NIST Special Publication 800
NIST SP 800-82r4 ipd

Guide to Operational Technology (OT) Security

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Adam Hahn
Jim Gilsinn
Daniel Rebori-Carretero
Otis Alexander
Michael Fialk
Zackary Louis Silva

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r4.ipd

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

NIST Special Publication 800
NIST SP 800-82r4 ipd

Guide to Operational Technology (OT) Security

Initial Public Draft

Keith Stouffer
Michael Pease
CheeYee Tang
Applied Cybersecurity Division
Information Technology Laboratory

Adam Hahn
Jim Gilsinn
Daniel Rebori-Carretero
Otis Alexander
Michael Fialk
Zackary Louis Silva
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r4.ipd

September 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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.

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.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]
Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication, if applicable.]

How to Cite this NIST Technical Series Publication
Stouffer K, Pease M, Tang C, Hahn A, Gilsinn J, Rebori-Carretero D, Alexander O, Fialk M, Silva ZL (2026) Guide to Operational Technology (OT) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r4 ipd. https://doi.org/10.6028/NIST.SP.800-82r4.ipd

Author ORCID iDs
Keith Stouffer: 0000-0003-1220-5487
Michael Pease: 0000-0002-6489-2621
CheeYee Tang: 0009-0000-2847-1443
Adam Hahn: 0000-0003-1214-3466
Zackary Louis Silva: 0000-0002-0721-1420

Public Comment Period
September 21, 2026 – November 30, 2026

Submit Comments
sp800-82rev4@nist.gov

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

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/82/r4/ipd, including related content, potential updates, and document history.

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

Abstract

This document provides guidelines 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, such as industrial control systems, building automation and control systems (BACS), freight railroad, maritime vessels, water and wastewater systems (WWS), Industrial Internet of Things (IIoT), and cloud environments. This document provides an overview of OT and typical system topologies, identifies common threats and vulnerabilities to these systems, and offers recommended security countermeasures to mitigate the associated risks in alignment with the NIST Cybersecurity Framework (CSF) 2.0.

Keywords

computer security; distributed control system (DCS); industrial control system (ICS); information security; network security; operational technology (OT); programmable logic controller (PLC); risk management; security controls; supervisory control and data acquisition (SCADA); NIST Cybersecurity Framework (CSF) 2.0; zero trust.

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.

Note to Reviewers

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

- Expanded introduction to operational technology (OT) sectors to include Building Automation and Control Systems (BACS), Water and Wastewater Systems (WWS), food and agriculture, freight rail, maritime vessels, and Industrial Internet of Things (IIoT) and cloud convergence
- Restructured around the NIST Cybersecurity Framework (CSF) 2.0, including a reorganization of the previous risk management section to focus on the CSF Govern Function
- Expanded discussion of how OT risk management aligns with broader enterprise risk management, as described in NIST IR 8286r1
- Discussion of the adoption of the NIST Risk Management Framework (RMF) in Appendix F
- Expanded guidance on implementing OT security controls, including asset management and network monitoring and detection
- Security architecture guidelines focused on protecting system management functions and applying zero trust principles
- Appendix C, “Threat Sources, Vulnerabilities, and Incidents,” and Appendix D, “OT Security Organizations, Research, and Activities,” to be moved to web-based resources to support more timely content updates in the final publication
- Appendix E, “OT Overlay,” and Appendix F, “Applying the Risk Management Framework to OT Systems,” to be moved to separate documents in the final publication

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: sp800-82rev4@nist.gov

78 **Table of Contents**

List of Tables

List of Figures

Acknowledgments for Revision 4

The authors will acknowledge colleagues who have made significant contributions to this document in the final publication.

Acknowledgement 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, Lisa Kaiser, Department of Homeland Security, the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG), the Office of the Deputy Undersecretary of Defense for Installations and Environment, and Business Enterprise Integration Directorate staff 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. The authors would also like to thank Sallie Edwards, Blaine Jefferies, and John Hoyt, Megan Corso, Eran Salfati, Karen Scarfone, and Isabel Van Wyk.

Executive Summary

This document provides guidelines 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 do so. These systems and devices detect or cause a direct change through the monitoring and/or control of other 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. This document provides an overview of OT and typical system topologies, identifies common threats and vulnerabilities to these systems, and recommends security countermeasures to mitigate the associated risks.

OT is vital to the operation of U.S. critical infrastructure, which is often highly interconnected and mutually dependent. While federal agencies operate much of the Nation's critical infrastructure, a significant portion of it is privately owned and operated. Additionally, critical infrastructure is often referred to as a "system of systems" because of the interdependencies among various industrial sectors and the interconnections among business partners.

Initially, OT had little resemblance to traditional information technology (IT) systems because OT systems were isolated, ran proprietary control protocols, and used specialized hardware and software. As OT systems continue to adopt IT solutions to enable connectivity to enterprise business systems and remote access, they are being designed and implemented using industry-standard computers, operating systems (OSs), and network protocols, thus increasing their resemblance to IT systems. This integration supports new IT capabilities but provides significantly less isolation of OT from the outside world than predecessor systems. The increasing use of wireless networking places OT implementations at greater risk from adversaries who are in close physical proximity but lack direct physical access to the equipment. While security solutions have been designed to address these issues in typical IT systems, special precautions must be taken when introducing the same solutions into OT environments. In some cases, new security solutions that are tailored to the OT environment are needed.

The Evolving Threat Landscape and Mission and Business Risk

Although some characteristics are similar, OT also has features that differ from those of traditional information processing systems. Many of these differences stem from the fact that logic executing in OT directly affects the physical world. Some of these characteristics include significant risks to the health and safety of human lives, serious damage to the environment, and severe financial issues, such as production losses, negative impacts to the Nation's economy, and the compromise of proprietary information. OT has unique performance and reliability requirements and often uses OSs and applications that may be considered

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

unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of OT systems.

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, system complexities, natural disasters, malicious insider actions, and unintentional actions (e.g., human error, failure to follow established policies and procedures). OT security objectives typically prioritize safety, followed by integrity, availability, and confidentiality.

To mitigate the unique threats facing operational environments, organizations must align their defensive strategies with potential operational consequences. Table 1 outlines possible OT incidents alongside their corresponding security objectives.

Table 1. OT cyber risks and security objectives

Strategic Focus	Potential OT Incident / Consequence	Key Security Objective
Access & Architecture **(Protect)**	- Unauthorized changes to instructions, commands, or alarm thresholds that could damage equipment or endanger life - Modified software or configurations, including malware infections	- **Restrict Logical Access:** Employ multi-layer network topologies, DMZs, and unidirectional gateways, and separate IT/OT credentials. - **Restrict Physical Access:** Use physical controls (e.g., locks, card readers, guards) to protect components. - **Protect Components:** Deploy tested patches, disable unused ports, and restrict user privileges.
System & Data Integrity **(Protect & Detect)**	- Inaccurate information sent to operators to disguise malicious actions or prompt inappropriate responses - Interference with the operation of equipment protection or safety systems	- **Restrict Data Modification:** Protect data from unauthorized modification in all states (i.e., at rest, in transit, in use) and across network boundaries. - **Detect Events:** Deploy continuous monitoring to detect failed components, exhausted resources, and anomalies to break the attack chain early.
Resilience & Continuity **(Respond & Recover)**	- Blocked or delayed flow of information through OT networks, causing a critical loss of view or loss of control for operators	- **Maintain Functionality:** Design redundant systems that are capable of graceful degradation (moving from automated to manual operations) during adverse conditions. - **Restore and Recover:** Develop and rigorously test incident response

Strategic Focus	Potential OT Incident / Consequence	Key Security Objective
		plans to ensure rapid system recovery.

Strategic Governance and Risk Management

Because cyber incidents can directly cause safety and reliability failures, OT cybersecurity programs must be seamlessly integrated into broader enterprise risk management (ERM) and facility safety programs. Effective OT governance requires organizations to focus on the following strategic imperatives:

- **Shared governance and accountability:** Securing OT requires a shared governance structure that brings together senior leadership, OT, IT, safety, legal, operations, and other relevant stakeholders to establish the program's scope, assign responsibilities, and coordinate day-to-day cybersecurity activities. Ultimate accountability for OT cybersecurity and any resulting physical impacts resides with executive leadership, including the Chief Executive Officer (CEO), Chief Operating Officer (COO), and Chief Information Officer (CIO) or Chief Security Officer (CSO).
- **OT risk management strategy:** Organizations must establish how OT cybersecurity risks are prioritized, evaluated, tracked, reported, and addressed in a manner consistent with the organization's mission, operational requirements, and risk tolerance. This includes maintaining risk registers and documenting risk responses (e.g., mitigate, transfer, accept, avoid).
- **Supply chain risk management:** Organizations should manage cybersecurity supply chain risks that arise from the products, services, suppliers, and third parties that support OT environments. Because OT systems often depend on specialized equipment and remote vendor maintenance, organizations must vet suppliers to ascertain the adequacy of their internal security practices and continuously manage supplier risk across the product lifecycle.

Core OT Cybersecurity Capabilities: A Defense-in-Depth Strategy

Organizations should not rely on "security by obscurity." Securing OT requires a consequence-driven defense-in-depth strategy that not only layers security mechanisms to minimize the impact of a failure in any single control but also aligns with the core functions of the NIST Cybersecurity Framework (CSF) 2.0:

- **Identify:** Organizations must establish an accurate inventory of hardware, software, and network baselines to fully understand asset criticality. Risk assessments must evaluate both logical dependencies and potential physical consequences.
- **Protect:** Safeguards must be implemented without compromising continuous physical processes. This includes using multi-layer network topologies, restricting logical and

physical access through role-based privileges and demilitarized zones (DMZs), and securing data at rest and in transit with appropriate cryptography.

- **Detect:** Organizations must deploy continuous monitoring across networks, devices, and physical environments to identify anomalies, unauthorized changes, and cyber threats before they escalate into high-impact incidents.
- **Respond and Recover:** Incidents are inevitable, making robust incident response plans essential. Systems must be designed for graceful degradation, moving from full automation to manual operations if necessary, and recovery procedures must ensure the safe, timely restoration of physical processes.

Unlike traditional IT environments, security controls in OT must never compromise continuous physical processes. Therefore, the defense-in-depth implementation strategies outlined in Table 2 should be applied ***when safe, technically feasible*** and thoroughly tested to ensure that they do not adversely affect OT operations or human safety.

Table 2. Components of an OT defense-in-depth strategy

Strategic Domain (Focus)	Implementation Strategies
Governance & Life Cycle **(Policy & Program Management)**	- Develop OT-specific security policies, procedures, training, and educational material. - Align security postures with the National Terrorism Advisory System (NTAS). - Address security throughout the entire system life cycle, from architecture design and procurement to operations and decommissioning.
Architecture & Boundaries **(Network Isolation & Topologies)**	- Implement multi-layer network topologies that keep critical communications in the most secure layers. - Provide logical and physical separation between enterprise and OT networks using DMZs, stateful firewalls, and unidirectional gateways. - Employ reliable and secure network protocols.
Access Control **(Identity & Privilege Management)**	- Restrict physical access to OT networks and devices. - Enforce the principle of least privilege using role-based access control (RBAC). - Require multi-factor authentication (MFA) for remote access, and use modern technologies (e.g., smart cards). - Maintain separate authentication mechanisms and credentials for IT and OT networks.
System Protection & Detection **(Asset Hardening & Monitoring)**	- Expeditiously deploy security patches after testing them under field conditions. - Disable unused ports and services. - Apply encryption and/or cryptographic hashes to protect data.

Strategic Domain (Focus)	Implementation Strategies
	- Implement malware protection, intrusion detection, and file integrity checking. - Track and monitor audit trails in critical areas.
System Resilience **(Fault Tolerance)**	- Ensure that critical components and networks are redundant. - Design critical systems for graceful degradation to prevent catastrophic cascading events.

OT Cybersecurity Architecture and the SP 800-53r5 Overlay

In cooperation with the public and private-sector OT community, NIST has developed specific guidelines (see Appendix E) for applying the security controls in NIST Special Publication (SP) 800-53r5 (Revision 5), *Security and Privacy Controls for Information Systems and Organizations* [SP800-53r5], to OT. While many of the controls in SP 800-53r5 are applicable to OT as written, some controls require OT-specific interpretation and/or augmentation by adding one or more of the following:

- **OT Discussion** provides organizations with additional information on the application of security controls and control enhancements to OT and the environments in which these specialized systems operate. This also explains 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 SP 800-53r5.
- **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, OT engineers and operators, the IT organization, and a trusted OT advisor. This team should draw upon the wealth of information available from the Federal Government, industry groups, vendors, and standards activities.

1. Introduction

1.1. Purpose and Scope

The purpose of this document is to provide guidelines for establishing secure OT[2] while addressing its unique performance, reliability, and safety requirements. This document provides an overview of OT systems and typical system topologies, identifies common threats and vulnerabilities, and recommends security countermeasures to mitigate associated risks. The recommendations are aligned with the NIST Cybersecurity Framework (CSF) 2.0. Additionally, it presents an OT-tailored security control overlay based on NIST Special Publication (SP) 800-53r5 (Revision 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. ***It should not be used as a checklist to secure a specific system.*** Readers are encouraged to conduct a risk-based assessment of their systems and tailor the recommended guidelines and solutions to their specific security, business, and operational requirements. The range of applicability of the basic concepts for securing OT systems presented in this document will continue to expand.

1.2. Audience

This document covers details that are specific to OT systems. Readers of this document should be familiar with general computer security concepts and communication protocols, including those used in networking. The document is technical in nature but 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 needs to better understand the risks to OT systems as they justify and apply an OT cybersecurity program
- Researchers and analysts who are trying to understand the unique security needs of OT systems

[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 who 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 compared with IT systems. It provides a more in-depth review of various OT sectors, including building automation, maritime, freight railroad, water, and agriculture. It also discusses the growing convergence of OT with IIoT and cloud environments.
- Section 3 discusses implementation of the Govern CSF function to address risk management and governance in an OT environment, including organizational context and shared governance, OT risk management strategy, cybersecurity supply chain risk management (C-SCRM), and OT security policy and oversight.
- Section 4 provides OT-specific guidelines for implementing the CSF's Identify, Protect, Detect, Respond, and Recover functions.
- Section 5 provides recommendations for integrating security into network architectures that are typically found in OT systems with an emphasis on network segmentation and separation practices.
- The References section provides a list of citations used in the development of this document.

This guide also contains several appendices with supporting material:

- Appendix A lists the acronyms and abbreviations used in this document.
- Appendix B contains a glossary of the terms used in this document.

While included in this draft for public review, the following appendices will be transitioned to online supplemental resources or separate documents for the final publication:

- Appendix C discusses OT threat sources, vulnerabilities, predisposing conditions, threat events, and incidents.
- Appendix D presents lists and descriptions of OT security organizations, research, and activities.
- Appendix E defines the SP 800-53r5 OT overlay and lists security controls, enhancements, and supplemental guidance that apply specifically to OT systems.
- Appendix F includes guidelines for implementing the NIST Risk Management Framework (RMF) on OT systems.

