RESPONSE TO AUDIT LOGGING PROCESS FAILURES | REAL-TIME ALERTS*			Select

No OT Discussion for this control.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-6	**Audit Review, Analysis, and Reporting**	Select	Select	Select
AU-6 (1)	*AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION*		**Select**	**Select**
AU-6 (3)	*AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES*		Select	Select
AU-6 (5)	*AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS*			Select
AU-6 (6)	*AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*			Select

No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: Example compensating controls include manual mechanisms or procedures. For devices where audit records cannot be feasibly collected, periodic manual review may be necessary.

Control Enhancement: (3) (5) (6) No OT Discussion for this control.

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-7	**Audit Record Reduction and Report Generation**		Select	Select
AU-7 (1)	*AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		Select	Select

No OT Discussion for this control.

AU-8 TIME STAMPS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-8	**Time Stamps**	**Select**	**Select**	**Select**

OT Discussion: Example compensating controls include using a separate system designated as an authoritative time source. See related control SC-45.

AU-9 PROTECTION OF AUDIT INFORMATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-9	**Protection of Audit Information**	Select	Select	Select
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS*			Select
AU-9 (3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*			Select
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*		Select	Select

No OT Discussion for this control.

AU-10 NON-REPUDIATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-10	**Non-Repudiation**			**Select**

OT Discussion: OT devices may not enforce non-repudiation of audit records and may require compensating controls. Example compensating controls include physical security systems, cameras to monitor user access, or a separate device for log collection.

AU-11 AUDIT RECORD RETENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-11	**Audit Record Retention**	Select	Select	Select

No OT Discussion for this control.

AU-12 AUDIT RECORD GENERATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-12	**Audit Record Generation**	Select	Select	Select
AU-12 (1)	*AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL*			**Select**
AU-12 (3)	*AUDIT RECORD GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*			**Select**

No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: Example compensating controls include providing time-correlated audit records on a separate system.

Control Enhancement: (3) OT Discussion: Example compensating controls include employing nonautomated mechanisms or procedures.

F.7.4 ASSESSMENT, AUTHORIZATION, AND MONITORING – CA

Tailoring Considerations for the Security Assessment and Authorization Family

In situations where the OT cannot support specific assessment, authorization, and monitoring requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

CA-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

CA-2 CONTROL ASSESSMENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-2	**Control Assessments**	**Select**	**Select**	**Select**
CA-2 (1)	*CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS*		Select	Select
CA-2 (2)	*CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS*			**Select**

OT Discussion: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing OT) authorized by the organization. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the OT security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. The organization ensures that the assessment does not affect system operation or result in unintentional system modification. If assessment activities must be performed on the production OT, it may need to be taken off-line before an assessment can be conducted, or the assessment should be scheduled to occur during planned OT outages whenever possible.

Control Enhancement: (1) No OT Discussion on this control.

Control Enhancement: (2) OT Discussion: The organization conducts risk analysis to support selection of an assessment target (e.g., the live system, an off-line replica or lab system).

CA-3 INFORMATION EXCHANGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-3	**Information Exchange**	**Select**	**Select**	**Select**
CA-3 (6)	*INFORMATION EXCHANGE | TRANSFER AUTHORIZATION*			Select

OT Discussion: Organizations perform risk-benefit analysis to support determining whether an OT should be connected to other system(s). The authorizing official (AO) fully understands the organizational information security policies and procedures; the OT security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the nation associated with the connection to other system(s); the individuals and organizations that operate and maintain the systems, including maintenance contractors or service providers; and the specific health, safety, and environmental risks associated with a particular interconnection. Connections from the OT environment to other security zones may cross the authorization boundary, such that two different authorizing officials may be required to approve the connection. Decisions to accept risk are documented.

Control Enhancement: (6) No OT Discussion for this control.

CA-5 PLAN OF ACTION AND MILESTONES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-5	**Plan of Action and Milestones**	**Select**	**Select**	**Select**

OT Discussion: Corrective actions identified in assessments may not be immediately actionable in an OT environment; therefore, short-term mitigations may be implemented to reduce risk as part of the gap closure plan or plan of action and milestones.

CA-6 AUTHORIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-6	**Authorization**	Select	Select	Select

No OT Discussion for this control.

CA-7 CONTINUOUS MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-7	**Continuous Monitoring**	**Select**	**Select**	**Select**
CA-7 (1)	*CONTINUOUS MONITORING* | *INDEPENDENT ASSESSMENT*		Select	Select
CA-7 (4)	*CONTINUOUS MONITORING* | *RISK MONITORING*	Select	Select	Select

OT Discussion: Continuous monitoring programs for OT are designed, documented, and implemented with input from OT personnel. The organization ensures that continuous monitoring does not interfere with OT functions. The individual/group designing and conducting the continuous monitoring for the OT systems implements monitoring consistent with the organizational information security policies and procedures, the OT security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Continuous monitoring can be automated or manual at a frequency sufficient to support risk-based decisions. For example, the organization may determine for lower-risk, isolated systems to monitor event logs manually on a specified frequency less often than for higher-risk, networked systems.

Control Enhancement: (1) (4) No OT Discussion for this control.

CA-8 PENETRATION TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-8	**Penetration Testing**			**Select**
CA-8 (1)	*PENETRATION TESTING* | *INDEPENDENT PENETRATION TESTING AGENT OR TEAM*			~~Remove~~

OT Discussion: Penetration testing is used with care on OT networks to ensure that OT functions are not adversely impacted by the testing process. In general, OT systems are highly sensitive to timing constraints and have limited resources. Example compensating controls include employing a replicated, virtualized, or simulated system to conduct penetration testing. Production OT may need to be taken off-line before testing can be conducted. If OT systems are taken off-line for testing, tests are scheduled to occur during planned OT outages whenever possible. If penetration testing is performed on non-OT networks, extra care is taken to ensure that tests do not propagate into the OT network.

Rationale for removing CA-8 (1) from HIGH baseline: Specific expertise is necessary to conduct effective penetration testing on OT systems; it may not be feasible to identify independent personnel with the appropriate skillset/knowledge to perform penetration testing on an OT environment. While an independent penetration test agent/team is recommended, it may not be feasible for all high-impact OT systems.

CA-9 INTERNAL SYSTEM CONNECTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-9	**Internal System Connections**	**Select**	**Select**	**Select**

OT Discussion: Organizations perform risk-benefit analysis to determine whether OT equipment should be connected to other internal system components, then document these connections. The AO fully understands the potential risks associated with approving individual connections or approving a class of components to be connected. As an example, the AO may broadly approve the connection of any sensors limited to 4 to 20 milliamp (mA) communication, while other connection types (e.g., serial or ethernet) require individual approval. Decisions to accept risk are documented.

F.7.5 CONFIGURATION MANAGEMENT – CM

Tailoring Considerations for the Configuration Management Family

In situations where the OT cannot be configured to restrict the use of unnecessary functions or cannot support the use of automated mechanisms to implement configuration management functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

CM-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

CM-2 BASELINE CONFIGURATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-2	**Baseline Configuration**	Select	Select	Select
CM-2 (2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		Select	Select
CM-2 (3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		Select	Select
CM-2 (7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		Select	Select

No OT Discussion for this control.

CM-3 CONFIGURATION CHANGE CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-3	**Configuration Change Control**		**Select**	**Select**
CM-3 (1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*			Select
CM-3 (2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*		Select	Select
CM-3 (4)	*CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES*		Select	Select
CM-3 (6)	*CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*			Select
CM-3 (7)	*CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES*			
CM-3 (8)	*CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES*			

OT Discussion: Configuration change control procedures should align with the organization's management of change practices.

Control Enhancement: (1) (2) (4) (6): No OT Discussion for this control.

Control Enhancement: (7) OT Discussion: The organization takes into consideration OT-specific requirements when determining frequency and/or circumstances for reviewing system changes. As an example, safety instrumented systems may be justified for review of system changes on a predetermined frequency to ensure that no inadvertent changes have been made to the logic solver portion of a safety instrumented function.

Control Enhancement: (8) OT Discussion: The organization prevents or restricts configuration changes based on a risk determination that the system should not be modified without additional permission. For example, some PLCs have physical key switches that are used to place the PLC in a mode that allows for programming changes. Physical key switches can restrict configuration changes so that physical access is required to make a modification to the system.

CM-4 IMPACT ANALYSES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-4	**Impact Analyses**	**Select**	**Select**	**Select**
CM-4 (1)	*IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS*			Select
CM-4 (2)	*IMPACT ANALYSES | VERIFICATION OF CONTROLS*		Select	Select

OT Discussion: The organization considers OT safety and security interdependencies. OT security and safety personnel are included in change process management if the change to the system may have an impact on safety or security.