2. OT Overview

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

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

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

This section provides an overview of several types of common OT systems, including supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), building automation systems (BASs), physical access control systems (PACSs), and the Industrial Internet of Things (IIoT). Diagrams depict the network topology, connections, components, and protocols that are typically used for each system type. These examples only attempt to identify notional concepts in topology. Actual implementations of these types of control systems may be hybrids that blur the lines between them. The diagrams in this section do not focus on securing OT. Security architecture and security controls are discussed in Sec. 5 and Appendix E 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 driven this evolution and led to many of today's "smart" technologies, such as the smart electric grid, smart transportation, smart buildings, smart manufacturing, and IoT. While this increases the connectivity and criticality of these systems, it also creates a greater need for their adaptability, resilience, safety, and security. Engineering OT continues to provide new capabilities while maintaining the typical longevity of these systems. The introduction of IT capabilities into physical systems presents emergent behavior

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

with security implications. Engineering models and analyses are evolving to address these emergent properties, including interdependence across safety, security, privacy, and environmental impact.

2.2. OT-Based Systems and Their Interdependencies

OT is used in many industries and infrastructures, including those identified by the Cybersecurity and Infrastructure Security Agency (CISA) as critical infrastructure sectors listed below. OT can be found across all critical infrastructures and is more prevalent in the sectors highlighted in bold and marked with an asterisk (*):

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

OT is vital to the operation of U.S. critical infrastructure, which is often highly interconnected and mutually dependent, both physically and through a host of information and communications technologies. While federal agencies operate many of the critical infrastructures mentioned above, many others are privately owned and operated. Additionally, critical infrastructure is often referred to as a “system of systems” because of interdependencies among industrial sectors and interconnections among business partners [Peerenboom][Rinaldi]. An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures. For example, both the electrical power transmission and distribution grid industries use geographically distributed SCADA control technology to operate highly interconnected, dynamic systems comprising thousands of

public and private utilities and rural cooperatives that supply 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 the distribution of water, oil, and natural gas, as well as pipelines, ships, trucks, rail systems, and wastewater collection systems.

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

2.3. Strategic Defense Mindsets

Defense-in-depth (DiD) should be treated as more than layered cybersecurity tooling. It is a deliberate strategy to create diverse and independent barriers across people, processes, technology, and the physical system so that no single failure, person, control, or knowledge gap can lead directly to an unacceptable consequence. While administrative and technical controls (e.g., procedures, access control, network segmentation, monitoring, backups, detection, response plans, recovery capabilities) reduce risk, the primary objective in OT is to prevent or limit unsafe, unreliable, or destructive physical outcomes.

A mature OT defense mindset is consequence-driven. Cyber controls should be evaluated alongside engineering countermeasures that can remove or reduce the impact of a successful attack. For example, if manipulation of a control system could cause a tank to over-pressurize, the risk may be reduced not only through monitoring and access control but also through pressure relief valves, hardwired interlocks, safety instrumented functions, fail-safe design, or manual operating procedures. When selecting countermeasures, organizations should incorporate engineering-based methods (e.g., Cyber-Informed Engineering[4])[CIE] so that risk reduction includes both cyber resilience and physical process resilience.

[4] Wright, Virginia L., Jakob P. Meng, Robert S. Anderson, et al. *Cyber-Informed Engineering Implementation Guide*. INL/RPT-23-74072-Rev000. Idaho National Laboratory (INL), Idaho Falls, ID (United States), 2023. https://www.osti.gov/biblio/1995796.

2.4. OT System Operation, Architectures, and Components

A typical OT system includes numerous control loops, human-machine interfaces, and remote diagnostics and maintenance tools, as shown in Fig. 1.

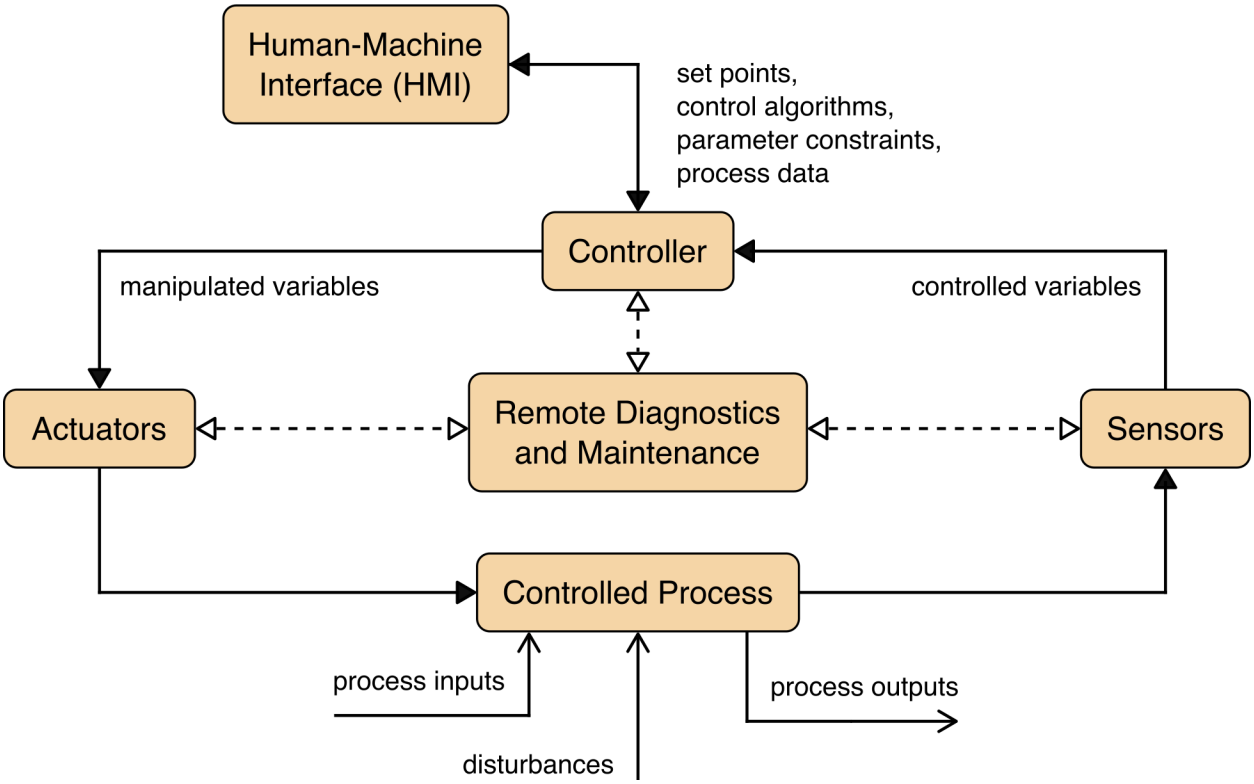

Fig. 1. Basic operation of a typical OT system

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 processes. A *sensor* is a device that measures a physical property and then sends that information as a controlled variable to the controller. The controller interprets the measurements, generates the corresponding manipulated variables based on a control algorithm and target set points, and transmits them to the actuators. *Actuators* (e.g., control valves, breakers, switches, motors) are used to directly manipulate the controlled process in response to commands from the controller.

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

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

Sometimes, control loops are nested and/or cascaded, meaning that 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 throughout a process with cycle times ranging from milliseconds to minutes.

2.4.1. OT System Design Considerations

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

- **Safety.** Systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations, human oversight and control of a potentially dangerous process are essential.
- **Control timing requirements.** System processes have a wide range of time-related requirements, including very high speed, consistency, regularity, and synchronization. Humans may be unable to reliably and consistently meet these requirements, so automated controllers may be necessary. Some systems may require computation to be performed as close to sensors and actuators as possible to reduce communication latency and perform necessary control actions on time.
- **Geographic distribution.** Systems have varying degrees of distribution, ranging from small systems (e.g., local PLC-controlled processes) 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 provides a central location that aggregates data from multiple locations to support control decisions based on the current state of the system. A hierarchical or centralized control is often used to provide human operators with a comprehensive view of the entire system.
- **Control complexity.** Simple controllers and preset algorithms can often perform control functions. However, more complex systems (e.g., air traffic control) require human operators to ensure that all control actions are appropriate for meeting the larger objectives of the system.

- **Availability.** Systems with stringent availability and uptime requirements may require greater redundancy or alternative implementations across all communications and controls.
- **Impact of failures.** The failure of a control function could cause substantially different impacts across domains. Systems with greater impacts often require the ability to continue operations through redundant controls or to operate in a degraded state.

2.4.2. SCADA Systems

SCADA systems are used to control dispersed assets for which centralized data acquisition is as important as control [Bailey][Boyer]. These systems are used in distribution systems, such as water distribution and wastewater collection systems, oil and natural gas pipelines, and electrical utility transmission and distribution 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, satellite), and one or more geographically distributed field sites consisting of remote terminal units (RTUs) and/or PLCs that control actuators and/or monitor sensors. The control server stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process. The communications hardware allows for the transfer of information and data between the control server and the RTUs or PLCs. The software is programmed to tell the system what to monitor, what parameter ranges are acceptable, and what response to initiate when a process variable changes outside of acceptable values. An intelligent electronic device (IED), such as a protective relay, may communicate directly to the control server, or a local RTU may poll the IEDs to collect the data and pass it to the control server. IEDs provide a direct interface for controlling and monitoring 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 with significant redundancy built in, although redundancy may not be a sufficient countermeasure against a malicious attack.

Figure 2 shows the components and general configuration of a SCADA system.

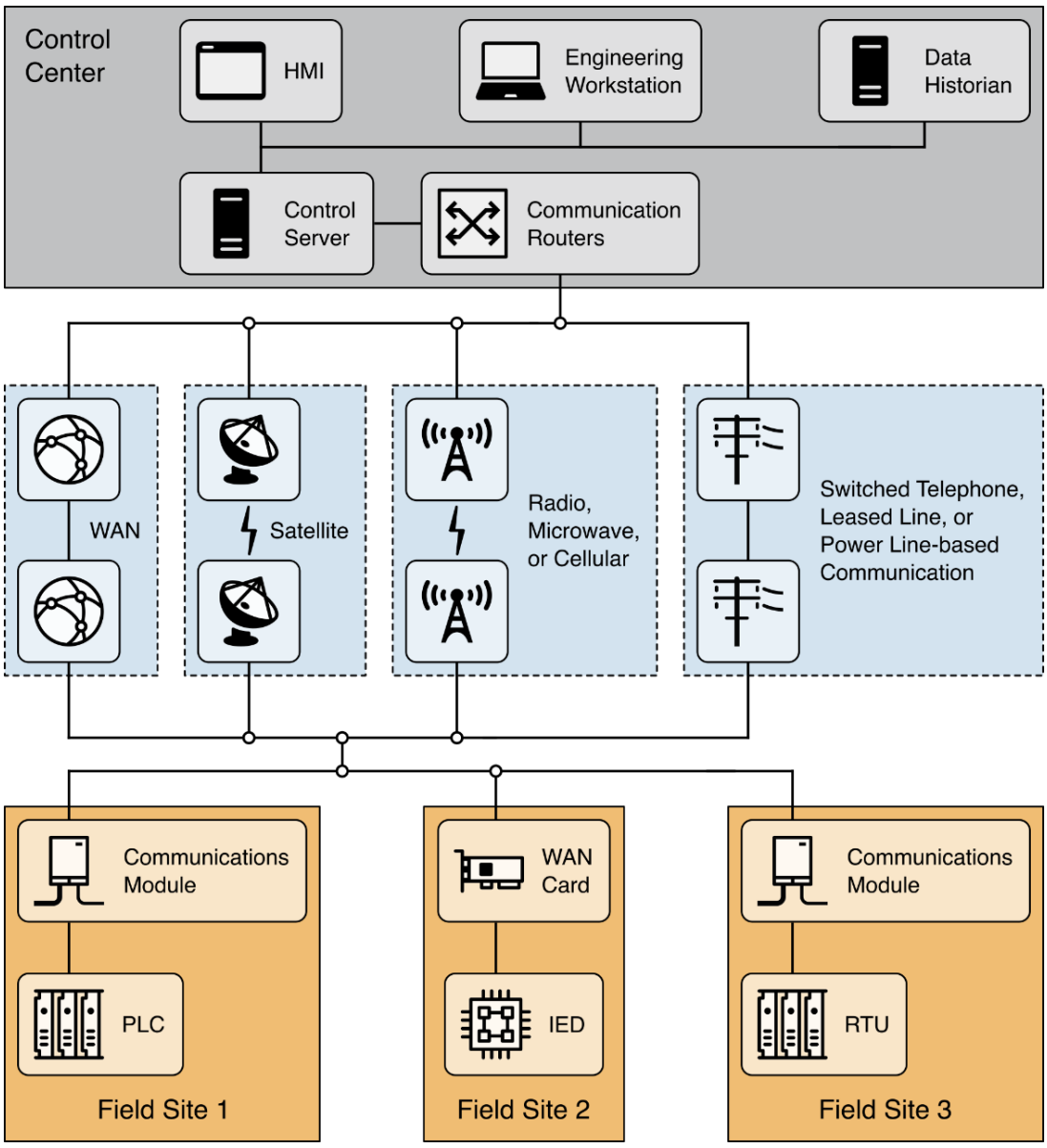

Fig. 2. A general SCADA system layout that shows control center devices, communications equipment, and field sites

The control center at the top of the diagram houses the control server and 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 it to the HMI, and may trigger actions based on detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting.

The field sites at the bottom of Fig. 2 locally control actuators and monitor sensors. Field sites are often equipped with remote access capabilities to allow operators to perform diagnostics and repairs, usually via a separate dial-up modem or a wide-area network (WAN) connection. Standard and proprietary communication protocols that run over serial and network

communications are used to transport information between the control center and field sites using telemetry techniques, such as telephone lines, cables, fibers, and radio frequencies (e.g., broadcast, microwave, satellite).

SCADA communication topologies vary among implementations. The various topologies used are shown in Fig. 3, including point-to-point, series, series-star, and multi-drop [AGA12].

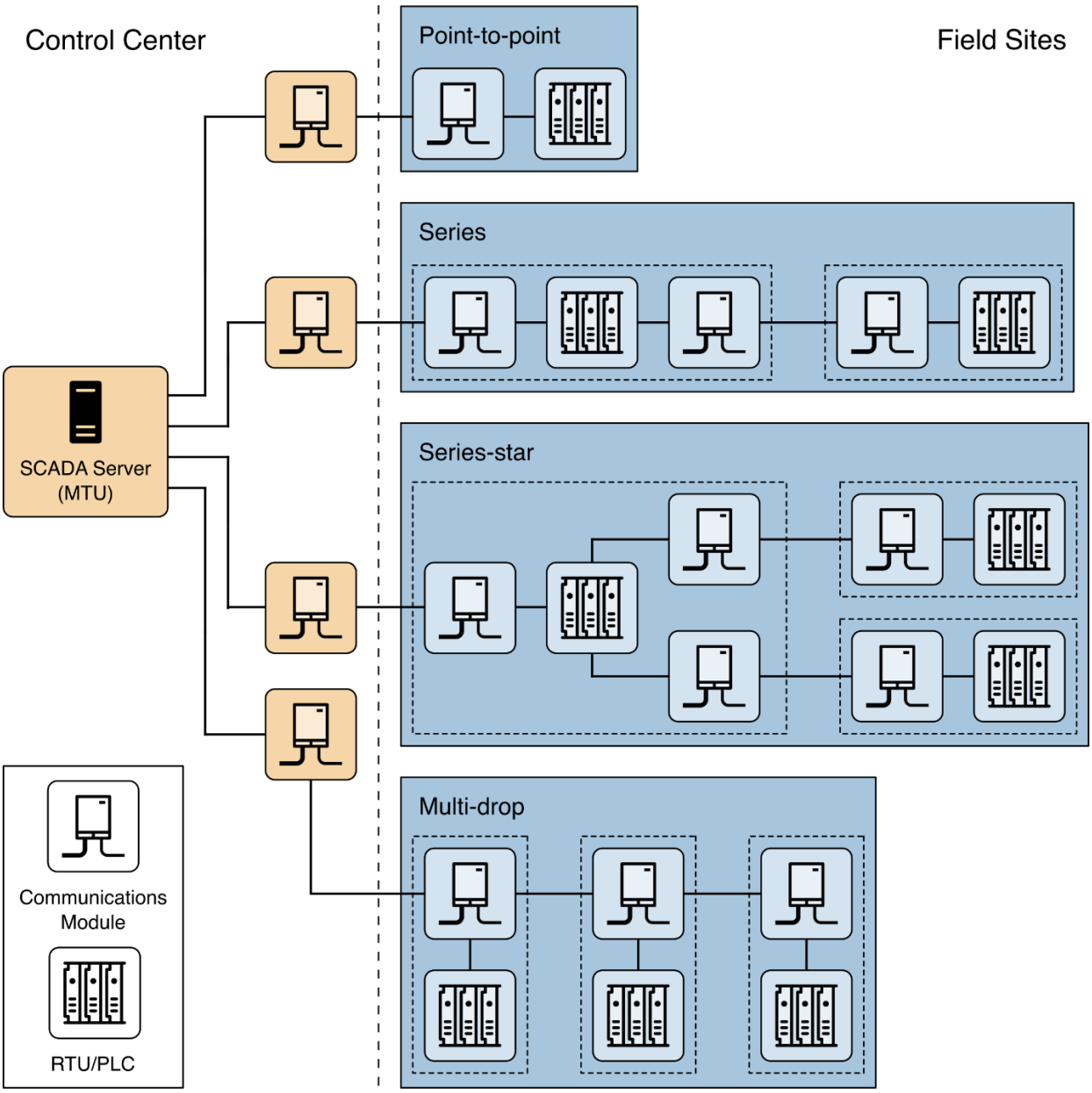

Fig. 3. Examples of point-to-point, series, series-star, and multi-drop SCADA communications topologies

Point-to-point is functionally the simplest type, though it can be expensive due to the individual channels required for each connection. In a series configuration, the number of channels used is reduced, but channel-sharing impacts the efficiency and complexity of SCADA operations.

Similarly, the series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and increased system complexity.

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

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

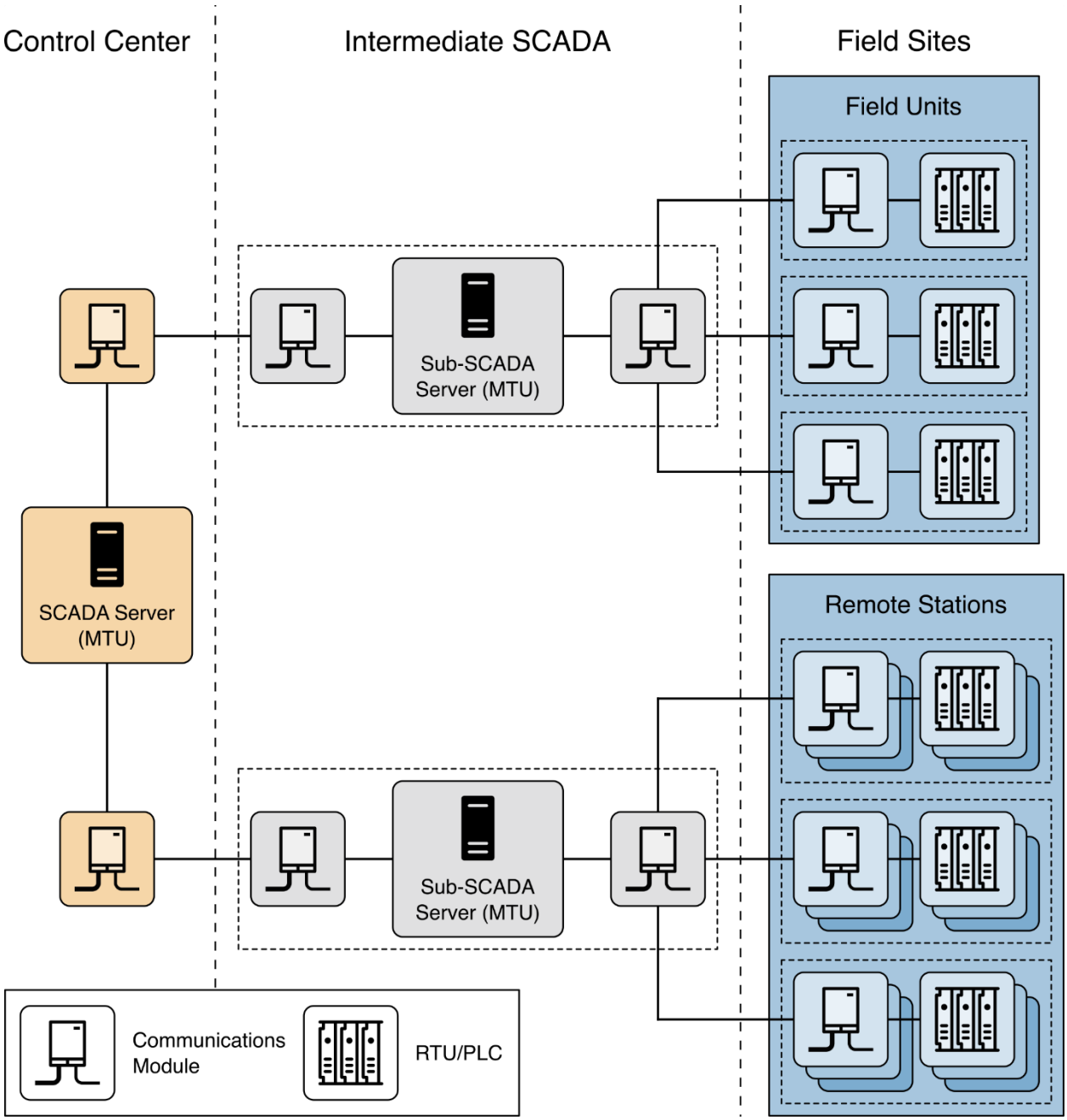

Fig. 4. An example SCADA topology that supports a large number of remote stations

Figure 5 shows an example SCADA system implementation that consists of a primary control center and three field sites.

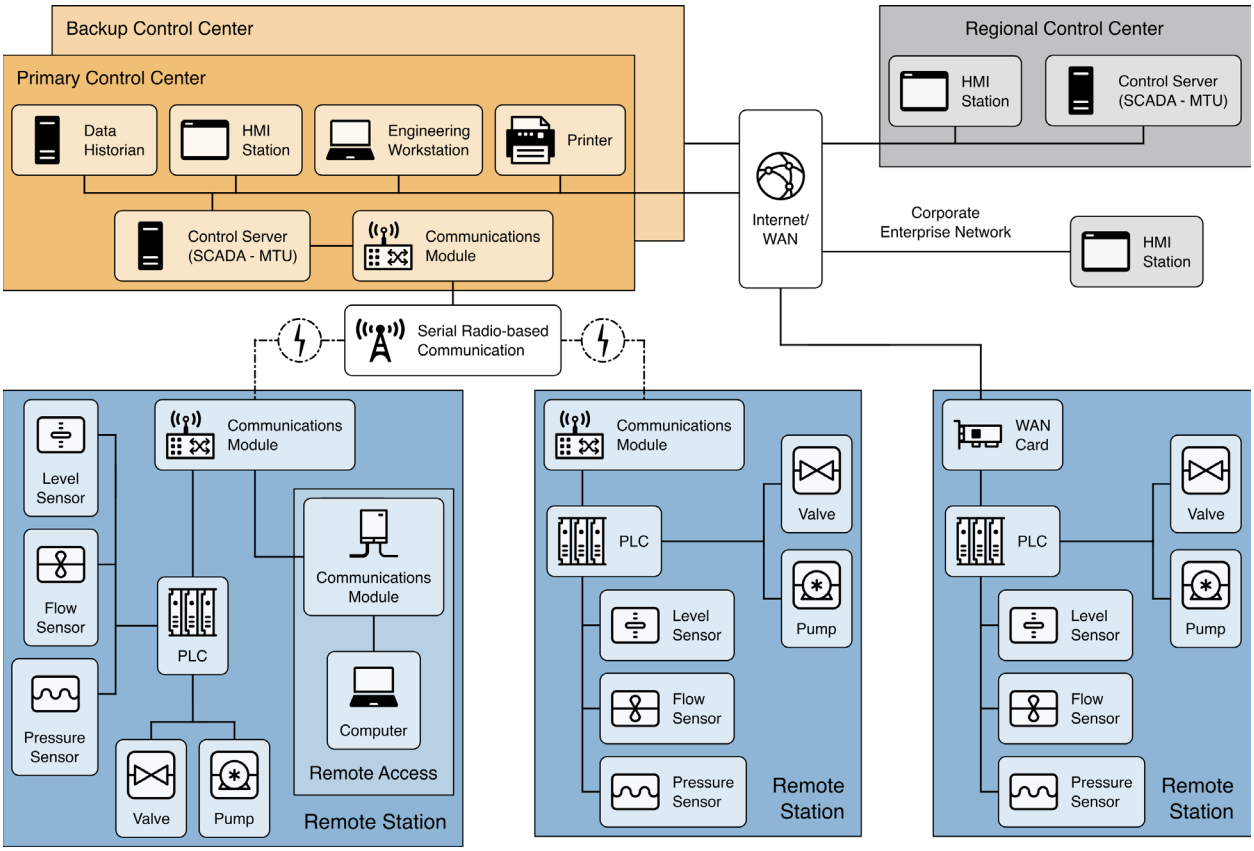

Fig. 5. A comprehensive SCADA system implementation example

A second backup control center provides redundancy in the event of a primary control center malfunction. Point-to-point connections are used for all communications between the control center and the field site, and two of those connections use radio telemetry. The third field site is local to the control center and uses the WAN for communications. A regional control center resides above the primary control center for a higher level of supervisory control. The enterprise network has access to all control centers via 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 monitors priority interrupts from field-site alarm systems.

2.4.3. Distributed Control Systems

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

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

Figure 6 shows an example implementation of the components and general configuration of a DCS.

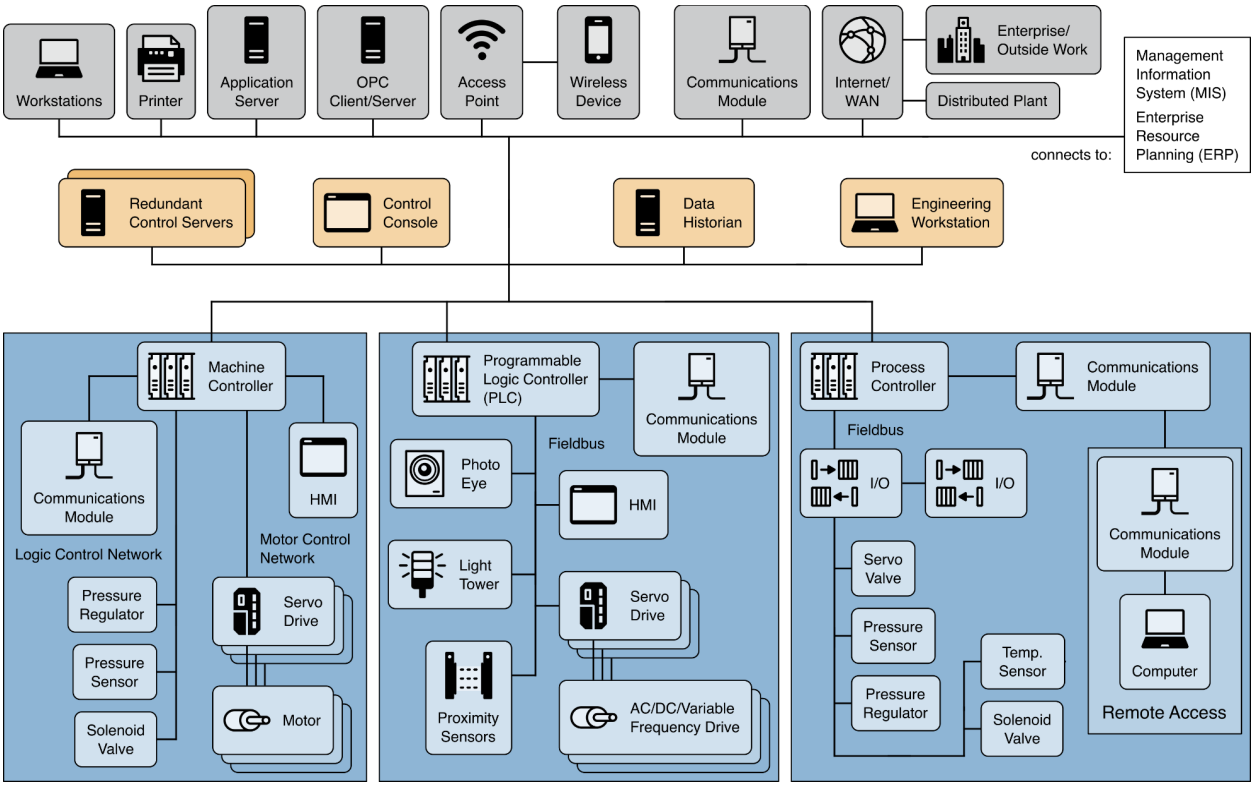

Fig. 6. A comprehensive DCS implementation example

This DCS encompasses an entire facility, from the bottom-level production processes up to the 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 6 also provides 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 via point-to-point wiring, while the

other three field devices use fieldbus networks to connect to process sensors and actuators. Fieldbus networks eliminate the need for point-to-point wiring between a controller and individual field sensors and actuators. Additionally, a fieldbus allows for greater functionality beyond control, including field device diagnostics, and can accomplish control algorithms within the fieldbus, thereby avoiding signal routing back to the PLC for every control operation. Standard industrial communication protocols designed by industry groups (e.g., 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 in 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.

2.4.4. Programmable Logic Controller-Based Topologies

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

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

Figure 7 shows a PLC over a fieldbus network performing the control of a manufacturing process. The PLC is accessible via a programming interface located on an engineering workstation, and data is stored in a data historian, all of which are connected on a LAN.