Control Enhancement: (1) (2) No OT Discussion for this control.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-5	**Access Restrictions for Change**	**Select**	**Select**	**Select**
CM-5 (1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*			Select

OT Discussion: Some OT devices allow for the configuration and use of mode change switches. Where available, these should be used to prevent unauthorized changes. As an example, many PLCs have key switches that allow the device to be placed in a programming mode or a running mode. Those PLCs should be placed in a running or remote mode to prevent unauthorized programming changes, and the key should be removed from the key switch and managed appropriately.

Control Enhancement: (1) No OT Discussion for this control.

CM-6 CONFIGURATION SETTINGS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-6	**Configuration Settings**	Select	Select	Select
CM-6 (1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*			Select
CM-6 (2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*			Select

No OT Discussion for this control.

CM-7 LEAST FUNCTIONALITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-7	**Least Functionality**	**Select**	**Select**	**Select**
CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*		Select	Select
CM-7 (2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*		Select	Select

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION*		**Select**	**Select**

OT Discussion: The organization implements least functionality by allowing only specified functions, protocols, and/or services required for OT operations. For non-routable protocols such as serial communications, interrupts could be disabled or set points could be made read-only except for privileged users to limit functionality. Ports are part of the address space in network protocols and are often associated with specific protocols or functions. For routable protocols, ports can be disabled on many networking devices to limit functionality to the minimum required for operation.

Control Enhancement: (1) (2) No OT Discussion.

Control Enhancement: (5) OT Discussion: The set of applications that run in OT is relatively static, making allowlisting practical. DHS recommends using application allowlisting for OT equipment.

CM-8 SYSTEM COMPONENT INVENTORY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-8	**System Component Inventory**	Select	Select	Select
CM-8 (1)	*SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		Select	Select
CM-8 (2)	*SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*			Select
CM-8 (3)	*SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		Select	Select
CM-8 (4)	*SYSTEM COMPONENT INVENTORY | PROPERTY ACCOUNTABILITY INFORMATION*			Select

No OT Discussion for this control.

CM-9 CONFIGURATION MANAGEMENT PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-9	**Configuration Management Plan**		**Select**	**Select**

OT Discussion: Configuration management plans apply to internal and external (e.g., contractors, integrators) resources responsible for device configuration.

CM-10 SOFTWARE USAGE RESTRICTIONS

CNTL no.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-10	**Software Usage Restrictions**	Select	Select	Select

No OT Discussion for this control.

CM-11 USER-INSTALLED SOFTWARE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-11	**User-Installed Software**	Select	Select	Select

No OT Discussion for this control.

CM-12 INFORMATION LOCATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-12	**Information Location**		**Select**	**Select**
CM-12 (1)	*INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION*		Select	Select

OT Discussion: Organizations identify specific information types or components to track where information is being processed and stored. Information to consider in the OT environment may include shared account passwords; PLC backup files; detailed network drawings; and risk assessments that identify specific threats with the environment.

Control Enhancement: (1) No OT Discussion for this control.

F.7.6 CONTINGENCY PLANNING - CP

Tailoring Considerations for the Contingency Planning Family

OT systems often contain a physical component at a fixed location. Such components may not be relocated logically. Some replacement components may not be readily available. Continuance of essential missions and business functions with little or no loss of operational continuity may not be possible. In situations where the organization cannot provide necessary essential services, support, or automated mechanisms during contingency operations, the organization provides nonautomated mechanisms or predetermined procedures as compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

CP-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

CP-2 CONTINGENCY PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-2	**Contingency Plan**	**Select**	**Select**	**Select**
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*		Select	Select
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*			Select
CP-2 (3)	*CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS*		Select	Select
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS*			Select
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*		Select	Select

OT Discussion: The organization defines contingency plans for categories of disruptions or failures. In the case of a contingency, the OT equipment executes preprogrammed functions such as alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, or alert the operator and then maintain the last operational setting prior to failure. Contingency plans for widespread disruption may involve specialized organizations (e.g., FEMA, emergency services, regulatory authorities).

Control Enhancement: (1) (2) (3) (5) (8) No OT Discussion for this control.

CP-3 CONTINGENCY TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-3	**Contingency Training**	Select	Select	Select
CP-3 (1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*			Select

No OT Discussion for this control.

CP-4 CONTINGENCY PLAN TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-4	**Contingency Plan Testing**	Select	Select	Select
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		Select	Select
CP-4 (2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*			**Select**

No OT Discussion for this control.

Control Enhancement: (1) No OT Discussion for this control.

Control Enhancement: (2) OT Discussion: Not all systems will have alternate processing sites as discussed in CP-7.

CP-6 ALTERNATE STORAGE SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-6	**Alternate Storage Site**		Select	Select
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*		Select	Select
CP-6 (2)	*ALTERNATE STORAGE SITE | RECOVERY TIME AND RECOVERY POINT OBJECTIVES*			Select
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*		Select	Select

No OT Discussion for this control.

CP-7 ALTERNATE PROCESSING SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-7	**Alternate Processing Site**		**Select**	**Select**
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*		Select	Select
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*		Select	Select
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*		Select	Select
CP-7 (4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*			Select

OT Discussion: Many site-wide supervisory or optimization servers (i.e., Level 3 and above of the Purdue model) can be supported from an alternative processing site. It is likely not feasible for control systems or field devices, such as sensors or final elements (i.e., Level 1 and 0 of the Purdue model), to be made available from an alternative processing site.

Control Enhancement: (1) (2) (3) (4) No OT Discussion for this control.

CP-8 TELECOMMUNICATIONS SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-8	**Telecommunications Services**		**Select**	**Select**
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*		Select	Select
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*		Select	Select
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS*			Select
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*			Select

OT Discussion: Quality of service factors for OT include latency and throughput.

Control Enhancement: (1) (2) (3) (4) No OT Discussion for this control.

CP-9 SYSTEM BACKUP

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-9	**System Backup**	Select	Select	Select
CP-9 (1)	*SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY*		**Select**	**Select**
CP-9 (2)	*SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*			**Select**
CP-9 (3)	*SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*			Select
CP-9 (5)	*SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*			Select
CP-9 (8)	*SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION*		Select	Select

No OT Discussion for this control.

Control Enhancement: (1) (2) OT Discussion: Testing for reliability and integrity increases confidence that the system can be restored after an incident, and minimizes the impact associated with downtime and outages. The ability to test backups is often dependent on resources, such as the availability of spare devices and testing equipment, needed to appropriately represent the environment. Testing backup and restoration on OT is often limited to systems with redundancy or spare equipment; in certain cases, sampling will be limited to those redundant systems.

Compensating controls may include alternative methods for testing backups such as hash or checksum validations.

Control Enhancement: (3) (5) (8) No OT Discussion for this control.

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
CP-10	**System Recovery and Reconstitution**	**Select**	**Select**	**Select**
CP-10 (2)	*SYSTEM RECOVERY AND RECONSTITUTION* | *TRANSACTION RECOVERY*		Select	Select
CP-10 (4)	*SYSTEM RECOVERY AND RECONSTITUTION* | *RESTORE WITHIN TIME PERIOD*			Select
CP-10 (6)	*SYSTEM RECOVERY AND RECONSTITUTION* | *COMPONENT PROTECTION*		**Add**	**Add**

OT Discussion: Reconstitution of the OT includes consideration whether system state variables should be restored to initial values or values before disruption (e.g., are valves restored to full open, full closed, or settings prior to disruption). Restoring system state variables may be disruptive to ongoing physical processes (e.g., valves initially closed may adversely affect system cooling).

Control Enhancement: (2) (4) No OT Discussion for this control.

Control Enhancement: (6) OT Discussion: Organizations should consider recovery and reconstitution timeframes when storing spare equipment, including environmental hazards that could damage the equipment. Storage locations and environments should be chosen appropriately for the type of backup equipment.

Rationale for adding CP-10 (6) to MOD and HIGH baselines: OT system components stored without protection against environmental threats and unauthorized physical or logical access can be susceptible to compromise or damage. Certain system components may include embedded electronics that must be protected from environmental hazards.

CP-12 SAFE MODE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
CP-12	**Safe Mode**	Add	Add	Add

No OT Discussion for this control.

Rationale for adding CP-12 to LOW, MOD and HIGH baselines: This control provides a framework for the organization to plan its policy and procedures for dealing with IT and OT conditions beyond its control in the environment of operations to minimize potential safety and environmental impacts.

F.7.7 IDENTIFICATION AND AUTHENTICATION - IA

Tailoring Considerations for the Identification and Authentication Family

Before implementing controls in the IA family, consider the tradeoffs among security, privacy, latency, performance, and throughput. For example, the organization considers whether latency induced from the use of authentication mechanisms employing cryptographic mechanisms would adversely impact the operational performance of the OT.