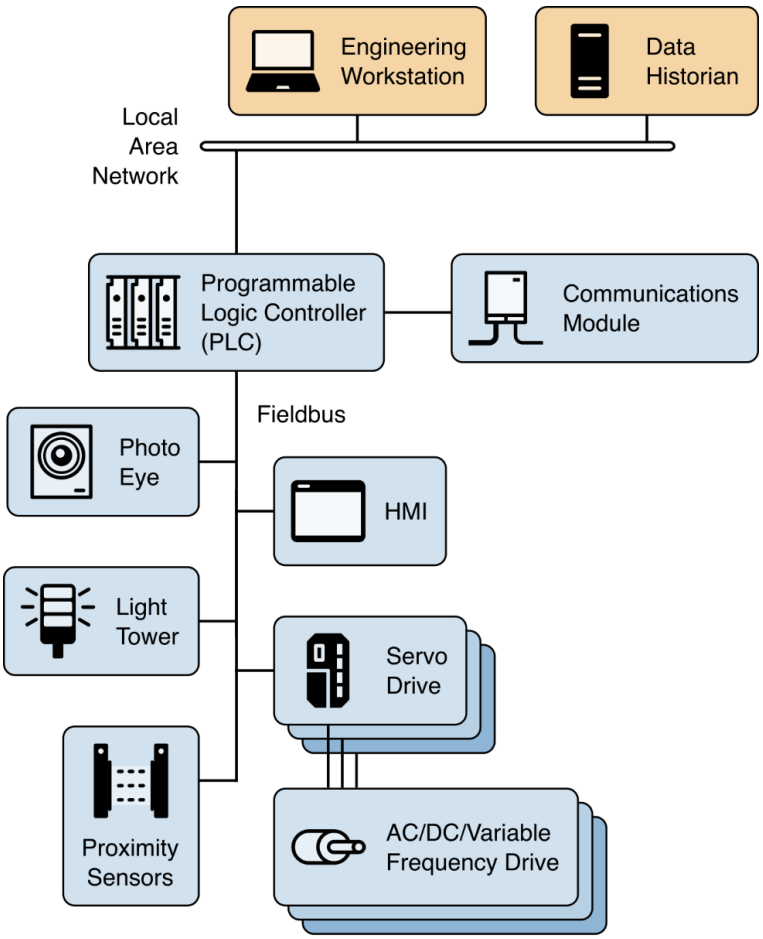

Fig. 7. A PLC control system implementation example

2.4.5. Safety Systems

Many of the physical processes that OT systems control have the potential to create hazardous situations to human life and safety, property, and the environment. Safety systems are designed to reduce the likelihood and/or consequences 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 shutdown (ESD), process safety shutdown (PSS), and fire and gas systems (FGS).

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

An SIS is often independent from all other control systems in such a manner that a failure of the basic process control system (BPCS) will not negatively affect SIS functionality. Historically, an SIS was designed to be stand-alone, physically and logically separated, and air-gapped from the rest of the control system. In the configuration shown in Fig. 8, the SIS and BPCS operate completely independently of each other with no direct communication between the systems.

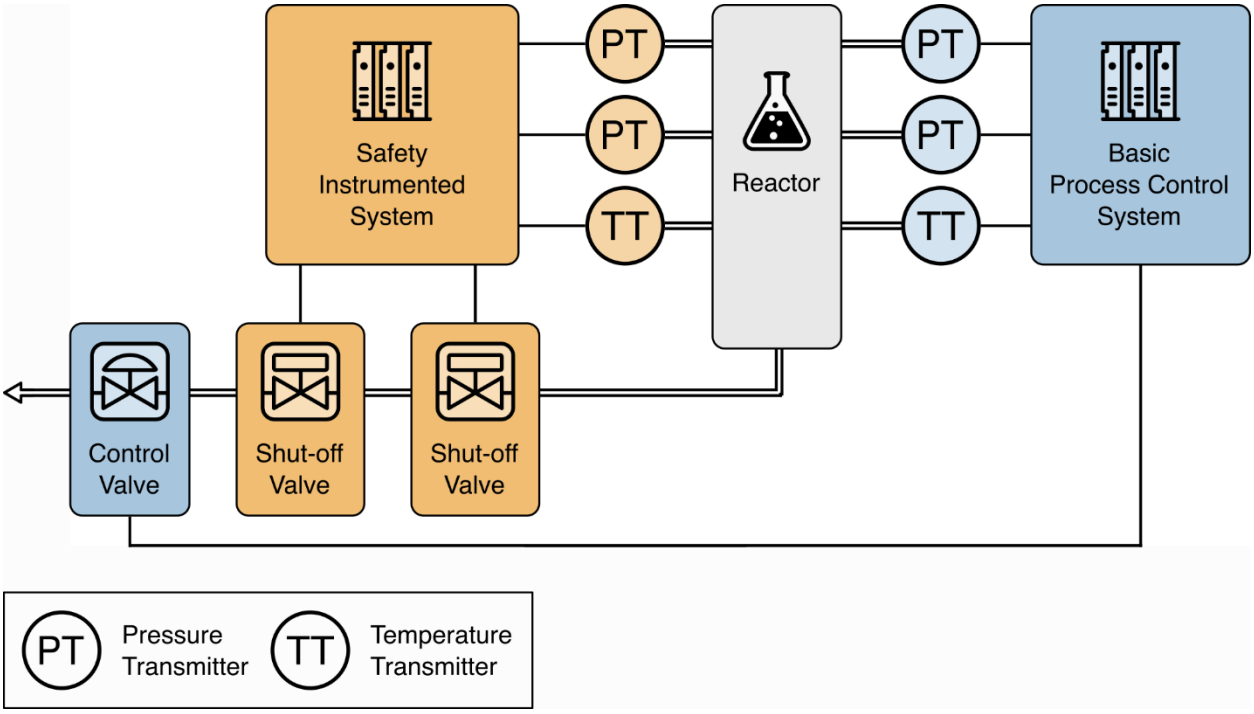

Fig. 8. An SIS implementation example

However, some modern SISs have been designed to allow communication with the control system. These types of SISs are called Integrated Control and Safety Systems (ICSSs). An ICSS solution may be an all-in-one device from a single vendor or incorporate multiple devices from multiple vendors. While an ICSS combines the functionality of both control and safety systems, the SIS must still comply with the requirements outlined in [IEC61511]. One of the advantages of this ICSS methodology is the ability to communicate information from the SIS to the BPCS.

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

2.4.6. Cloud and IoT/IIoT Convergence

OT environments are increasingly connected to cloud services, IoT, and IIoT platforms. Cloud environments are shared pools of configurable computing resources that are typically operated by external service providers. While IoT refers to both consumer and industrial devices connected to the internet, the Industrial IoT Consortium (IIC) defines IIoT as “subset of IoT and

focuses specifically on industrial applications such as transportation, manufacturing, healthcare, energy and agriculture" [IIC1].

These technologies can support data collection, monitoring, analytics, remote access, enterprise integration, predictive maintenance, managed services, and security operations. Common examples include advanced metering infrastructure (AMI), environmental and asset condition monitoring, enterprise resource planning (ERP), manufacturing execution systems (MES), security information and event management (SIEM), vulnerability management, threat detection, remote engineering access, and zero trust network access (ZTNA). These capabilities can reduce the need to operate some local infrastructure and offer provider-managed scalability, analytics, maintenance, and security capabilities. That said, these integrations can also expand the OT attack surface by introducing externally operated services, remotely managed devices, shared infrastructure, and new communication paths into or near OT networks.

Figure 9 illustrates an example architecture with IIoT and cloud connectivity.

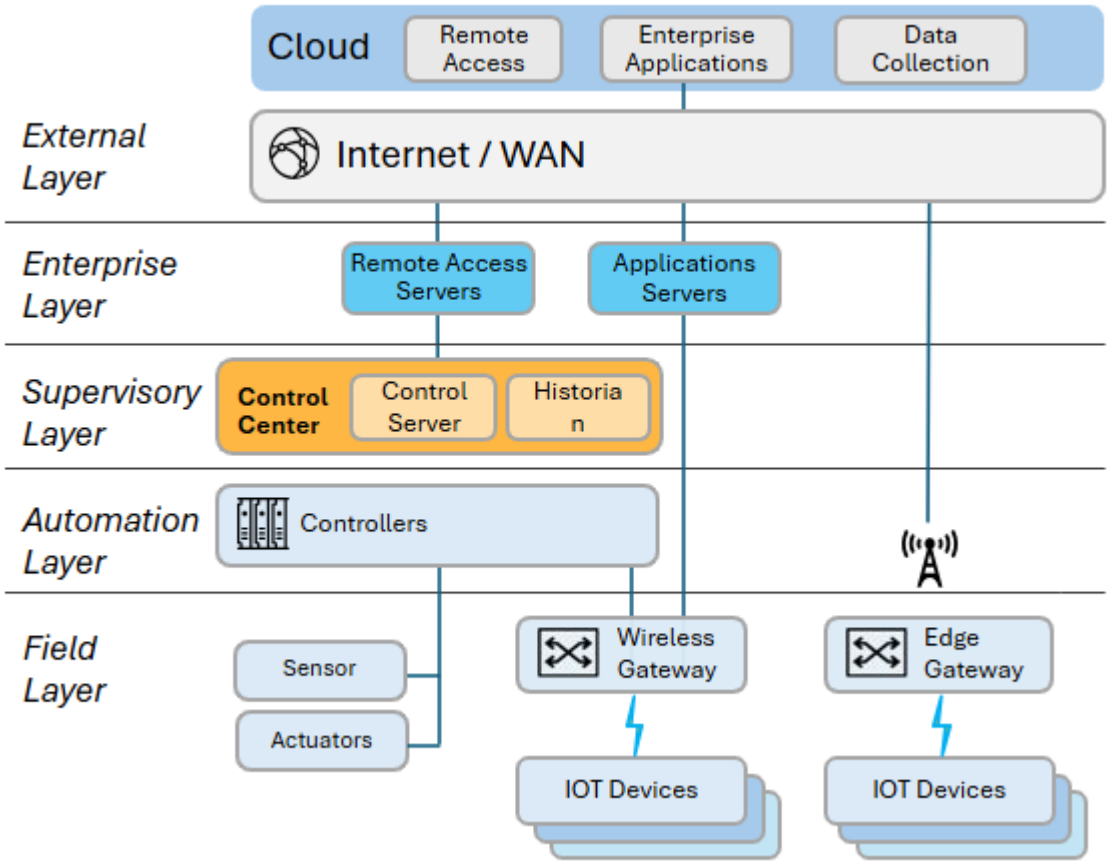

Fig. 9. Cloud and IIoT convergence example architecture

IIoT architectures commonly include sensors, instruments, machines, edge gateways, wireless or wired access networks, and backend platforms hosted on premises, in the cloud, or with a

vendor. Cloud, IoT, and IIoT integrations can be implemented using several common architectural patterns, such as:

- **Telemetry-to-cloud architecture.** Sensors, monitoring devices, or gateways send selected operational data to a cloud platform for dashboards, analytics, reporting, or predictive maintenance. Control functions typically remain local.
- **Edge gateway architecture.** OT devices communicate with an industrial gateway or edge platform that normalizes protocols, filters data, enforces policy, and forwards selected data to cloud, vendor, or enterprise systems.
- **Remote access/ZTNA architecture.** Cloud-hosted identity, broker, or zero trust access services mediate remote engineering, vendor support, or administrative access into the OT environment.

Cloud and IIoT integrations can introduce dependencies on external services, vendor-managed devices, telecommunications providers, SaaS platforms, and cloud infrastructure. These dependencies can complicate many security functions and require additional planning, coordination, and controls, especially when used to expand existing OT systems. Examples of key considerations include:

- **Shared responsibility.** Organizations should define responsibility for identity and access management, patching, configuration, monitoring, logging, incident response, backup, vulnerability handling, and recovery. These responsibilities may be shared among OT, IT, cloud providers, SaaS providers, telecommunications providers, system integrators, and equipment vendors.
- **Availability and resilience.** Organizations should determine which OT functions can tolerate loss of cloud, vendor, or communications services. Safety, protection, and time-critical control functions should generally remain capable of local operation with documented fallback, fail-safe behavior, and tested recovery procedures.
- **Data governance and terms of use.** Organizations should review what data is collected, transmitted, stored, analyzed, retained, or shared by cloud and IIoT devices. This includes operational data, asset information, logs, metadata, user activity, and maintenance data. Terms of use, contracts, and service agreements should define data ownership, access rights, storage location, third-party sharing, retention, deletion, and security protections.
- **Network boundaries and communications.** Connections between OT systems, IIoT devices, edge gateways, cloud services, and vendor environments should use defined and monitored boundaries, strong authentication, encrypted communications, least-privilege access, and logging. Cellular modems and vendor-managed connections can bypass enterprise and OT network security controls. Organizations should inventory and approve these connections, restrict what they can reach, monitor their use where possible, and prevent them from creating unmanaged paths into OT networks.
- **Device life cycle management.** IIoT devices should be inventoried, uniquely identified, securely configured, patched or otherwise mitigated, and monitored throughout their

life cycle. Organizations should evaluate default credentials, firmware update mechanisms, secure boot, vulnerability disclosure practices, vendor remote access, and end-of-support risks before deployment.

Organizations (e.g., Industry IoT Consortium) provide additional guidance on IIoT architectures and operations [IICSMM]. Further guidance on IoT security is defined in the following documents:

- SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*
- SP 1800-36, *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security*
- IR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*

2.5. Sector Specific Architecture and Security Challenges

Some sectors rely on specialized architectures and technologies that introduce distinct cybersecurity challenges. This section examines sector-specific architectures associated operational requirements and related cybersecurity considerations.

2.5.1. Building Automation and Control Systems (BACS)

A building automation and control system (BACS) is a type of OT system used to manage critical building infrastructure and optimize facility operations. These systems oversee heating, ventilation, and air conditioning (HVAC), fire safety, electrical and lighting systems, physical security and access controls, and energy management. While most modern buildings are constructed with BACS integration, older facilities often require retrofitting to achieve this level of centralized control and the associated operational benefits.

2.5.1.1. Architectures and Technologies

BACS may include supervisory-level systems that collect, analyze, and report data across many subsystems. The automation layer will have controllers for dedicated subsystems that may be connected to the supervisory layer, depending on system functions. The BACS may have multiple different subsystems, including:

- **Fire and life safety systems.** Fire and life safety systems are typically built around centralized fire alarm control panels connected to distributed detection, notification, and suppression field devices. These systems are often among the most critical BACS assets and should operate in an isolated or heavily segmented network with fail-safe architectures.

- **Electronic Security Systems (ESS).** ESS include systems used to monitor and control access to the facility. Physical access control systems (PACS) use access control panels to manage readers, credentials, locks, and door position sensors. PACS systems may be integrated with enterprise systems, especially identity management and monitoring. They may also include CCTV and motion sensors to monitor for unauthorized access.
- **HVAC systems.** HVAC systems use direct digital control (DDC) controllers to manage sensors, valves, dampers, and air handlers and may need integration with enterprise IT systems. HVAC systems can be critical because failures may create unsafe conditions or damage equipment if climate requirements cannot be maintained.
- **Lighting management systems.** Lighting systems use controllers to manage zones and respond to occupancy sensors. Lighting can be important for safety in certain locations.
- **Energy management systems.** Meters may be used to collect and monitor energy usage within the building.

An example of a BACS is shown in Fig. 10.