In situations where the OT cannot support the specific Identification and Authentication requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

IA-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-2	**Identification and Authentication (Organizational Users)**	**Select**	**Select**	**Select**
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS*	**Select**	**Select**	**Select**
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS*	**Select**	**Select**	**Select**
IA-2 (5)	*IDENTIFICATION AND AUTHENTICATION | INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION*			**Select**
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION | ACCESS TO ACCOUNTS - REPLAY RESISTANT*	Select	Select	Select
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*	**Select**	**Select**	**Select**

OT Discussion: In cases where shared accounts are required, compensating controls include providing increased physical security, personnel security, and auditing measures. For certain OT, the capability for immediate operator interaction is critical. Local emergency actions for OT are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical controls.

Control Enhancement: (1) (2) OT Discussion: As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided the system is not remotely accessible.

Control Enhancement: (5) OT Discussion: For local access, physical access controls and logging may be used as an alternative to individual authentication on an OT system. For remote access, the remote access authentication mechanism will be used to identify, permit, and log individual access before permitting use of shared accounts.

Control Enhancement: (8) No OT Discussion for this control.

Control Enhancement: (12) OT Discussion: The acceptance of PIV credentials is only required for federal organizations, as defined by OMB Memorandum M-19-17 [OMB-M1917]. Non-federal organizations should refer to IA-2 (1) (2) for guidance on multi-factor authentication credentials. Furthermore, many OT systems do not have the ability to accept PIV credentials and will require compensating controls.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
IA-3	**Device Identification and Authentication**	Add	Select	Select
IA-3 (1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*			
IA-3 (4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*			

OT Discussion: OT devices often may not inherently support device authentication. If devices are local to one another, physical security measures that prevent unauthorized communication between devices can be used as compensating controls. For remote communication, additional hardware may be required to meet authentication requirements.

Control Enhancement: (1) (4) OT Discussion: For OT systems that include IIoT devices, these enhancements may be needed to protect device-to-device communication.

Rationale for adding IA-3 to LOW baseline: Given the variety of OT devices and physical locations of OT devices, organizations may consider if types of OT devices that may be vulnerable to tampering or spoofing require unique identification and authentication, and for what types of connections.

IA-4 IDENTIFIER MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-4	**Identifier Management**	Select	Select	Select

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-4 (4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*		**Select**	**Select**

No OT Discussion for this control.

Control Enhancement: (4) OT Discussion: This control enhancement is typically implemented by the organization, rather than at the system level. However, to manage risk for certain OT environments, identifiers such as badges may have different markings to indicate the status of individuals such as contractors, foreign nationals, and non-organizational users.

IA-5 AUTHENTICATOR MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-5	**Authenticator Management**	**Select**	**Select**	**Select**
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*	Select	Select	Select
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION*		Select	Select
IA-5 (6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*		Select	Select

OT Discussion: Example compensating controls include physical access control and encapsulating the OT to provide authentication external to the OT.

Control Enhancement: (1) (2) (6) No OT Discussion for this control.

IA-6 AUTHENTICATION FEEDBACK

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-6	**Authentication Feedback**	**Select**	**Select**	**Select**

OT Discussion: This control assumes a visual interface that provides feedback of authentication information during the authentication process. When OT authentication uses an interface that does not support visual feedback (e.g., protocol-based authentication), this control may be tailored out.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH

IA-7	**Cryptographic Module Authentication**	Select	Select	Select

No OT Discussion for this control.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-8	**Identification and Authentication (Non-Organizational Users)**	**Select**	**Select**	**Select**
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*	**Select**	**Select**	**Select**
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS*	**Select**	**Select**	**Select**
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES*	**Select**	**Select**	**Select**

OT Discussion: The OT Discussion for IA-2, Identification and Authentication (Organizational Users) is applicable for Non-Organizational Users.

Control Enhancement: (1) OT Discussion: Acceptance of PIV credentials is only required for organizations that follow OMB Memorandum M-19-17 [OMB-M1917] (e.g., federal agencies and contractors).

Control Enhancement: (2) (4) OT Discussion: Example compensating controls include implementing support external to the OT and multi-factor authentication.

IA-11 RE-AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-11	**Re-authentication**	Select	Select	Select

No OT Discussion for this control.

IA-12 IDENTITY PROOFING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
IA-12	**Identity Proofing**		**Select**	**Select**
IA-12 (1)	*IDENTITY PROOFING | SUPERVISOR AUTHORIZATION*			**Add**
IA-12 (2)	*IDENTITY PROOFING | IDENTITY EVIDENCE*		**Select**	**Select**
IA-12 (3)	*IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION*		**Select**	**Select**

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
IA-12 (4)	*IDENTITY PROOFING | IN-PERSON VALIDATION AND VERIFICATION*			**Select**
IA-12 (5)	*IDENTITY PROOFING | ADDRESS CONFIRMATION*		**Select**	**Select**

<u>OT Discussion:</u> Identity proofing is likely performed by different departments within the organization. It is encouraged to leverage existing organizational systems (i.e., HR or IT processes) to perform this control.

<u>Control Enhancement:</u> (1) <u>OT Discussion:</u> Maintenance, Engineering, or third-party organizations may require OT access in order to support operations. The organization should determine the AO for proving identity prior to allowing access to the OT environment. Consider obtaining supervisor or sponsor authorization, where the sponsor may be someone within operations.

<u>Control Enhancement:</u> (2) (3) (4) (5) <u>OT Discussion:</u> If the organization already performs these controls, it is recommended to leverage existing organizational processes. For example, Human Resources may provide a system for tracking identity evidence. OT does not need to develop an independent system for achieving this control. Rather, it is advised to leverage the existing processes developed by other departments within the organization.

<u>Rationale for adding IA-12</u> (1) <u>to HIGH baseline:</u> A supervisor or sponsor should be made aware of any access an employee has to the OT environment, since unauthorized or accidental access could create consequences to the physical process.

F.7.8 INCIDENT RESPONSE - IR

Tailoring Considerations for the Incident Response Family

The automated mechanisms used to support the tracking of security incidents are typically not part of, or connected to, the OT.

IR-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-1	**Policy and Procedures**	**Select**	**Select**	**Select**

<u>OT Discussion:</u> The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

IR-2 INCIDENT RESPONSE TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-2	**Incident Response Training**	Select	Select	Select
IR-2 (1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*			Select
IR-2 (2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*			Select

No OT Discussion for this control.

IR-3 INCIDENT RESPONSE TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-3	**Incident Response Testing**		Select	Select
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*		Select	Select

No OT Discussion for this control.

IR-4 INCIDENT HANDLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-4	**Incident Handling**	**Select**	**Select**	**Select**
IR-4 (1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*		Select	Select
IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*			Select
IR-4 (11)	*INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM*			Select

<u>OT Discussion:</u> As part of the incident handling capability, the organization coordinates with external vendors, integrators, or suppliers as necessary to ensure they have the capability to address events specific to embedded components and devices.

<u>Control Enhancement:</u> (1) (4) (11) No OT Discussion for this control.

IR-5 INCIDENT MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-5	**Incident Monitoring**	Select	Select	Select
IR-5 (1)	*INCIDENT MONITORING | AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS*			Select

No OT Discussion for this control.

IR-6 INCIDENT REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-6	**Incident Reporting**	**Select**	**Select**	**Select**
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*		**Select**	**Select**
IR-6 (3)	*INCIDENT REPORTING | SUPPLY CHAIN COORDINATION*		Select	Select

OT Discussion: The organization should report incidents on a timely basis. CISA collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Control Enhancement: (1) OT Discussion: The automated mechanisms used to support the incident reporting process are not necessarily part of, or connected to, the OT.

Control Enhancement: (3) No OT Discussion for this control.

IR-7 INCIDENT RESPONSE ASSISTANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-7	**Incident Response Assistance**	Select	Select	Select
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT*		Select	Select

No OT Discussion for this control.

IR-8 INCIDENT RESPONSE PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH

IR-8	**Incident Response Plan**	Select	Select	Select

No OT Discussion for this control.

F.7.9 MAINTENANCE - MA

Tailoring Considerations for the Maintenance Family

The automated mechanisms used to schedule, conduct, and document maintenance and repairs are not necessarily part of, or connected to, the OT.

In situations where the OT cannot support the specific maintenance requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

MA-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

MA-2 CONTROLLED MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-2	**Controlled Maintenance**	Select	Select	Select
MA-2 (2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*			Select

No OT Discussion for this control.