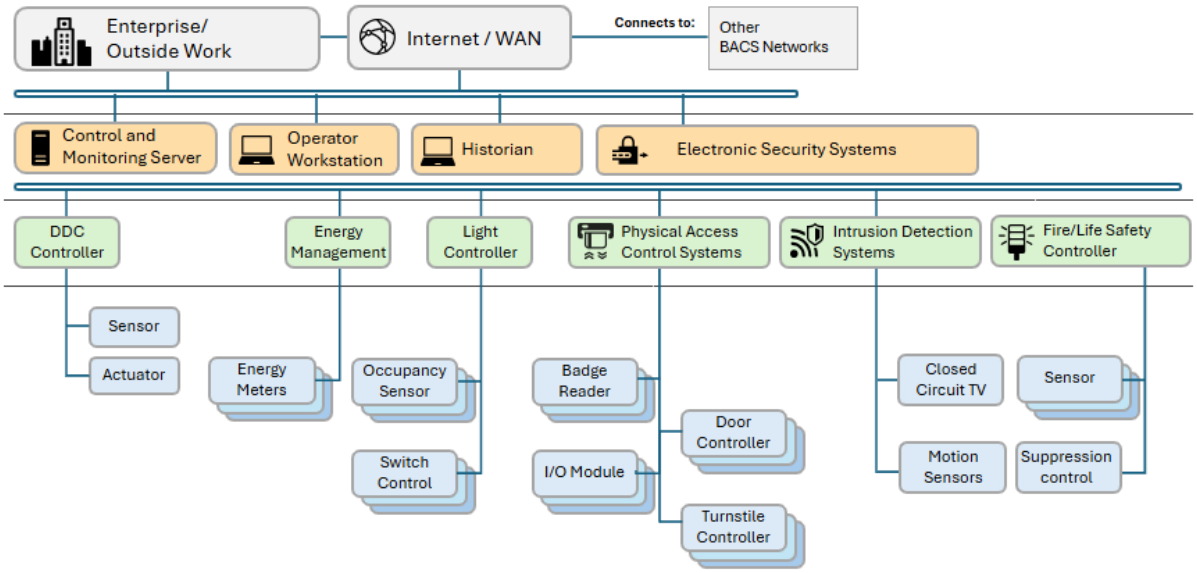

Fig. 10. Example BACS architecture

Key properties of BACS architectures include:

- **BACS environment variability.** BACS architectures can differ depending on the scale of the facility (e.g., a single building versus a campus environment). BACS subsystems can range from isolated analog systems to digital networked control systems that integrate multiple BACS subsystems through a single-pane-of-glass dashboard. Security needs for a BACS environment depend heavily on the extent to which the system uses digital technology, interconnects multiple subsystems, and requires connectivity with remote sites or external systems.

- **Unique criticality and risk across subsystems.** Different BACS subsystems have different criticality and cybersecurity risks. Some subsystems perform safety-critical functions (e.g., fire suppression, sprinkler activation, elevator safety) but may be isolated from other systems. Other subsystems are networked and integrated with supervisory control layers, which can increase their exposure to threats.
- **Commercial versus government/military operation.** Common architectures, technologies, and security requirements often vary significantly between commercial buildings and those used in government and defense environments. Therefore, organizations should explore guidance that is tailored to their specific operating environment.
- **Shared network infrastructure.** A BACS often leverages a building's existing telecommunications infrastructure because it is a highly efficient way to connect devices distributed across a large physical footprint. However, utilizing this shared medium can create unintended connection points and security vulnerabilities between the OT environment and the organization's enterprise IT network.
- **Use of wireless.** Wireless communications offer deployment flexibility, which is particularly beneficial when retrofitting older facilities where installing new cabling is impractical. However, wireless BACS deployments face specific physical and security challenges. Operationally, signals are prone to degradation and dead zones caused by structural building materials (e.g., concrete walls, steel, treated glass). From a security standpoint, because these signals are broadcast through spaces shared by a wide variety of occupants and visitors, they are inherently more exposed to eavesdropping, jamming, and unauthorized access.

2.5.1.2. Key Cybersecurity Challenges and Recommendations

Cybersecurity challenges and recommendations include:

- **Poorly defined security responsibility.** BACS security is often overlooked, primarily due to ambiguous governance responsibilities among facilities management, OT, and IT cybersecurity groups. This can be further complicated in buildings with landlord/tenant relationships, especially in multi-tenant commercial buildings. Unresolved items often include ownership of the BACS network, responsibility for security management, and accountability for BACS data. BACS security requires a shared responsibility model with clearly defined roles, including the owner of BACS security risk, the entity responsible for secure design, vulnerability management, and dedicated roles for security monitoring and operations.
- **Prioritize investments by criticality.** Due to the variety of BACS systems within a building, organizations may have to prioritize efforts and investments based on subsystem criticality rather than apply uniform controls across all BACS subsystems. Particular emphasis should be placed on safety-critical functions and systems that are

subject to regulatory requirements. Criticality should be validated with appropriate groups, including operations and technical teams.

- **Cybersecurity insufficiently defined during integration and commissioning.** BACS also commonly exhibits security challenges during the construction of new buildings, especially large commercial projects that can have many subcontractors with access to the OT network and devices. Common issues include default credentials, improperly managed laptops, and unauthorized remote access systems. Often, the commissioning process does not adequately address security, meaning default credentials or keys are never changed before the system transitions to production. Security responsibilities should be clearly defined for contractors who support building integration efforts. These responsibilities should specify who is accountable for securely configuring infrastructure, changing critical credentials and cryptographic keys during commissioning, and validating that these changes have been completed.
- **Insufficient incident response and recovery planning.** BACS systems and facilities personnel may not have performed adequate incident response and recovery planning or have not incorporated it into broader incident response and recovery plans within the organization. This means that BACS environments and personnel may not be adequately prepared to respond to an incident. Organizations should ensure that BACS environments are incorporated into their incident response plans along with supporting groups and external organizations (e.g., vendors, service providers). These activities need to be commensurate with the criticality of the subsystems and avoid overburdening key operational staff. The BACS environment should also include dedicated playbooks that address key threats, such as ransomware, unauthorized remote access, and integrity loss in critical systems. Tabletop exercises (TTXs) should be held periodically and should include BACS-specific scenarios. Recovery procedures should be documented and tested on representative devices and environments.
- **Cloud and AI adoption.** For new commercial installations, cloud-connected BACS is becoming the standard approach and may be required for full support and features. AI is also increasingly common for many BACS functions, including occupancy sensing, smart HVAC controls, appliance management, renewable energy balancing, and malfunction detection.
- **Regulatory requirements for safety and data collection.** BACS environments often have regulatory requirements that dictate the operation of safety-critical systems, such as elevators and fire suppression systems. Regulations may also require the reporting of data from buildings, such as for energy or environmental purposes. Organizations should understand relevant regulations and ensure that cybersecurity decisions and architectures broadly align with the associated requirements.

2.5.2. Food and Agriculture

Food and agriculture OT spans the full production chain: primary production (e.g., crop and animal agriculture), processing and manufacturing, storage and refrigeration, and distribution.

The majority of the segments in this chain overlap with OT sectors that have already been addressed in these guidelines. For example, processing corresponds to existing manufacturing guidance; storage and refrigeration correspond to building automation and cold-chain monitoring; and distribution corresponds to transportation OT. Because architectures, technologies, and security requirements vary significantly across these segments, organizations should apply guidance tailored to the specific segment of the food and agriculture chain in which they operate. This guidance accordingly focuses on the on-farm and first-handler environment and encompasses technologies such as guided and automated field equipment, irrigation control, livestock environmental control, and grain handling and storage.

2.5.2.1. Architectures and Technologies

Five system types cover most of the on-farm and first-handler footprint:

1. **Guided and automated field equipment.** Tractors, combines, planters, and sprayers use Global Navigation Satellite System (GNSS) guidance to support autosteer functions, while late-model machines report continuously to a manufacturer's cloud platform.
2. **Irrigation control.** Automated valves, center-pivot controllers, and soil-moisture sensor networks are often adjusted remotely over cellular links through small SCADA systems or vendor portals.
3. **Livestock environmental control and automated milking.** Ventilation and climate controllers are typically used in poultry and swine housing, robotic milking systems, RFID animal tracking, herd-management software (e.g., invisible fencing), and milk cooling tanks. These technologies are often closely interconnected, and a single compromised controller can disable an entire working operation.
4. **Grain handling and storage.** Dryers, aeration fans, and silo temperature and level sensors are frequently integrated with elevator automation at cooperatives.
5. **Farm-management and cooperative software platforms.** A cloud layer aggregates field data and returns prescriptions to equipment.

Key properties of food and agriculture control environments include:

- **Unique criticality across system types.** Different food and agriculture system types carry different criticality and risk profiles. Some directly affect animal life and welfare if compromised, such as livestock environmental control and milking systems. For example, a ventilation shutoff or emergency-stop function should sit on a circuit or controller that is independent of the monitoring and data systems so that a compromise of the monitoring layer cannot cascade into a safety failure. Others primarily affect operational continuity and economic outcomes, such as grain handling and farm-management platforms. Security priorities and controls should be calibrated to the specific consequences of each system type rather than applied uniformly.
- **Biological and environmental operating constraints.** Many food and agriculture control processes are governed by biological or environmental cycles rather than a schedule set

by operators. For example, animal welfare, growth cycles, and seasonal windows dictate when systems must run continuously and when they cannot be interrupted. These systems often have no downtime window, and a missed operating cycle cannot always be recovered afterward.

- **Prevalence of small, under-resourced operations.** Unlike many OT sectors dominated by large enterprises, food and agriculture is composed overwhelmingly of small operations. Most American farms lack dedicated compliance staff, security budgets, or reliable broadband; typically operate with limited resources; and often rely on manual processes, paper-based recordkeeping, and legacy analog or mechanical equipment. As a result, a baseline level of digital maturity or security posture cannot be assumed across the sector, and guidance intended for well-resourced enterprises will not reach most of the organizations that make up this space.
- **Reliance on public and shared networks.** Connectivity at the farm edge relies on whatever reaches a remote site, including cellular service across 3G, 4G, and 5G; commercial satellite; low-power wide-area networks, such as LoRaWAN; and Wi-Fi. That reliance extends to the operator's own device. Personal smartphones running vendor equipment apps and weather tools have become an operational interface of their own. These phones typically carry no security management and mix personal and farm use freely. On a small operation, the phone is often the only way to reach either function.
- **Equipment and fixed-installation protocols.** On equipment, the ISOBUS standard (ISO 11783) running over a Controller Area Network (CAN) bus handles communication between a tractor and its implements and governs interoperability rather than security. In fixed installations (e.g., irrigation, grain handling), Modbus and similar industrial protocols are common, and few carry authentication or encryption.

2.5.2.2. Key Cybersecurity Challenges and Recommendations

Cybersecurity challenges and recommendations include:

- **Guided and autonomous equipment vulnerable to signal disruption.** Guided and autonomous field equipment relies on GNSS signals and correction services, so spoofing, jamming, or natural disruption can halt or misdirect machinery across a wide area. Organizations should evaluate the availability of correction-service redundancy and manual fallback procedures for planting and harvest operations. They should confirm that equipment vendors disclose remote-access and remote-disable capabilities since a field operation needs to be completable if that connectivity is lost.
- **Platform dependence.** Farm operations and cooperatives frequently depend on a single cloud or software platform to conduct essential functions. When this platform is disrupted, the resulting impact is not confined to a single operation. Given the degree to which operations rely on a common underlying system, it may extend across an entire region or industry segment. Organizations should assess their dependence on individual platforms, maintain degraded-mode or offline-capable fallback procedures, and ensure

data portability so that no single platform constitutes an unrecoverable point of failure. For example, irrigation controllers should be segmented from the business network with inbound internet access removed, and grain-handling operations should maintain manual, offline procedures for receiving and movement so that a platform outage does not halt physical operations on its own.

- **Cyber incidents can surface as food-safety incidents.** Pasteurization, clean-in-place sanitation, and allergen dosing are governed by OT, so a manipulated setpoint or a lost monitoring record becomes a food-safety problem with the same consequences as contamination. Security controls in these environments should be evaluated jointly with food-safety teams, and cyber-incident scenarios should be built into food-safety hazard analyses.
- **Small operators lack security resources.** Most American farms are small operations without dedicated compliance staff or security budgets. For the large population of small operations, the critical security controls are multi-factor authentication, regular offline backups, sound password practices, and security awareness training, which together help deter the opportunistic automated scanning responsible for most attacks against this segment.
- **Cloud and AI adoption.** Cloud computing is already pervasive because manufacturer telematics platforms are cloud-based by default, and the associated risk is both operational dependence and an expanded network attack surface. AI adoption is growing in computer vision for weed and pest detection, yield prediction, and autonomy, raising concerns about the manipulation of sensor and vision inputs, the poisoning of training data, and the additional connectivity that these systems require.

2.5.3. Transportation — Freight Rail

Freight railroad environments rely on control systems to support the safe and reliable movement of trains across mainlines, yards, and terminals. These environments are highly distributed and often depend on a combination of fixed infrastructure, mobile assets, remote field equipment, and enterprise systems. Freight railroad OT environments can include train control systems, dispatch and traffic management systems, signal and interlocking systems, wayside monitoring systems, grade crossing warning systems, yard and terminal automation, locomotive onboard systems, and supporting telecommunications infrastructure.

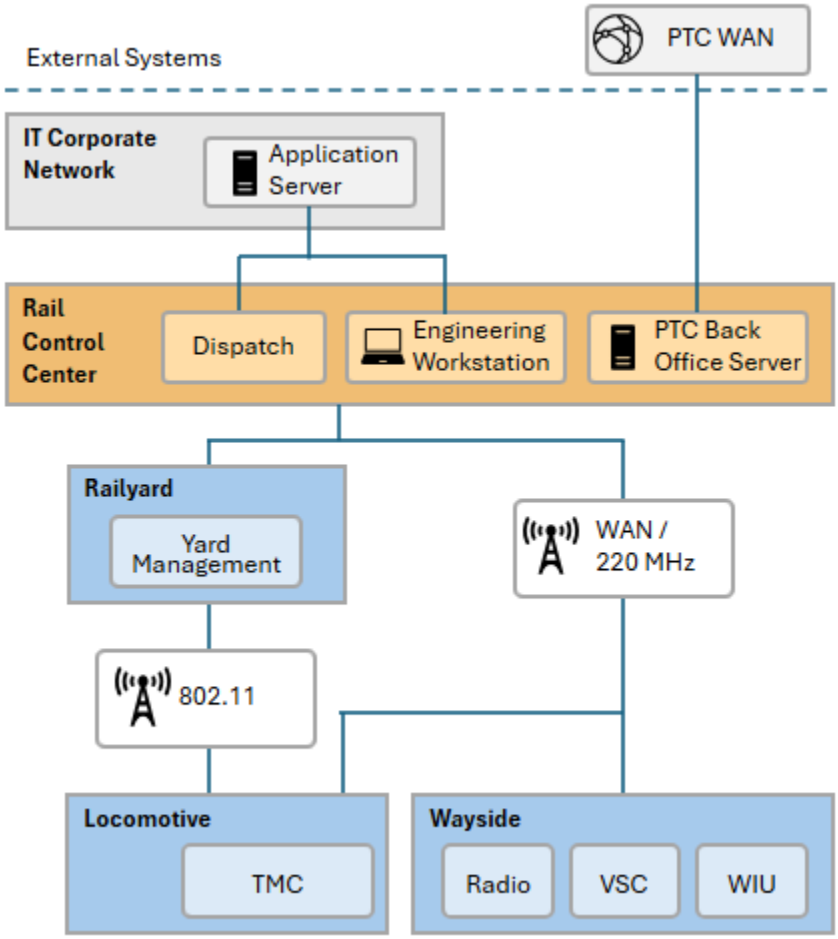

Fig. 11. Example freight rail architecture

2.5.3.1. Architectures and Technologies

An example of a freight railroad architecture is shown in Fig. 11. Railroad control systems depend on multiple components, including:

- **Wayside and switching/signaling systems.** Wayside environments include infrastructure that monitors track state, controls signals and switches, and communicates with locomotives, dispatch, and back-office systems. This can include wayside interface units (WIUs), signal bungalows, switch machines, grade crossing equipment, vital signal controllers (VSCs), and train management computers (TMC).
- **Dispatch and traffic management systems.** Dispatch systems provide centralized visibility and control over train movements, track occupancy, work authorities, and operational restrictions. These systems often integrate with IT-based planning, crew, maintenance, and monitoring systems, making them a critical IT/OT boundary.

- **Locomotives.** Locomotives include onboard control systems, event recorders, PTC controllers, end-of-train (EOT) devices, telemetry systems, and remote diagnostics. EOT devices transmit train-line and rear-of-train statuses to head-end equipment and may support braking functions. Locomotives increasingly maintain connectivity with manufacturers or fleet systems for health monitoring and real-time telemetry.
- **Positive Train Control (PTC) systems.** PTC uses locomotive-mounted units (LMUs), wayside interface units (WIUs), wireless communications, positioning data, and back-office systems to enforce train movement limits and reduce the risk of collisions, overspeed derailments, incursions into work zones, and movement through misaligned switches.
- **Yard and terminal systems.** Railyards and terminals may include yard management systems, scales, inspection portals, gate systems, and local communications networks.

Key properties of freight railroad architectures include:

- **Geographically distributed and remote sites.** Freight railroads include numerous geographically distributed endpoints, such as locomotives, wayside devices, signal bungalows, grade crossings, and communications shelters. This distribution creates dependencies on diverse communications services, including private networks, commercial carriers, and wireless modalities.
- **Use of wireless.** Freight rail devices depend heavily on wireless communications because assets are mobile, transient, and geographically dispersed. Communications to wayside assets and locomotives may rely on cellular, radio, microwave, or other wireless services. PTC also uses 220 MHz radio systems to support interoperable communications among locomotives, wayside devices, and back-office systems.
- **Interconnection with IT and external systems.** Rail OT often exchanges data with enterprise systems for dispatch support, train planning, crew management, maintenance, asset management, customer visibility, cybersecurity monitoring, and regulatory reporting. These integrations create operational value but also introduce IT/OT dependencies that should be segmented, monitored, and governed.

2.5.3.2. Key Cybersecurity Challenges and Recommendations

Cybersecurity challenges and recommendations include:

- **Safety-related and regulated systems.** Many rail systems are safety-critical, including switching, signaling, highway-rail grade crossings, dispatch authority, and PTC. Cybersecurity teams should coordinate relevant decisions with operations, signal, communications, safety, legal, and regulatory personnel.
- **IT/OT interdependencies in dispatch and operations.** Many systems (e.g., dispatch, traffic management, planning, maintenance applications) are critical to rail operations but often depend on enterprise systems and data. Organizations should identify these

dependencies, understand how enterprise disruptions could affect rail operations, and establish response plans that support sustained operations.

- **Dependencies on commercial communications.** Railroads are often highly dependent on external communications services to connect remote sites and assets. Organizations should ensure communications redundancy where needed and develop operating procedures for telecom outages, degraded wireless coverage, or the loss of remote connectivity.
- **Interoperability and shared operational responsibility.** Freight rail operations often involve multiple railroads, shared corridors, tenant operations, and terminal partners. Cybersecurity roles and responsibilities should be documented for shared systems, shared data, incident reporting, and recovery coordination.

2.5.4. Transportation – Maritime/Vessels

Vessels depend on control systems to support safe, environmentally sound, and reliable operations, including navigation, propulsion, steering, and communication needs. A compromise or malfunction of these systems can result in service disruption, casualties (i.e., loss of life), or harm to the marine environment. These systems are typically deployed across the shipboard control network, bridge systems, and various control rooms. Vessels often have a shared cybersecurity responsibility model. Shipyards, OEMs, classification societies, vessel owners, and rotating crews each contribute to the implementation of a cybersecurity program.

2.5.4.1. Architectures and Technologies

An example of a vessel architecture is shown in Fig. 12.

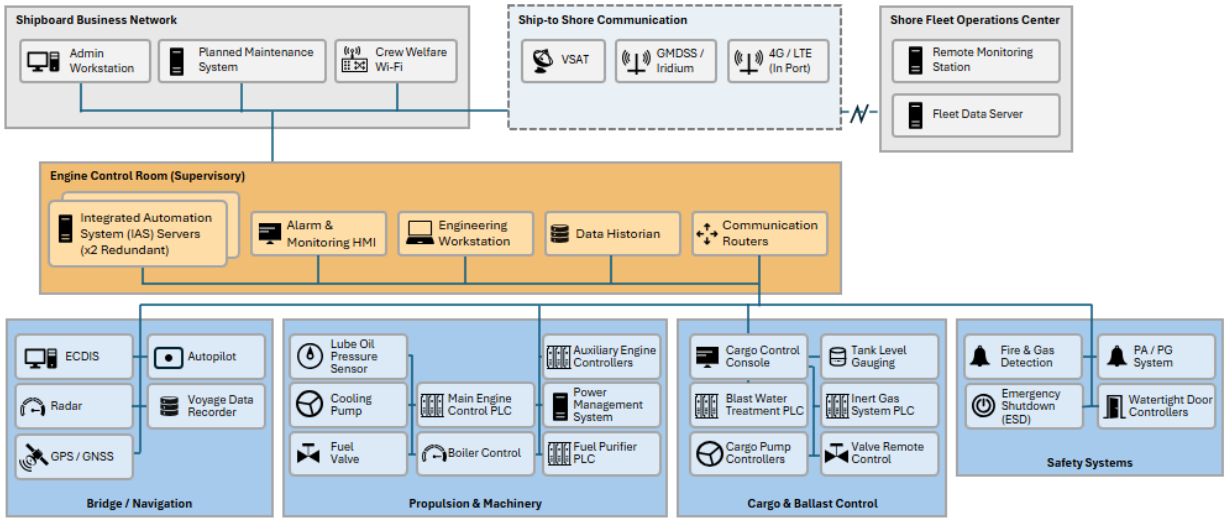

Fig. 12. Maritime cargo vessel example architecture

Vessel control systems have multiple components that are grouped by function into zones, including:

- **Bridge/navigation.** Vessels use a variety of systems to support navigation and avoid collisions. The Automatic Identification System (AIS) is a transponder-based system that displays a vessel's location on Electronic Chart Display and Information Systems (ECDIS). Navigation also relies heavily on GPS/GNSS, radar, and weather data. Vessels must often maintain voyage rata recorders as well.
- **Propulsion and machinery.** Control systems support engine control, cooling, fuel management, boiler control, thruster operations, and power management. These systems are important to maneuverability, safe operation, and the continuity of vessel services.
- **Safety and security.** This includes fire and gas detection systems, watertight door controllers, CCTV, PACS, and alarm systems, including the public address/general alarm (PA/GA). These systems are often critical to the safe operation of the vessel.
- **Cargo, ballast, and power management**. Control systems support cargo handling and monitoring (e.g., loading computers, tank level gauging), ballast water management, and electrical power generation and distribution. These systems directly affect vessel stability, stress limits, and the continuity of electrical services.
- **Engine control room.** This includes systems that are necessary for supervisory control of key OT systems, including automation servers, historians, HMIs, and workstations.
- **Shipboard business network.** Vessels also have networks that support administrative workstations, maintenance systems, passenger support systems, and crew welfare systems.
- **Ship-to-shore communication.** Most vessels require a Global Maritime Distress and Safety System (GMDSS) for ship-to-shore communication, safety, operational requirements, and passenger convenience.

Key characteristics of maritime vessel architectures include:

- **Safety-related systems.** Bridge/navigation, propulsion and machinery, cargo/ballast, power, and safety/security systems directly affect safe operations.
- **Mobile and intermittent connectivity.** Vessels rely on satellite communications while at sea and may use cellular or Wi-Fi when close to shore or in port. Depending on its operational phase (e.g., at sea, dry dock, in port), the vessel can present a different network topology and attack surface.
- **Integrated and shared infrastructure.** Vessels include components from many OEMs or vendors that share access to vessel OT networks. These organizations often need vessel access to perform management roles for these components.

- **Diverse wireless communications.** Ships are heavily dependent on satellite communications; HF, VHF, and UHF Radio to provide communication when at sea; and cellular or Wi-Fi when close to shore.
- **Navigation and specific communications.** Ships depend on multiple communication systems to support navigation functions, including AIS, ECDIS, and GPS/GNSS.
- **Emergency communications.** Ships require emergency communications to be operational in times of distress to provide swift response to maritime incidents, including GMDSS, Distress Radio Beacons, and NAVTEX alerts.
- **Shipboard OT protocols.** Navigation and automation systems commonly communicate using maritime-specific protocols (e.g., NMEA 0183/2000 and IEC 61162-450 Ethernet networks) alongside industrial protocols (e.g., Modbus, CAN bus) in machinery systems, many of which lack native authentication or encryption.

2.5.4.2. Key Cybersecurity Challenges and Recommendations

- **Mixed criticality systems using shared infrastructure.** Vessels have multiple control systems and network segments that perform separate functions with varying criticality but share core communication architectures. Therefore, less critical systems (e.g., crew welfare and passenger systems) should be strongly segmented from more critical systems (e.g., engine control, safety, security).
- **Interfacing with untrusted systems and devices.** Vessels must often communicate with untrusted devices (e.g., ship-to-shore communication systems used at overseas ports). Systems and networks that must interact with untrusted systems should be strongly segmented from critical control systems.
- **Dependency on remote access.** Vessels are often physically inaccessible to maintenance staff since they are primarily at sea. Therefore, vessels require remote access for authorized staff to perform maintenance. OEMs and vendors often require exclusive or privileged remote access to equipment for maintenance purposes, especially during a voyage.
- **Insider threat.** Vessels often have requirements for unfamiliar but high-privilege individuals onboard (e.g., harbor pilots, port captains, superintendents, riding crew, vendor technicians). Vessels may also house diverse populations, especially for cruise and passenger vessels. Therefore, vessels should consider insider threats and develop adequate plans and controls to manage risks, including physical security measures and limited use of removable media (e.g., USB devices).
- **Crew rotation.** Vessel crews rotate on fixed cycles, so personnel responsible for operating and interacting with OT systems change regularly. Rotations introduce credential management challenges. Accounts need to be provisioned/deprovisioned in environments that may lack centralized identity management and use shared accounts. Security awareness and training levels will vary across crews, which can affect

knowledge transfer between rotations. Vessels can enforce role-based access controls that are aligned to shipboard positions and require cybersecurity turnover briefings as part of standard crew change procedures.

- **Fragmented governance.** OEMs often maintain their own systems on board, requiring access from multiple organizations. Additionally, many vessels must operate internationally, but flag states often have their own set of requirements, and vessels must comply with standards across multiple ports, states, or nations. This can result in redundant or conflicting requirements.

2.5.5. Water and Wastewater Systems (WWS)

Water and Wastewater Systems (WWS) use a combination of DCS, SCADA, and PLCs to monitor and control water treatment, distribution networks, wastewater collection, and wastewater treatment operations. These environments are often geographically distributed and include both centralized control facilities and remote stations.

2.5.5.1. Architectures and Technologies

An example of a WWS architecture is shown in Fig. 13.

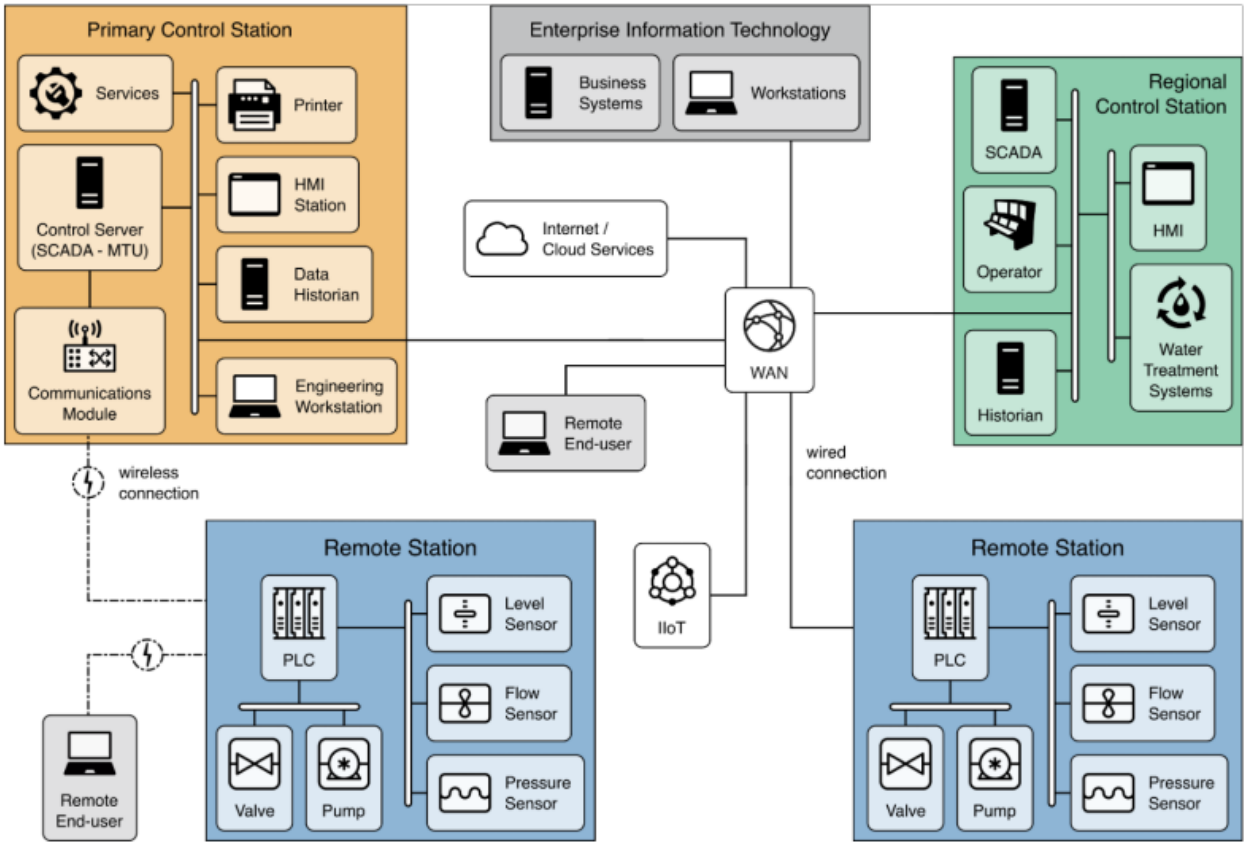

Fig. 13. WWS example architecture [SP1800-45]

WWSs have multiple components, including:

- **Primary control station.** A centralized control station operates water or wastewater treatment plants with remote access to other control stations, remote stations, and business information systems.
- **Regional control station.** Larger utilities may have secondary control stations for monitoring and controlling multiple treatment plants in a service area. OT network infrastructure located in a service area or at localized treatment centers can include servers, SCADA systems, human-machine interfaces (HMIs), and programmable logic controllers (PLCs) with process control data and sensor readings.
- **Remote stations.** Wireless or wired telemetry is used to monitor remote infrastructure (e.g., pump stations, water distribution networks) that feed data back to SCADA servers and operators.
- **Various locations/stations.** PLCs and controls are distributed among the network and pump stations with sensors to enable the logging of metrics, such as pressure, temperature, and physical-chemical characteristics [SP1800-45].