MA-3 MAINTENANCE TOOLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-3	**Maintenance Tools**		Select	Select
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*		Select	Select
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*		Select	Select
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*		Select	Select

MA-4 NONLOCAL MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
MA-4	**Nonlocal Maintenance**	Select	Select	Select
MA-4 (1)	*NONLOCAL MAINTENANCE | LOGGING AND REVIEW*		<u>Add</u>	<u>Add</u>
MA-4 (3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION*			**Select**

No OT Discussion for this control.

<u>Control Enhancement:</u> (1) No OT Discussion for this control.

<u>Control Enhancement:</u> (3) <u>OT Discussion:</u> The organization may need access to nonlocal maintenance and diagnostic services in order to restore essential OT operations or services. Example compensating controls include limiting the extent of the maintenance and diagnostic services to the minimum essential activities, and carefully monitoring and auditing the non-local maintenance and diagnostic activities.

<u>Rationale for adding MA-4</u> (1) <u>to MOD and HIGH baselines:</u> OT environments are often heavily dependent on nonlocal maintenance providers, so organizations should have the ability to review logs about relevant maintenance activities.

MA-5 MAINTENANCE PERSONNEL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-5	**Maintenance Personnel**	Select	Select	Select
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*			Select

No OT discussion for this control.

MA-6 TIMELY MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-6	**Timely Maintenance**		Select	Select

No OT discussion for this control.

MA-7 FIELD MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
MA-7	**Field Maintenance**	**Add**	**Add**	**Add**

OT Discussion: Organizations identify OT systems/system components with specific calibration, maintenance, or other requirements and limit maintenance to specific facilities. Some examples may include safety critical systems or systems involved in custody transfer where accuracy tolerances are limited and additional quality control checks are required.

Rationale for adding MA-7 to LOW, MOD and HIGH baselines: Some OT equipment has specific requirements for calibration, maintenance, and modification to meet regulatory or safety standards. Different deployed locations may impact the quality and precision of field maintenance.

F.7.10 MEDIA PROTECTION –MP

MP-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

MP-2 MEDIA ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-2	**Media Access**	Select	Select	Select

No OT discussion for this control.

MP-3 MEDIA MARKING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-3	**Media Marking**		Select	Select

No OT Discussion for this control.

MP-4 MEDIA STORAGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-4	**Media Storage**		Select	Select

No OT Discussion for this control.

MP-5 MEDIA TRANSPORT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-5	**Media Transport**		Select	Select

No OT Discussion for this control.

MP-6 MEDIA SANITIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-6	**Media Sanitization**	Select	Select	Select
MP-6 (1)	*MEDIA SANITIZATION | REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY*			Select
MP-6 (2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*			Select
MP-6 (3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*			Select

No OT Discussion for this control.

MP-7 MEDIA USE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-7	**Media Use**	Select	Select	Select

No OT Discussion for this control.

F.7.11 PHYSICAL AND ENVIRONMENTAL PROTECTION – PE

Tailoring Considerations for the Physical and Environmental Protection Family

Physical and environmental protections are often used as a compensating control for many OT systems; therefore, physical and environmental protection controls are especially important. Any selected compensating control mitigates risk to an acceptable level.

PE-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems. The OT components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network OT. Regulatory controls may also apply.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-2	**Physical Access Authorizations**	Select	Select	Select

No OT Discussion for this control.

PE-3 PHYSICAL ACCESS CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-3	**Physical Access Control**	**Select**	**Select**	**Select**
PE-3 (1)	*PHYSICAL ACCESS CONTROL | SYSTEM ACCESS*			Select

OT Discussion: The organization considers OT safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to OT facilities and assets to authorized individuals only. OT systems are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement OT security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan.

Control Enhancement: (1) No OT discussion for this control.

PE-4 ACCESS CONTROL FOR TRANSMISSION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-4	**Access Control for Transmission**		Select	Select

No OT Discussion for this control.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-5	**Access Control for Output Devices**		Select	Select

No OT Discussion for this control.

PE-6 MONITORING PHYSICAL ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PE-6	**Monitoring Physical Access**	Select	Select	Select
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT*		Select	Select
PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS*		<u>Add</u>	Select

No OT discussion for this control.

<u>Control Enhancement:</u> (1) (4) No OT Discussion for this control.

<u>Rationale for adding PE-6</u> (4) <u>to MOD baseline:</u> Many of the OT components are in remote geographical and dispersed locations. Other components may be in ceilings, floors, or distribution closets. Furthermore, physical access controls are frequently used as compensating controls when devices lack the ability to enforce logical access restrictions.

PE-8 VISITOR ACCESS RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-8	**Visitor Access Records**	Select	Select	Select
PE-8 (1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW*			Select

No OT Discussion for this control.

PE-9 POWER EQUIPMENT AND CABLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-9	**Power Equipment and Cabling**		Select	Select

No OT Discussion for this control.

PE-10 EMERGENCY SHUTOFF

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-10	**Emergency Shutoff**		**Select**	**Select**

OT Discussion: It may not be possible or advisable to shut off power to some OT. The [organizational-defined parameters] for this control should be implemented in consultation with safety and operational personnel. Example compensating controls include failing to a known state and emergency procedures.

PE-11 EMERGENCY POWER

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PE-11	**Emergency Power**		Select	Select
PE-11 (1)	*EMERGENCY POWER | ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*			Select
PE-11 (2)	*EMERGENCY POWER | ALTERNATE POWER SUPPLY - SELF-CONTAINED*			

No OT Discussion for this control.

PE-12 EMERGENCY LIGHTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-12	**Emergency Lighting**	Select	Select	Select

No OT Discussion for this control.

PE-13 FIRE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-13	**Fire Protection**	**Select**	**Select**	**Select**
PE-13 (1)	*FIRE PROTECTION | DETECTION SYSTEMS – AUTOMATIC ACTIVATION AND NOTIFICATION*		Select	Select
PE-13 (2)	*FIRE PROTECTION | SUPPRESSION SYSTEMS – AUTOMATIC ACTIVATION AND NOTIFICATION*			Select

OT Discussion: Fire suppression mechanisms should take the OT environment into account (e.g., water sprinkler systems could be hazardous in specific environments).

Control Enhancement: (1) (2) No OT Discussion for this control.

PE-14 ENVIRONMENTAL CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-14	**Environmental Controls**	**Select**	**Select**	**Select**

OT Discussion: Temperature and humidity controls are typically components of other OT systems such as the HVAC, process, or lighting systems, or can be a standalone and unique OT system. OT can operate in extreme environments and both interior and exterior locations. For a specific OT, the temperature and humidity design and operational parameters dictate the performance specifications. As OT and IT become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers, and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity. When environmental controls cannot be implemented, use hardware that is engineered to withstand the unique environmental hazards.

PE-15 WATER DAMAGE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-15	**Water Damage Protection**	**Select**	**Select**	**Select**
PE-15 (1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*			Select

OT Discussion: Water damage protection and use of shutoff and isolation valves is both a procedural action and a specific type of OT. OT used in the manufacturing, hydropower, transportation/navigation, water, and wastewater industries rely on the movement of water and are specifically designed to manage the quantity/flow and pressure of water. As OT and IT become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems should ensure that water will not disable the system (e.g., a fire that activates the sprinkler system does not spray onto the fire control servers, router, switches and short out the alarms, egress systems, emergency lighting, and suppression systems).

Control Enhancement: (1) No OT Discussion for this control.

PE-16 DELIVERY AND REMOVAL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-16	**Delivery and Removal**	Select	Select	Select

No OT Discussion for this control.

PE-17 ALTERNATE WORK SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-17	**Alternate Work Site**		Select	Select

No OT Discussion for this control.

PE-18 LOCATION OF SYSTEM COMPONENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-18	**Location of System Components**			Select

No OT Discussion for this control.

PE-21 ELECTROMAGNETIC PULSE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-21	**Electromagnetic Pulse Protection**			

OT Discussion: Organizations managing OT equipment may choose to utilize electromagnetic (EM) pulse protection to prevent adversarial or environmental EM threats. Organizations may select to follow National Coordinating Center for Communications (NCC) guidelines on EM pulse protection.

PE-22 COMPONENT MARKING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PE-22	**Component Marking**		**Add**	**Add**

OT Discussion: Hardware components are marked or labeled to indicate which information is processed, stored, or transmitted. Component markings can be useful in differentiating between safety and control systems, OT and IT equipment, and internally and externally connected systems. Marking components reduces the probability of mismanaging the system or performing maintenance on an incorrect device.

Rationale for adding PE-22 to MOD and HIGH baselines: OT is unique in that it may look like an IT component, but it may perform a very different function. Visible differentiation between components performing different functions can help reduce reliability incidents due to maintenance errors.

F.7.12 PLANNING – PL

PL-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

PL-2 SYSTEM SECURITY AND PRIVACY PLANS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-2	**System Security and Privacy Plans**	**Select**	**Select**	**Select**

OT Discussion: When systems are highly interconnected, coordinated planning is essential. A low-impact system could adversely affect a higher-impact system.

PL-4 RULES OF BEHAVIOR

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-4	**Rules of Behavior**	Select	Select	Select
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE / APPLICATION USAGE RESTRICTIONS*	Select	Select	Select

No OT Discussion for this control.

PL-7 CONCEPT OF OPERATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PL-7	**Concept of Operations**			

<u>OT Discussion:</u> Organizations need to consider documenting known operational procedures and exploring how they relate to the combination of IT and OT technologies within the environment.

PL-8 SECURITY AND PRIVACY ARCHITECTURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PL-8	**Security and Privacy Architectures**		Select	Select
PL-4 (1)	*SECURITY AND PRIVACY ARCHITECTURES* | *DEFENSE IN DEPTH*			

No OT Discussion for this control.

<u>Control Enhancement:</u> (1) <u>OT Discussion:</u> Defense in depth is considered a common practice for security architecture within OT environments.

PL-9 CENTRAL MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-9	**Central Management**			

<u>OT Discussion</u>: If the architecture allows, consider centrally managing flaw remediation, malicious code protection, logging, incident detection, etc.

PL-10 BASELINE SELECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-10	**Baseline Selection**	Select	Select	Select

No OT Discussion for this control.

PL-11 BASELINE TAILORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-11	**Baseline Tailoring**	Select	Select	Select

No OT Discussion for this control.

F.7.13 ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS - PM

Characteristics of the Organization-Wide Information Security Program Management Control Family

Organization-Wide Information Security Program Management Controls are deployed organization-wide supporting the information security program. They are not associated with control baselines and are independent of any system impact level.

Program Management Controls should specifically address the unique properties and requirements of OT, the relationship to non-OT systems, and the relationship to other programs concerned with operational characteristics of OT (e.g., safety, efficiency, reliability, resilience). To achieve this, the security program should utilize interdisciplinary teams that can help reconcile and balance conflicting equities, objectives, and responsibilities such as capability, adaptability, resilience, safety, security, usability, and efficiency.

PM-1 INFORMATION SECURITY PROGRAM PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-1	**Information Security Program Plan**

No OT Discussion for this control.

PM-2 INFORMATION SECURITY PROGRAM LEADERSHIP ROLE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-2	**Information Security Program Leadership Role**

No OT Discussion for this control.

PM-3 INFORMATION SECURITY AND PRIVACY RESOURCES

CNTL NO.	CONTROL NAME

	Control Enhancement Name
PM-3	**Information Security and Privacy Resources**

No OT Discussion for this control.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-4	**Plan of Action and Milestones Process**

No OT Discussion for this control.

PM-5 SYSTEM INVENTORY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-5	**System Inventory**

No OT Discussion for this control.

PM-6 MEASURES OF PERFORMANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-6	**Measures of Performance**

No OT Discussion for this control.

PM-7 ENTERPRISE ARCHITECTURE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-7	**Enterprise Architecture**

No OT Discussion for this control.

PM-8 CRITICAL INFRASTRUCTURE PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-8	**Critical Infrastructure Plan**

<u>OT Discussion:</u> Organizations should be familiar with protection requirements and guidance defined by executive orders, government sector specific agencies (SSAs), and industry trade organizations.

PM-9 RISK MANAGEMENT STRATEGY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-9	**Risk Management Strategy**

No OT Discussion for this control.

PM-10 AUTHORIZATION PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-10	**Authorization Process**

No OT Discussion for this control.

PM-11 MISSION AND BUSINESS PROCESS DEFINITION

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-11	**Mission and Business Process Definition**

No OT Discussion for this control.

PM-12 INSIDER THREAT PROGRAM

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-12	**Insider Threat Program**

No OT Discussion for this control.

PM-13 SECURITY AND PRIVACY WORKFORCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-13	**Security and Privacy Workforce**

No OT Discussion for this control.

PM-14 TESTING, TRAINING, AND MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-14	**Testing, Training, and Monitoring**

No OT Discussion for this control.

PM-15 SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-15	**Security and Privacy Groups and Associations**

OT Discussion: Organizations should be familiar with relevant security-focused and industry-specific groups or associations, including government sector specific agencies (SSAs), information sharing and analysis centers (ISAC), and industry trade organizations.

PM-16 THREAT AWARENESS PROGRAM

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-16	**Threat Awareness Program**

OT Discussion: The organization should collaborate and share information about potential incidents on a timely basis. CISA serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. Organizations should consider having both an unclassified and classified information sharing capability.

PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-17	**Protecting Controlled Unclassified Information on External Systems**

OT Discussion: This control applies to federal organizations and other organizations supporting the government that process Controlled Unclassified Information (CUI).

PM-18 PRIVACY PROGRAM PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-18	**Privacy Program Plan**

No OT Discussion for this control.

PM-19 PRIVACY PROGRAM LEADERSHIP ROLE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-19	**Privacy Program Leadership Role**

No OT Discussion for this control.

PM-20 DISSEMINATION OF PRIVACY PROGRAM INFORMATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-20	**Dissemination of Privacy Program Information**
PM-20 (1)	*DISSEMINATION OF PRIVACY PROGRAM INFORMATION | PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES*

No OT Discussion for this control.

PM-21 ACCOUNTING OF DISCLOSURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-21	**Accounting of Disclosures**

No OT Discussion for this control.

PM-22 PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-22	**Personally Identifiable Information Quality Management**

No OT Discussion for this control.

PM-23 DATA GOVERNANCE BODY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-23	**Data Governance Body**

No OT Discussion for this control.

PM-24 DATA INTEGRITY BOARD

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-24	**Data Integrity Board**

No OT Discussion for this control.

PM-25 MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-25	**Minimization of Personally Identifiable Information Used in Testing, Training, and Research**

No OT Discussion for this control.

PM-26 COMPLAINT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-26	**Complaint Management**

No OT Discussion for this control.

PM-27 PRIVACY REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-27	**Privacy Reporting**

No OT Discussion for this control.

PM-28 RISK FRAMING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-28	**Risk Framing**

No OT Discussion for this control.

PM-29 RISK MANAGEMENT PROGRAM LEADERSHIP ROLES

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-29	**Risk Management Program Leadership Roles**

No OT Discussion for this control.

PM-30 SUPPLY CHAIN RISK MANAGEMENT STRATEGY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-30	**Supply Chain Risk Management Strategy**
PM-30 (1)	*SUPPLY CHAIN RISK MANAGEMENT STRATEGY | SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS*

No OT Discussion for this control.

PM-31 CONTINUOUS MONITORING STRATEGY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-31	**Continuous Monitoring Strategy**

No OT Discussion for this control.

PM-32 PURPOSING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-32	**Purposing**

No OT Discussion for this control.

F.7.14 PERSONNEL SECURITY – PS

Tailoring Considerations for the Personnel Security Family

Personnel security controls require collaboration between OT, IT, security, and HR personnel.

PS-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

PS-2 POSITION RISK DESIGNATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-2	**Position Risk Designation**	**Select**	**Select**	**Select**

OT Discussion: Private organizations should utilize existing sector specific regulations, laws, policy, or guidance for determining appropriate risk designations for positions.

PS-3 PERSONNEL SCREENING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-3	**Personnel Screening**	Select	Select	Select

No OT Discussion for this control.

PS-4 PERSONNEL TERMINATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-4	**Personnel Termination**	Select	Select	Select
PS-4 (2)	*PERSONNEL TERMINATION | AUTOMATED ACTIONS*			Select

No OT Discussion for this control.

PS-5 PERSONNEL TRANSFER

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-5	**Personnel Transfer**	Select	Select	Select

No OT Discussion for this control.

PS-6 ACCESS AGREEMENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-6	**Access Agreements**	Select	Select	Select

No OT Discussion for this control.

PS-7 EXTERNAL PERSONNEL SECURITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-7	**External Personnel Security**	Select	Select	Select

No OT Discussion for this control.

PS-8 PERSONNEL SANCTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-8	**Personnel Sanctions**	Select	Select	Select

No OT Discussion for this control.

PS-9 POSITION DESCRIPTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-9	**Position Descriptions**	Select	Select	Select

No OT Discussion for this control.

F.7.15 RISK ASSESSMENT – RA

Many OT organizations have well-established risk assessment programs that can be leveraged for cybersecurity risk analysis.