Key properties of WWS architectures include:

- **Safety-related systems.** Many WWS have safety-related systems, especially water treatment systems that perform filtration (e.g., reverse osmosis), chemical feeds (e.g., sodium hypochlorite), or UV purification. Other safety-critical functions include those necessary for testing and reporting on water quality. Cybersecurity teams should coordinate relevant decisions with operations, signal, communications, safety, legal, and regulatory personnel.
- **Geographically remote sites.** Water distribution systems often depend on remote stations, including pump systems, pressure sensors, and telemetry equipment. This creates dependencies on communications infrastructure, such as microwave radio links, leased lines, or cellular modems.

2.5.5.2. Key Cybersecurity Challenges and Recommendations

- **Regulatory requirements for safety and data collection.** WWSs include systems that are critical to water safety and must often report testing results to state agencies. Organizations should understand applicable regulations and ensure that cybersecurity decisions, system architectures, and operational procedures align with those requirements.
- **MSPs for OT management.** Many small organizations depend on managed service providers (MSPs) to manage OT infrastructure. Cybersecurity responsibilities and functions are often not adequately specified in service contracts and, therefore, may not be performed by the utility or the provider. WWS operators should ensure that contracts clearly define the cybersecurity responsibilities, access controls, incident-reporting expectations, and maintenance practices that MSPs must follow.

- **Internet exposure and remote access.** Because WWSs often rely on geographically remote sites and remote access from external MSPs or vendors to manage OT assets, they may require internet-exposed systems or remote-access services. These services can introduce risks if they lack adequate security controls, such as multi-factor authentication, strong credential management, secure configuration, monitoring, and timely patching.

2.6. Comparing OT and IT System Security

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

Initially, OT systems had little resemblance to IT systems because they were isolated and ran proprietary control protocols using specialized hardware and software. Widely available, low-cost Ethernet, Internet Protocol (IP), and wireless devices are now replacing older proprietary technologies, increasing the likelihood of cybersecurity vulnerabilities and incidents. OT systems are increasingly resembling IT systems as they adopt IT technologies to promote enterprise connectivity and remote access capabilities (e.g., using industry-standard computers, OSs, network protocols). This integration supports new IT capabilities but provides significantly less isolation for OT from the outside world than predecessor systems. 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 tailored to the OT environment are needed.

Some special considerations when securing OT include:

- **Timeliness and performance requirements.** OT systems are generally time-critical, and individual installations determine acceptable levels of delay and jitter. Some systems require reliable, deterministic responses. High throughput is typically not essential to OT. In contrast, IT systems typically require high throughput and can withstand some level of delay and jitter. For some OT, automated response times or system responses to human interaction are critical. Many OT systems use real-time operating systems (RTOSs), which refer to timeliness requirements. The units of real time are highly application-dependent and must be explicitly stated.

- **Availability requirements.** Many OT processes are continuous in nature. Unexpected outages of systems that control industrial processes are unacceptable. Outages must often be planned and scheduled days or weeks in advance. Exhaustive pre-deployment testing is essential to ensuring high availability (i.e., reliability). OT systems often cannot be stopped and started without affecting production. In some cases, the products produced or equipment being used are more important than the information being

relayed. Therefore, typical IT strategies (e.g., rebooting a component) are usually not acceptable for OT due to adverse impacts on the requirements for high availability, reliability, and maintainability. Some OT employ redundant components that often run in parallel to provide continuity when primary components are unavailable.

- **Risk management requirements.** For OT, primary concerns include safety, fault tolerance to prevent the loss of life or the endangerment of public health or confidence, regulatory compliance, the loss of equipment, the loss of intellectual property, and 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 can manifest in physical events. Understanding these potential physical effects often requires communication between OT experts and experts in the relevant physical domain.
- **System operation.** OT OSs and control networks often require different skill sets, experience, and levels of expertise than their IT counterparts. Control networks are typically managed by control engineers rather than IT personnel. Assuming that differences are insignificant can have disastrous consequences on system operations.
- **Resource constraints.** OT systems and their RTOSs are often resource-constrained and lack typical contemporary IT security capabilities. Legacy systems often lack the resources common to modern IT systems. Many systems may also lack desired features, including encryption capabilities, error logging, and password protection. The indiscriminate use of IT security practices in OT may cause disruptions to availability and timing. 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 to IT systems, including security patches, are typically applied in a timely manner in accordance with appropriate security policies and procedures. In addition, these procedures are often automated using server-based tools. Software updates on OT cannot always be implemented on a timely basis. These updates need to be thoroughly tested by both the vendor and the end user of the industrial control application before being implemented. Additionally, the OT owner must plan and schedule OT outages days or weeks in advance. The OT may also require revalidation as part of the update process. Another issue is that many OT systems utilize older versions of OSs that are no longer supported by the vendor through patches.

Change management is also applicable to hardware and firmware. The change management process requires careful assessment by OT experts (e.g., control engineers) working in conjunction with security and IT personnel.

- **Managed support.** Typical IT systems support diverse support styles that span disparate but interconnected technology architectures. For OT, service support is sometimes only available from a single vendor. In some instances, third-party security solutions are not allowed due to OT vendor licensing and service agreements, and service support can be lost if third-party applications are installed without vendor acknowledgment or approval.
- **Component lifetime.** Typical IT components have a lifespan of three to five years due to rapid technological evolution. For OT, where technology has often been developed for specific uses and implementations, the lifetime of the deployed technology may be in the order of 10 to 15 years and sometimes longer.
- **Component location.** Most IT components and some OT components are located in business and commercial facilities that are physically accessible by local transportation. Remote locations may be utilized for backup facilities. Distributed OT components may be isolated, remote, and require extensive transportation effort to reach. The component location must also account for the necessary physical and environmental security measures.

Table 3. Summary of typical differences between IT and OT systems

Category	Information Technology	Operational Technology
Performance Requirements	• Non-real time. • Response must be consistent. • High throughput is demanded. • High delay and jitter may be acceptable. • Emergency interaction is less critical. • Tightly restricted access control can be implemented to the degree necessary for security.	• Real time. • Response is time-critical. • Modest throughput is acceptable. • High delay and/or jitter is unacceptable. • Response to human and other emergency interaction is critical. • Access to OT should be strictly controlled but should not hamper or interfere with human-machine interaction.
Availability (Reliability) Requirements	• Responses (e.g., rebooting) are acceptable. • Availability deficiencies can often be tolerated, depending on the system's operational requirements.	• Responses (e.g., rebooting) may not be acceptable because of process availability requirements. • Availability requirements may necessitate redundant systems. • Outages must be planned and scheduled days or weeks in advance. • High availability requires exhaustive pre-deployment testing.
Risk Management Requirements	• Manage data. • Data confidentiality and integrity is paramount.	• Control the physical world. • Human safety is paramount, followed by protection of the process.

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

In summary, the operational and risk differences between IT and OT systems require greater 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 potential implications of installing, operating, and maintaining security solutions alongside control system operations. IT professionals working with OT need to understand the reliability impacts of information security technologies before deployment. Moreover, some OSs and applications running on OT may not operate correctly with commercial-off-the-shelf (COTS) IT cybersecurity solutions due to their unique requirements.

3. OT Risk Management and Governance (CSF 2.0 – GOVERN)

This section describes the development and outcomes of an OT cybersecurity program and governance structure for new and deployed OT systems as well as OT-specific considerations. The organization should apply its own organizational processes to develop workflows for establishing, implementing, and reviewing programs.

To establish an effective OT cybersecurity governance capability, develop a process and assign responsibilities and accountability to appropriate roles in the enterprise risk management function. A cybersecurity governance process should include the following:

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

At a high level, OT governance should include the policies, procedures, and processes for managing the organization's regulatory, legal, risk, environmental, and operational requirements. Governance should ensure that the policies, procedures, and processes are well-understood by staff and inform the management of OT cybersecurity risk.

Organizations come in various sizes, structures, geographical spreads, and levels of complexity. These factors, along with strategies related to resource and budget constraints, may drive organizations to hire OT cybersecurity resources as employees or contractors or to outsource the OT security operations function as a managed security service. Regardless of the security operation and resource model used, the responsibility for OT cybersecurity management should be integrated with IT cybersecurity and the enterprise risk management function. In addition, although the following sections are described separately, they often occur in an iterative process or in different sequences, depending on the organizational approach.

Additional information and specific examples for establishing a cybersecurity governance capability are also provided in NIST Interagency Report (NIST IR) 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A].

3.1. Organizational Context and Shared Governance (GV.OC and GV.RR)

The following describes how organizations should align OT cybersecurity risk management with enterprise risk management (ERM) and define the collaborative roles needed to govern risk effectively and support the broader mission. Because OT cybersecurity events can affect safety, operations, regulatory compliance, the environment, and business performance, OT risk should not be managed as a stand-alone technical issue but as part of the organization's broader risk management processes.

Achieving this requires a shared governance structure that brings together senior leadership, OT, IT, safety, legal, operations, and other relevant stakeholders to establish program scope, assign responsibilities and decision-making authority, and coordinate day-to-day cybersecurity activities. Through this organizational context and shared governance model, organizations can ensure that OT cybersecurity decisions are informed by both enterprise priorities, risk tolerances and operational realities.

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

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

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

A charter for a cybersecurity program is a plain-language high-level description that establishes clear ownership and accountability, including for protecting OT resources and provides a mandate for the most senior person responsible to establish and maintain the cybersecurity program (e.g., the CISO).

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 the appropriate authority to lead the program. The OT cybersecurity manager should define the roles and responsibilities of system owners, mission and business process managers, and users. The OT cybersecurity manager should also document the objectives and scope of the OT security program, including the affected business organizations, 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 are specific to the OT system. Ultimately, it will be more effective for the team to share resources with others in the organization that have similar objectives.

3.1.1. Building an OT Cybersecurity Business Case

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

- **Physical impacts.** Physical impacts encompass the set of direct consequences of OT failure, particularly personal and public health and safety. Other effects include the loss of property (including data) and potential damage to the environment.
- **Economic impacts.** Economic impacts are a second-order effect of the physical impacts that ensue from an OT incident, which in turn cause greater economic losses to the facility, organization, or others who depend on the OT systems. The unavailability of critical infrastructure (e.g., electrical power, transportation) can have economic impacts far beyond the systems that sustain direct and physical damage. These effects could negatively impact the local, regional, national, or possibly global economy.
- **Social impacts.** Another second-order effect is the loss of national or public confidence in an organization.

The potential consequences of an OT incident also include the following intersecting examples:

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

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

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

- Potential costs and failure scenarios if an OT cybersecurity program is not implemented
- High-level overview of the process, costs, and resources required to implement, operate, monitor, review, maintain, and improve the information security program
- Opportunities to improve efficiencies by coordinating and aligning with existing governance structures and security programs (e.g., enterprise, IT)

The economic benefits of the cybersecurity program may be evaluated in the same way as worker health and safety programs. However, an attack on the OT system could have significant consequences that far exceed monetary costs.

3.1.2. Presenting the OT Cybersecurity Business Case to Leadership

Organization-level management in both IT and OT operations has the perspective to understand 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 program's security vulnerabilities and needs are better understood and additional strategies are developed.

Often, a good approach to obtaining management buy-in is to build the business case on a successful example of how another organization solved a similar problem. This often prompts management to ask how that solution might apply to their organization.

3.1.3. Aligning OT Cybersecurity With the Enterprise Mission (GV.OC)

OT cybersecurity should be guided by the organization's mission, business objectives, and broader ERM strategy. OT risk management should not be treated as an isolated technical activity. Rather, it should support the organization's ability to safely and reliably carry out its core functions, such as producing goods, generating energy, or delivering essential services. Establishing this organizational context helps define the scope of the OT cybersecurity program, identify relevant internal and external stakeholders, clarify dependencies, and ensure that OT cybersecurity decisions are aligned with operational, regulatory, mission, and business priorities.

The organizational context should define the scope of the OT security programs, especially the alignment of responsibilities and coordination with closely related programs, including IT, physical security, legal, safety, operations, and procurement. The context must also clearly define the external stakeholders, including regulators, suppliers, contractors, and service providers. It should have a clearly defined mission, involve all relevant stakeholders, maintain awareness of requirements (e.g., regulatory, contractual), define and achieve objectives, and address organizational dependencies.

3.1.3.1. Understanding Operational Consequences and Requirements

Organizations must understand the possible negative consequences that an OT cybersecurity event could cause and what organizational requirements could be impacted. OT organizations are often required to perform a hazard analysis to demonstrate that associated risks are adequately managed. These processes should account for the possibility that OT security incidents could influence or contribute to these harms. The organization should ensure that the cybersecurity decisions are informed by the analysis. Relevant approaches include Cyber-Informed Engineering [CIE] and Cyber PHAs.

3.1.4. Navigating the Regulatory and Compliance Landscape (GV.OC)

The legal, regulatory, and compliance landscape shapes the governance of OT cybersecurity risk. In addition to managing technical and operational risk, organizations should understand and account for the administrative, reporting, safety, health, environmental, and sector-specific obligations that apply to their OT environments. These requirements should be incorporated into the organizational context, risk management processes, and cybersecurity program so that OT cybersecurity decisions support not only safe and reliable operations but also compliance with applicable laws, regulations, and contractual obligations. Appendix D provides examples of cybersecurity regulations and directives applicable to critical infrastructure sectors.

The programs should ensure that they align with all necessary requirements across the regulatory, safety, health, and environmental landscape. Regulated industries must consider cyber-related regulatory requirements when designing their cybersecurity architecture. Organizations should also ensure that their compliance program helps prevent business decisions and system operations from unduly generating environmental hazards (e.g., waste). Substantial hazards may lead to non-compliance, fines, or injury.

3.1.5. Defining Shared Roles, Responsibilities, and Authorities (GV.RR)

This section addresses the human and organizational aspects of OT cybersecurity by defining shared roles, responsibilities, and decision-making authorities across IT, OT, and business leadership. It should clarify who owns OT cybersecurity risk, who has the authority to approve changes to operational systems, and how cross-functional teams coordinate enterprise cybersecurity priorities with operational requirements. Governance should also address boundary technologies (e.g., firewalls, data diodes) so that ownership, administration, and

monitoring responsibilities are clearly assigned, and the use of these devices does not create unmanaged "shadow OT" functions or communication gaps between IT and OT teams. This governance should not only account for operational data that crosses IT/OT boundaries, but also for cybersecurity telemetry, alerts, and logs generated by devices and monitoring systems within the OT environment.