RA-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

RA-2 SECURITY CATEGORIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-2	**Security Categorization**	**Select**	**Select**	**Select**

OT Discussion: Process hazard analysis (PHA), functional safety assessments, and other organization-established risk assessments can be referenced to identify the impact level of the OT systems.

RA-3 RISK ASSESSMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-3	**Risk Assessment**	Select	Select	Select
RA-3 (1)	*RISK ASSESSMENT* | *SUPPLY CHAIN RISK ASSESSMENT*	Select	Select	Select

No OT Discussion for this control.

RA-5 VULNERABILITY MONITORING AND SCANNING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-5	**Vulnerability Monitoring and Scanning**	**Select**	**Select**	**Select**
RA-5 (2)	*VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED*	Select	Select	Select
RA-5 (4)	*VULNERABILITY MONITORING AND SCANNING | DISCOVERABLE INFORMATION*			**Select**
RA-5 (5)	*VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS*		Select	Select
RA-5 (11)	*VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM*	**Select**	**Select**	**Select**

OT Discussion: The organization makes a risk-based determination of how to monitor or scan for vulnerabilities on their system. This may include active scanning, passive monitoring, or compensating controls, depending on the system being scanned. For example, vulnerability examination may be performed using passive monitoring and manual visual inspection to maintain an up-to-date inventory of assets. That inventory can be cross-referenced against a list of known vulnerabilities (e.g., CISA advisories and NIST NVD). Production may need to be taken off-line before active scans can be conducted. Scans are scheduled to occur during planned OT outages whenever possible. If vulnerability scanning tools are used on adjacent non-OT networks, extra care is taken to ensure that they do not mistakenly scan the OT network. Automated network scanning is not applicable to non-routable communications such as serial networks. Compensating controls include providing a replicated or simulated system for conducting scans or host-based vulnerability applications.

Control Enhancement: (2) (5) No OT Discussion for this control.

Control Enhancement: (4) OT Discussion: Examples of discoverable information in OT could include information about key personnel or technical information relating to systems and configurations. Locations that may need to be monitored or scanned include technical forums, blogs, or vendor/contractor websites.

Control Enhancement: (11) OT Discussion: For federal organizations, CISA Binding Operational Directive 20-01 requires individual federal civilian executive branch agencies to develop and publish a vulnerability disclosure policy (VDP) for their internet-accessible systems and services, and maintain processes to support their VDP. A VDP may be implemented at the organization level, rather than for each individual system. Non-federal as well as federal organizations could achieve this control by creating and monitoring an email address published on a public-facing website for contacting the organization regarding disclosures.

RA-7 RISK RESPONSE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-7	**Risk Response**	Select	Select	Select

No OT Discussion for this control.

RA-9 CRITICALITY ANALYSIS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-9	**Criticality Analysis**		Select	Select

No OT Discussion for this control.

F.7.16 SYSTEM AND SERVICES ACQUISITION – SA

Tailoring Considerations for the System and Services Acquisition Family

In situations where the OT cannot support the specific System and Services Acquisition requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

SA-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

SA-2 ALLOCATION OF RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-2	**Allocation of Resources**	Select	Select	Select

No OT Discussion for this control.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-3	**System Development Life Cycle**	Select	Select	Select
SA-3 (1)	*SYSTEM DEVELOPMENT LIFE CYCLE | MANAGE PREPRODUCTION ENVIRONMENT*			
SA-3 (3)	*SYSTEM DEVELOPMENT LIFE CYCLE | TECHNOLOGY REFRESH*			

No OT Discussion for this control.

Control Enhancements: (1) OT Discussion: Organizations that do not maintain local preproduction environments and utilize a third-party integrator should ensure contracts are developed to limit the security and privacy risks.

Control Enhancements: (3) OT Discussion: Many OT systems have an expected life cycle that is longer than most IT components. Technology refresh is addressed in budget planning to limit the use of obsolete systems that present security or reliability risks.

SA-4 ACQUISITION PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SA-4	**Acquisition Process**	**Select**	**Select**	**Select**
SA-4 (1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF CONTROLS*		**Select**	**Select**
SA-4 (2)	*ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS*		**Select**	**Select**
SA-4 (5)	*ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS*			Select
SA-4 (9)	*ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE*		**Select**	**Select**
SA-4 (10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*	**Select**	**Select**	**Select**
SA-4 (12)	*ACQUISITION PROCESS | DATA OWNERSHIP*	Add	Add	Add

OT Discussion: Organizations engage with OT suppliers to raise awareness of cybersecurity needs. The SCADA/Control Systems Procurement Project provides example cybersecurity procurement language for OT.

Control Enhancements: (1) (2) (9) OT Discussion: When acquiring OT products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware, or plan for compensating controls.

Control Enhancement: (10) OT Discussion: The use of approved PIV products is only required for organizations that follow OMB Memorandum M-19-17, e.g., federal agencies and contractors. Example compensating controls include employing external products on the FIPS 201-approved products list for PIV capability in conjunction with OT products.

Control Enhancement: (5) (12) No OT Discussion for this control.

Rationale for adding SA-4 (12) to LOW, MOD and HIGH baselines: Organizationally sensitive or proprietary OT data is often provided to contractors for project development or support; therefore, data ownership should be defined prior to exchanging data with a vendor or integrator. The potential sharing of data with other parties and the potential deletion of the data after project completion should be determined. OT systems that are operated by contractors on behalf of the organization may be subject to the same requirements (legal, regulatory, etc.) for data ownership and retention.

SA-5 SYSTEM DOCUMENTATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-5	**System Documentation**	Select	Select	Select

No OT Discussion for this control.

SA-8 SECURITY AND PRIVACY ENGINEERING PRINCIPLES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-8	**Security and Privacy Engineering Principles**	Select	Select	Select

No OT Discussion for this control.

SA-9 EXTERNAL SYSTEM SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-9	**External System Services**	Select	Select	Select
SA-9 (2)	*EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES*		Select	Select

No OT Discussion for this control.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-10	**Developer Configuration Management**		**Select**	**Select**

<u>OT Discussion:</u> Personnel knowledgeable in security and privacy requirements are included in the change management process for the developer.

SA-11 DEVELOPER TESTING AND EVALUATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-11	**Developer Testing and Evaluation**		Select	Select

No OT Discussion for this control.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**		Select	Select
SA-15 (3)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*		Select	Select

No OT Discussion for this control.

SA-16 DEVELOPER-PROVIDED TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-16	**Developer-Provided Training**			Select

No OT Discussion for this control.

SA-17 DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-17	**Developer Security and Privacy Architecture and Design**			Select

No OT Discussion for this control.

SA-21 DEVELOPER SCREENING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-21	**Developer Screening**			Select

No OT Discussion for this control.

SA-22 UNSUPPORTED SYSTEM COMPONENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-22	**Unsupported System Components**	**Select**	**Select**	**Select**

OT Discussion: OT systems may contain system components that are no longer supported by the developer, vendor, or manufacturer and have not been replaced due to various operational, safety, availability, or lifetime constraints. Organizations identify alternative methods to continue supported operation of such system components and consider additional compensating controls to mitigate against known threats and vulnerabilities to unsupported system components.

F.7.17 SYSTEM AND COMMUNICATIONS PROTECTION - SC

Tailoring Considerations for the System and Communications Protection Family

The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the OT. While the legacy devices commonly found within OT often lack direct support of cryptographic functions, compensating controls (e.g., encapsulations) may be used to meet the intent of the control.

In situations where the OT cannot support the specific System and Communications Protection requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate.

SC-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

SC-2 SEPARATION OF SYSTEM AND USER FUNCTIONALITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-2	Separation of System and User Functionality		Select	Select

OT Discussion: Physical separation includes using separate systems for managing the OT than for operating OT components. Logical separation includes the use of different user accounts for administrative and operator privileges. Example compensating controls include providing increased auditing measures.

SC-3 SECURITY FUNCTION ISOLATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-3	Security Function Isolation			Select

OT Discussion: Organizations consider implementing this control when designing new architectures or updating existing components. An example compensating control includes access controls.

SC-4 INFORMATION IN SHARED SYSTEM RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-4	Information in Shared System Resources		Select	Select

OT Discussion: This control is especially relevant for OT systems that process confidential data. Example compensating controls include architecting the use of the OT to prevent sharing system resources.

SC-5 DENIAL-OF-SERVICE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-5	Denial-of-Service Protection	Select	Select	Select

OT Discussion: Some OT equipment may be more susceptible to DoS attacks due to the time criticality of some OT applications. Risk-based analysis informs prioritization of DoS protection and establishment of policy and procedure.

SC-7 BOUNDARY PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-7	**Boundary Protection**	Select	Select	Select
SC-7 (3)	*BOUNDARY PROTECTION | ACCESS POINTS*		Select	Select
SC-7 (4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*		Select	Select
SC-7 (5)	*BOUNDARY PROTECTION | DENY BY DEFAULT - ALLOW BY EXCEPTION*		Select	Select
SC-7 (7)	*BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES*		Select	Select
SC-7 (8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*		Select	Select
SC-7 (18)	*BOUNDARY PROTECTION | FAIL SECURE*		**Add**	**Select**
SC-7 (21)	*BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS*			Select
SC-7 (28)	*BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS*	**Add**	**Add**	**Add**
SC-7 (29)	*BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS*	**Add**	**Add**	**Add**

No OT Discussion for this control.

Control Enhancement: (3) (4) (5) (7) (8) (21) No OT discussion for this control.

Control Enhancement: (18) OT Discussion: The organization selects an appropriate failure mode (e.g., permit or block all communications).

Control Enhancement: (28) OT Discussion: Organizations consider the need for a direct connection to a public network for each OT system, including potential benefits, additional threat vectors, and potential adverse impact specifically relevant to what type of public access that connection introduces.

Control Enhancement: (29) OT Discussion: Subnets can be used to isolate low-risk functions from higher-risk ones, and control from safety. Subnets should be considered along with other boundary protection technologies.

Rationale for adding SC-7 (18) to MOD baseline: The ability to choose the failure mode for the physical part of the OT differentiates the OT from other IT systems. This choice may be a significant influence in mitigating the impact of a failure.

Rationale for adding SC-7 (28) to LOW, MOD and HIGH baselines: Access to OT should be restricted to individuals required for operation. A connection made from the OT directly to a public network has limited applicability in OT environments, but significant potential risk.

Rationale for adding SC-7 (29) to LOW, MOD and HIGH baselines: In OT environments, subnets and zoning is a common practice for isolating functions.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-8	**Transmission Confidentiality and Integrity**		Select	Select
SC-8 (1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION*		**Select**	**Select**

No OT discussion for this control.

Control Enhancement: (1) OT Discussion: When transmitting across untrusted network segments, the organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function) to protect confidentiality and integrity of the information. Example compensating controls include physical protections, such as a secure conduit (e.g., point-to-point link) between two system components.

SC-10 NETWORK DISCONNECT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-10	**Network Disconnect**		~~Remove~~	~~Remove~~

No OT Discussion for this control.

Rationale for removing SC-10 from MOD and HIGH baselines: The intent of this control is effectively covered by AC-17 (9) for OT systems.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-12	**Cryptographic Key Establishment and Management**	Select	Select	Select
SC-12 (1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*			Select

No OT Discussion for this control.

SC-13 CRYPTOGRAPHIC PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-13	**Cryptographic Protection**	Select	Select	Select

No OT Discussion for this control.

SC-15 COLLABORATIVE COMPUTING DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-15	**Collaborative Computing Devices**	Select	Select	Select

No OT Discussion for this control.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-17	**Public Key Infrastructure Certificates**		Select	Select

No OT Discussion for this control.

SC-18 MOBILE CODE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-18	**Mobile Code**		Select	Select

No OT Discussion for this control.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**	**Select**	**Select**	**Select**

OT Discussion: The use of secure name/address resolution services should be determined only after careful consideration and after verification that it does not adversely impact the operational performance of the OT.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Select	Select	Select

OT Discussion: The use of secure name/address resolution services should be determined only after careful consideration and after verification that it does not adversely impact the operational performance of the OT.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Select	Select	Select

OT Discussion: The use of secure name/address resolution services should be determined only after careful consideration and after verification that it does not adversely impact the operational performance of the OT.

SC-23 SESSION AUTHENTICITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-23	Session Authenticity		Select	Select

OT Discussion: Example compensating controls include auditing measures.

SC-24 FAIL IN KNOWN STATE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-24	Fail in Known State		Add	Select

OT Discussion: The organization selects an appropriate failure state. Preserving OT state information includes consistency among OT state variables and the physical state which the OT represents (e.g., whether valves are open or closed, communication permitted or blocked, continue operations).

Rationale for adding SC-24 to MOD baseline: As part of the architecture and design of the OT, the organization selects an appropriate failure state of an OT in accordance with the function performed by the OT and the operational environment. The ability to choose the failure mode for the physical part of OT differentiates OT systems from other IT systems. This choice may be a significant influence in mitigating the impact of a failure, since it may be disruptive to ongoing physical processes (e.g., valves failing in closed position may adversely affect system cooling).

SC-28 PROTECTION OF INFORMATION AT REST

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-28	**Protection of Information at Rest**		**Select**	**Select**
SC-28 (1)	*PROTECTION OF INFORMATION AT REST |CRYPTOGRAPHIC PROTECTION*		Select	Select

OT Discussion: The use of cryptographic mechanisms is implemented only after careful consideration and after verification that it does not adversely impact the operational performance of the OT. Cryptographic mechanisms may not be feasible on certain OT devices. In these cases, compensating controls may be relocating the data to a location that does support cryptographic mechanisms.

Control Enhancement: (1) No OT Discussion for this control.

SC-32 SYSTEM PARTITIONING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-32	**System Partitioning**			
SC-32 (1)	*SYSTEM PARTITIONING | SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS*			

No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: Organizations consider separate physical domains for privileged functions such as those affecting security and safety.

SC-39 PROCESS ISOLATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-39	**Process Isolation**	**Select**	**Select**	**Select**

OT Discussion: Example compensating controls include partition processes to separate platforms.

SC-41 PORT AND I/O DEVICE ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-41	**Port and I/O Device Access**	Add	Add	Add

No OT discussion for this control.

Rationale for adding SC-41 to LOW, MOD and HIGH baselines: OT functionality is generally defined in advance and does not change often.

SC-45 SYSTEM TIME SYNCHRONIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-45	**System Time Synchronization**	**Add**	**Add**	**Add**
SC-45 (1)	*SYSTEM TIME SYNCHRONIZATION | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*			

OT Discussion: Organizations coordinate time synchronization on OT to allow for accurate troubleshooting and forensics.

Control Enhancement: (1) OT Discussion: Syncing with an authoritative time source may be selected as a control when data is being correlated across organizational boundaries. OT employ suitable mechanisms (e.g., GPS, IEEE 1588) for time stamps.

Rationale for adding SC-45 to LOW, MOD and HIGH baselines: Organizations may find relative system time beneficial for many OT systems to ensure safe, reliable delivery of essential functions. Time synchronization can also make root cause analysis more efficient by ensuring audit logs from different systems are aligned so that, when the logs are aggregated, organizations have an accurate view of events across multiple systems.

SC-47 ALTERNATE COMMUNICATIONS PATHS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-47	**Alternate Communications Paths**			**Add**

OT Discussion: Organization considers which systems require alternate communications paths to ensure a loss of communication does not lead to an unacceptable loss of view, control, or safety event.

Rationale for adding SC-47 to HIGH baseline: For continuity of operations during an incident, organizations should consider establishing alternate communications paths for command-and-control purposes to continue to operate and take appropriate actions for high-impact systems where the loss of availability or integrity may result in severe or catastrophic adverse impact, which may include impacts on safety and critical service delivery.

SC-51 HARDWARE-BASED PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-51	**Hardware-Based Protection**			

<u>OT Discussion</u>: Some OT systems support write-protection by implementing physical key switches or write-protect switches. Organizations define the systems for which write-protection will be enabled and develop a process for how to take the system out of write-protect mode.

F.7.18 SYSTEM AND INFORMATION INTEGRITY - SI

Tailoring Considerations for the System and Information Integrity Family

In situations where the OT cannot support the specific System and Information Integrity requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

SI-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-1	**Policy and Procedures**	**Select**	**Select**	**Select**

<u>OT Discussion:</u> The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

SI-2 FLAW REMEDIATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-2	**Flaw Remediation**	**Select**	**Select**	**Select**
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*		Select	Select

<u>OT Discussion:</u> Flaw remediation, or patching, is complicated since many OT employ OSs and other software no longer maintained by the vendors. OT operators may also not have the resources or capability to test patches and are dependent on vendors to validate the operability of a patch. Sometimes the organization has no choice but to accept additional risk if no vendor

patch is available, patching requires additional time to complete validation/testing, or deployment requires an unacceptable operations shutdown. In these situations, compensating controls should be implemented (e.g., limiting the exposure of the vulnerable system, restricting vulnerable services, implementing virtual patching). Other compensating controls that do not decrease the residual risk but increase the ability to respond may be desirable (e.g., provide a timely response in case of an incident; devise a plan to ensure the OT can identify the exploitation of the flaw). Testing flaw remediation in an OT may exceed the organization's available resources.

Control Enhancement: (2) No OT discussion for this control.

SI-3 MALICIOUS CODE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-3	**Malicious Code Protection**	**Select**	**Select**	**Select**

OT Discussion: The use and deployment of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operation of the OT. Malicious code protection tools should be configured to minimize their potential impact on the OT (e.g., employ notification rather than quarantine). Example compensating controls include increased traffic monitoring and auditing.

SI-4 SYSTEM MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-4	**System Monitoring**	**Select**	**Select**	**Select**
SI-4 (2)	*SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS*		**Select**	**Select**
SI-4 (4)	*SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		Select	Select
SI-4 (5)	*SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		**Select**	**Select**
SI-4 (10)	*SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*			Select
SI-4 (12)	*SYSTEM MONITORING | AUTOMATED ORGANIZATION-GENERATED ALERTS*			Select
SI-4 (14)	*SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*			Select
SI-4 (20)	*SYSTEM MONITORING | PRIVILEGED USERS*			Select
SI-4 (22)	*SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*			Select

OT Discussion: The organization ensures that use of monitoring tools and techniques does not adversely impact the operational performance of the OT. Example compensating controls include deploying sufficient network, process, and physical monitoring.

Control Enhancement: (2) OT Discussion: In situations where the OT cannot support the use of automated tools to support near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, nonautomated mechanisms or procedures) in accordance with the general tailoring guidance.

Control Enhancement: (4) (10) (12) (14) (20) (22) No OT Discussion for this control.

Control Enhancement: (5) OT Discussion: Example compensating controls include manual methods of generating alerts.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-5	**Security Alerts, Advisories, and Directives**	**Select**	**Select**	**Select**
SI-5 (1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*			Select

OT Discussion: CISA generates security alerts and advisories relative to OT at https://www.cisa.gov/uscert/ics. Industry-specific ISACs often provide tailored advisories and alerts, which can be found at https://www.nationalisacs.org/.

Control Enhancement: (1) No OT Discussion for this control.

SI-6 SECURITY AND PRIVACY FUNCTION VERIFICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-6	**Security and Privacy Function Verification**			**Select**

OT Discussion: Shutting down and restarting the OT may not always be feasible upon the identification of an anomaly; these actions should be scheduled according to OT operational requirements.

SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-7	**Software, Firmware, and Information Integrity**		**Select**	**Select**

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		**Select**	**Select**
SI-7 (2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*			**Select**
SI-7 (5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*			**Select**
SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		**Select**	**Select**
SI-7 (15)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*			**Select**

<u>OT Discussion:</u> The organization determines whether the use of integrity verification applications would adversely impact operation of the ICS and employs compensating controls (e.g., manual integrity verifications that do not affect performance).

<u>Control Enhancements</u>: (1) <u>OT Discussion:</u> The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the OT.

<u>Control Enhancement</u>: (2) <u>OT Discussion</u>: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

<u>Control Enhancement</u>: (5) <u>OT Discussion:</u> Shutting down and restarting the ICS may not always be feasible upon identification of an anomaly; these actions should be scheduled according to ICS operational requirements.

<u>Control Enhancement</u>: (7) <u>OT Discussion</u>: In situations where the ICS cannot detect unauthorized security-relevant changes, the organization employs compensating controls (e.g., manual procedures) in accordance with the general tailoring guidance.

<u>Control Enhancement</u>: (15) <u>OT Discussion</u>: Code authentication provides assurance to the organization that the software and firmware have not been tampered with. If automated mechanisms are not available, organizations could verify code authentication by manually using a combination of techniques including verifying hashes, downloading from reputable sources, verifying version numbers with the vendor, or testing software/firmware in offline/test environment.

SI-8 SPAM PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-8	**Spam Protection**		**Select**	**Select**

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-8 (2)	*SPAM PROTECTION | AUTOMATIC UPDATES*		~~Remove~~	~~Remove~~

OT Discussion: OT organizations implement spam protection by removing spam transport mechanisms, functions, and services (e.g., electronic mail, web browsing) from the OT.

Rationale for removing SI-8 (2) from MOD and HIGH baselines: Spam transport mechanisms are disabled or removed from the OT, so automatic updates are not necessary.

SI-10 INFORMATION INPUT VALIDATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-10	**Information Input Validation**		Select	Select

No OT Discussion for this control.

SI-11 ERROR HANDLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-11	**Error Handling**		Select	Select

No OT Discussion for this control.

SI-12 INFORMATION MANAGEMENT AND RETENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-12	**Information Management and Retention**	Select	Select	Select

No OT Discussion for this control.

SI-13 PREDICTABLE FAILURE PREVENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SI-13	**Predictable Failure Prevention**			Add

No OT Discussion for this control.

Rationale for adding SI-13 control to HIGH baseline: OT are designed and built with certain boundary conditions, design parameters, and assumptions about their environment and mode of operation. OT may run much longer than conventional systems, allowing latent flaws to become effective that are not manifest in other environments. For example, integer overflow might never occur in systems that are re-initialized more frequently than the occurrence of the overflow. Experience and forensic studies of anomalies and incidents in OT can lead to identification of emergent properties that were previously unknown, unexpected, or unanticipated. Preventative and restorative actions (e.g., restarting the system or application) are prudent but may not be acceptable for operational reasons in OT.

SI-16 MEMORY PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-16	**Memory Protection**		Select	Select

No OT Discussion for this control.

SI-17 FAIL-SAFE PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SI-17	**Fail-Safe Procedures**	**Add**	**Add**	**Add**

OT Discussion: The selected failure conditions and corresponding procedures may vary among baselines. The same failure event may trigger different responses, depending on the impact level. Mechanical and analog systems can be used to provide mechanisms to ensure fail-safe procedures. Fail-safe states should incorporate potential impacts to human safety, physical systems, and the environment. Related controls: CP-6.

Rationale for adding SI-17 to LOW, MOD and HIGH baselines: This control provides a structure for the organization to identify its policy and procedures for dealing with failures and other incidents. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of changing environment of operations.

SI-22 INFORMATION DIVERSITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SI-22	**Information Diversity**			

OT Discussion: Many OT systems use information diversity in their design in order to achieve reliability requirements. Some examples of information diversity for an OT system include sensor voting and state estimation.

F.7.19 SUPPLY CHAIN RISK MANAGEMENT - SR

SR-1 POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-1	**Policy and Procedures**	**Select**	**Select**	**Select**

OT Discussion: Supply chain policy and procedures for OT should consider components received as well as components produced. Many OT systems use legacy components that cannot meet modern supply chain expectations. Appropriate compensating controls should be developed to achieve organization supply chain expectations for legacy systems.

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-2	**Supply Chain Risk Management Plan**	Select	Select	Select
SR-2 (1)	*SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM*	Select	Select	Select

No OT Discussion for this control.

SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SR-3	**Supply Chain Controls and Processes**	Select	Select	Select
SR-3 (1)	*SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY BASE*			

No OT Discussion for this control.

Control Enhancement: (1) OT Discussion**:** Using a diverse set of suppliers in the OT environment can improve reliability by reducing common cause failures. This is not always possible, since some technologies have limited supply options that meet the operational requirements.

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SR-5	**Acquisition Strategies, Tools, and Methods**	Select	Select	Select
SR-5 (1)	*ACQUISITION STRATEGIES, TOOLS, AND METHODS* | *ADEQUATE SUPPLY*		**Add**	**Add**

No OT Discussion for this control.

Control Enhancement: (1) OT Discussion**:** Vendor relationships and spare parts strategies are developed to ensure an adequate supply of critical components is available to meet operational needs.

Rationale for adding SR-5 (1) to MOD and HIGH baselines: OT systems and system components are often built-for-purpose, with a limited number of vendors/suppliers of a specific component. Organizations identify critical OT system components and controls to ensure an adequate supply in the event of supply chain disruptions.

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-6	**Supplier Assessments and Reviews**		Select	Select

No OT Discussion for this control.

SR-8 NOTIFICATION AGREEMENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-8	**Notification Agreements**	Select	Select	Select

No OT Discussion for this control.

SR-9 TAMPER RESISTANCE AND DETECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-9	**Tamper Resistance and Detection**			Select
SR-9 (1)	*TAMPER RESISTANCE AND DETECTION* | *MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE*			Select

No OT Discussion for this control.

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-10	**Inspection of Systems or Components**	Select	Select	Select

No OT Discussion for this control.

SR-11 COMPONENT AUTHENTICITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-11	**Component Authenticity**	Select	Select	Select
SR-11 (1)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*	Select	Select	Select
SR-11 (2)	*COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR*	Select	Select	Select

No OT Discussion for this control.

SR-12 COMPONENT DISPOSAL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-12	**Component Disposal**	Select	Select	Select

No OT Discussion for this control.