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

While control engineers will play a large role in securing OT, they cannot 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.

The responsibilities and authorities of each member of the cybersecurity team and peer groups must also be defined. Examples of key authorities that must be clearly defined include:

- Ownership of systems and networks, including areas of shared responsibility (e.g., between IT and OT) and boundary devices (e.g., firewalls, data diodes)
- The avoidance, acceptance, transfer, and mitigation of identified risks within the OT environment
- The approval of change management issues, including decisions to patch an OT system
- Access management changes, including the approval of access by both the organization and third parties.
- Support during incident response, including the changes in OT operational mode, recovery changes, and third-party communication and engagement
- Responsibilities for investing in the cybersecurity program and making decisions regarding additional investments
- The responsibilities for third-party providers, which can include service providers, contractors, and other organizations that provide OT system development and services and security operation and management

Supplemental guidance for establishing a cross-functional team can be found in the following documents IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide*.

3.2. Defining the OT Risk Management Strategy (GV.RM)

This section describes how organizations should define an OT risk management strategy that aligns with enterprise risk management while reflecting the unique characteristics and constraints of OT environments. This strategy should establish how OT cybersecurity risks are prioritized, evaluated, tracked, reported, and addressed in a manner consistent with the organization's mission, operational requirements, and risk tolerance. Because OT risk decisions can affect safety, system availability, production, and the environment, the risk management approach should be tailored to the organization's operating context and integrated with the broader governance processes established in Sec. 3.1 and the risk assessment activities described in Sec. 4.1.3.

Organizations should tailor a risk management approach that performs best based on their operating context. A general approach for ERM is defined in IR 8286 and shown in Fig. 14.

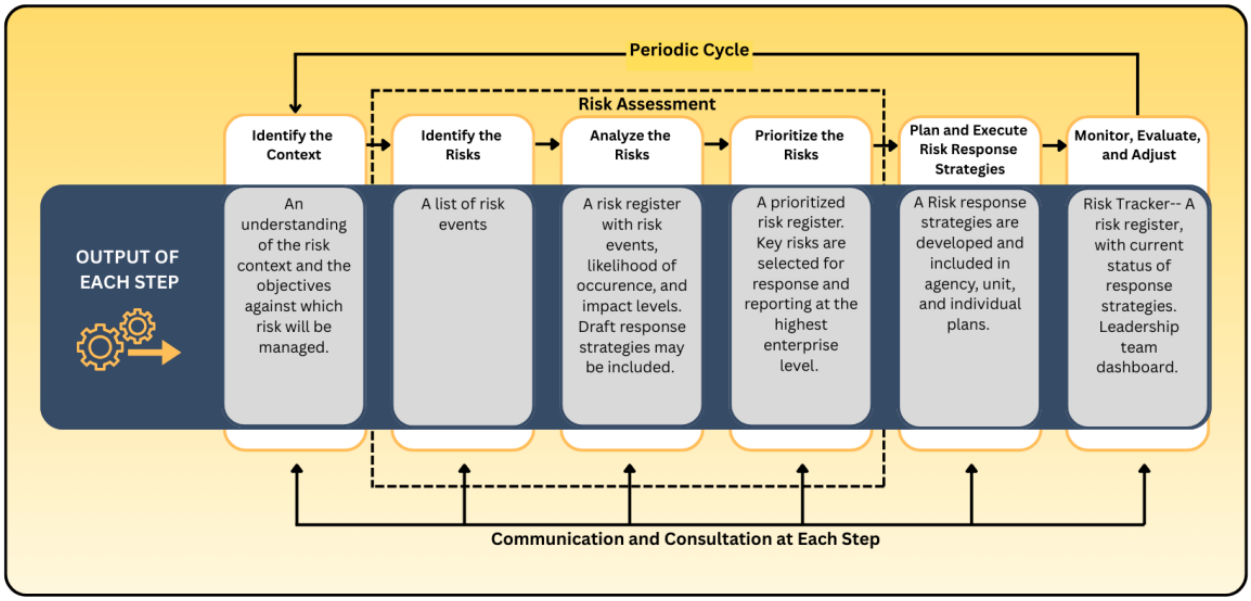

Fig. 14. Risk management life cycle

OT organizations should tailor this process to align with their existing processes for managing both business and operational risks. Additional guidance on how OT environments can align with the RMF are included in Appendix F.

There are multiple factors to consider when applying risk management to OT systems, including:

- **Safety.** It is the organization's greatest responsibility to ensure that each risk response is ultimately a decision that makes the workplace safer. Risks to safety are generally unacceptable and must be treated accordingly.
- **Operational impact.** Risk response options that require a mission-critical system to be taken offline may not be feasible. The organization should consider the criticality of

production assets and their continued operation before approving any action that would require downtime and potential cascading impact to other organizations.

The risk management process must align with other elements of cybersecurity programs, including key steps in governance, especially the defined Organizational Context (GV.OC), and the process of performing a risk assessment to identify risks and assess their severity and likelihood (ID.RA). Risk management should focus on how these risks are prioritized and reported, the decisions made to address them, and how they will be tracked and monitored.

3.2.1. Maintaining a Risk Register

Once risks are enumerated, they must be recorded and reported. Organizations should maintain a risk register with sufficient information to both make informed risk management decisions and inform stakeholders and interested parties. Criteria to include for each risk is included in Table 4.

Table 4. Risk register entry criteria

Register Criteria	Description
Priority	An ordinal or scaled indicator of the risk criticality relative to others (e.g., low, moderate, high, critical).
Risk Description	A summary of the risk scenario.
Risk Category	The high-level classification of the risk (e.g., Operational, Strategic, Compliance, Financial).
Estimated Likelihood	A qualitative measure (e.g., low, moderate, imminent) of the likelihood of occurrence.
Estimated Impact	A qualitative measure (e.g., low, moderate, high, critical) of how grave the associated consequences would be if the risk manifested.
Impact Categories	A list of potential business functions impacted by the risk (e.g., financial, health, safety, and environmental [HSE]; mission) and a description of how the impact would manifest.
Combined Exposure Rating	A measure (e.g., low, moderate, high, critical) of the total associated risk based on likelihood and impact in accordance with the matrix in use.
Chosen Risk Response	A concise narrative of the selected response strategy (e.g., mitigate, transfer, accept, avoid).
Risk Owner	The person or team responsible for managing and monitoring the risk and chosen risk response. This risk owner is also responsible for communicating the implications of their risk(s) to the ERM team.
Status	The current condition of the risk (e.g., Open, In-Progress, Closed) and information on next steps.

Figure 15 shows an example of the structure of a risk register using a risk associated with a SCADA vulnerability.

ID	Priority	Description	Category	Likelihood	Impact	Exposure	Categories	Response	Owner	Status
1	Medium	SCADA server vulnerability	Operational	Low	High	Medium	Operational – line cannot operate without server	Mitigate	P. Manager	Open

Fig. 15. Risk register example

In this example, the team receives an alert from the vendor indicating a vulnerability in the SCADA server software. They have created a patch to fix the vulnerability, but it requires a reboot. Since this server has no redundancy and cannot fail over, it cannot be rebooted while the plant is at peak operation, as a forced outage is unacceptable.

3.2.2. Risk Response

Once a risk has been identified and incorporated into the register, the organization must decide how to respond to it. Risk responses can be performed in many ways, including:

- **Mitigate.** The organization may choose to deploy a security control to mitigate that risk or make a change to the system (e.g., a patch). For risks where the organization decides mitigation is the best response, controls must be selected and subsequently implemented. For more information on the selection and implementation of security controls and other mechanisms, see Sec. 4.
- **Transfer.** The risk can be transferred to another business unit or organization. This can include purchasing cybersecurity insurance or establishing contractual clauses with third parties to define their liability for this risk.
- **Accept.** In many cases, OT organizations are constrained in their ability to either mitigate or transfer risks. This is often due to the inability to modify operational systems or to address vulnerabilities in critical components. In these cases, the organization may decide that the risk and associated consequences are within acceptable tolerances. Risk acceptance must be formally approved by the designated risk owner or governance team and documented accordingly.
- **Avoid.** Apply responses to ensure that the risk does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing the cybersecurity risk to an acceptable level. The cost of the lost opportunity associated with such a decision should be considered as well.

After risk response, the organization must estimate the residual risk to continually inform its overall risk environment. A key consideration, among others, is how to keep residual risk within the organization's defined risk appetite and risk tolerance.

Supplemental guidance for Risk Management can be found in IR 8286.

3.2.3. OT Risk Management Life Cycle

OT risk management should be implemented as a continuous life cycle rather than as a one-time assessment or compliance exercise. In OT environments, risk decisions should account for safety, reliability, environmental, regulatory, and mission impacts and should be revisited as systems, threats, and operating conditions change. Building on the strategy described in Sec. 3.2, this life cycle connects the organizational context and risk management approach established in Sec. 3.1 with the practical activities of framing risk, categorizing systems, selecting and tracking risk responses, applying compensating controls when necessary, planning transitions to more durable solutions, and continuously monitoring whether residual risk remains within defined tolerances.

The OT risk management life cycle should function as an iterative process that reflects OT-specific operational consequences. It links risk framing, system categorization, risk response, transition planning, compensating controls, and continuous monitoring in a manner that supports safe and reliable operations. Compensating controls should be treated as temporary measures rather than permanent substitutes for remediation. Organizations should maintain clear visibility into these temporary conditions and tie them to funded upgrade or remediation plans since adversaries may exploit such gaps when targeting the environment.

Risk management should be guided by the organizational context, roles, responsibilities, and risk tolerances established in Sec. 3.1 and 3.2. These elements define the assumptions, constraints, priorities, and risk tolerance that shape OT cybersecurity decisions. System categorization then translates those priorities into an understanding of system criticality, operational dependencies, and potential consequences.

Once risks are framed and systems are categorized, the organization selects an appropriate risk response consistent with Sec. 3.2.2. Where feasible, risks should be mitigated through engineering changes (e.g., architecture improvements, segmentation, secure configuration, access control, monitoring, patching, replacement of vulnerable components). However, OT environments often include legacy systems, unsupported components, proprietary protocols, fragile integrations, and limited maintenance windows that prevent immediate remediation. In these cases, compensating controls may be used to reduce exposure while maintaining safe and reliable operations.

Compensating controls may not always fully address the associated risk and may need to be treated as temporary mitigations rather than permanent substitutes for correcting the underlying weakness. Examples include additional segmentation, restricted remote access, enhanced logging, manual verification steps, additional jump host controls and monitoring, application allowlisting, increased operator awareness, vendor access supervision, and out-of-band monitoring. Each compensating control should be tied to a specific risk, a residual risk rating, an accountable owner, a review date, and a retirement condition. The risk register described in Sec. 3.2.1 should capture this information.

Transition planning is the mechanism that prevents compensating controls from becoming risk acceptance by default. When the preferred mitigation is not immediately feasible, the organization should establish a funded path to a durable solution. The transition plan should

identify the target-state control or architecture, required budget, procurement dependencies, maintenance-window requirements, engineering design work, vendor support, testing and validation activities, implementation milestones, and accountable owner. This ties temporary mitigation decisions to capital planning, outage planning, procurement, and life cycle management.

The OT risk management life cycle operates as a continuous loop: frame risk in terms of mission and operational consequences; categorize systems by criticality and physical impact; select risk responses appropriate to OT constraints; apply compensating controls only when necessary; establish funded transition plans to durable risk reduction; and continuously monitor whether residual risk remains within tolerance.

3.3. Cybersecurity Supply Chain Risk Management (GV.SC)

Organizations should manage cybersecurity supply chain risks arising from products, services, suppliers, and third parties that support OT environments. Because OT systems often depend on specialized equipment, limited supplier options, vendor-maintained services, and remote access by external parties, supply chain risks can directly affect the availability, integrity, and confidentiality of OT systems and data with possible consequences ranging from operational disruption to safety impacts. To address these risks, organizations should incorporate C-SCRM into their broader governance, procurement, and life cycle management practices, including identifying critical suppliers, defining required supplier security practices, and managing supplier and product risk throughout the system life cycle.

Supply chain risks can include the insertion of counterfeits, unauthorized production, malicious insiders, tampering, theft, the insertion of malicious software and hardware, and poor manufacturing and development practices across the products or services acquired to support OT needs. Whether they are malicious, natural, or unintentional, these risks have the potential to compromise the availability and integrity of critical OT systems and components as well as the availability, integrity, and confidentiality of the data utilized by the OT, thereby causing harms that range from minor disruptions to impacts on life and safety. OT organizations have key challenges with managing supply chain risks, including:

- Organizations often have sector-specific equipment requirements and depend on a smaller number of key suppliers. Therefore, organizations may be required to decide whether to accept or manage the risk posed by suppliers that do not meet organizational requirements.
- Many suppliers may require remote access to the OT environment, including MSPs that need remote access to OT networks or vendors that require access to data from their equipment within the OT network.
- OT environments must often integrate new equipment or systems that consist of many diverse digital devices (e.g., cranes, electric transformers, water treatment systems). The organization must track and validate the supply chain risk of that equipment and all associated digital components.

Identifying, assessing, and effectively responding to cybersecurity risks in supply chains is best accomplished by incorporating C-SCRM considerations into organizational policies, plans, and practices.

3.3.1. Identifying and Vetting Key Suppliers and Supplies

The organization must develop and maintain a process to prioritize suppliers according to their criticality to the mission, operations, and security of its systems. This means evaluating which suppliers, service providers, and components are most essential to maintaining safe and reliable operations. This should include embedded components, ICS firmware, and maintenance services.

The organization should first clearly define criteria for criticality. This may include the third party's role in sustaining normal operations (e.g., the extent to which they drive business outcomes), their role in safety functions, their level of access to organizational OT networks, and their influence on the confidentiality, integrity, or availability of systems.

Organizations should also consider whether OT is purchased directly from the original equipment manufacturer (OEM) or an authorized third-party distributor or reseller. Suppliers should be assessed or reviewed to ensure that they continue to follow best practices.

3.3.2. Defining Required Practices of Suppliers

Organizations should define the required processes, technical mitigations, and evidence expected from a supplier of any OT component. This can include:

1. Criteria for secure software development and life cycle management
2. Service level agreements (SLAs) that document the supplier's approach to the notification and resolution of vulnerabilities
3. Defined maintenance and support agreements to determine acceptable methods for vendor remote access (if necessary), SLAs for issue resolution and incident response (if applicable), and obligate the third party to comply with the organization's access control procedures when on-site
4. Technical mechanisms regarding the hardware and software components within the products, such as through HBOMs and SBOMs
5. Digital artifacts to validate the authenticity of vendor-provided OT hardware, software, and firmware, such as digital signatures
6. Clear incentive structures in supplier contracts to encourage and reward strong security practices

3.3.3. Identifying and Managing Supply Chain Risk Across Product Life Cycles

Organizations must manage supply chain risks across the product life cycle. This should include documented processes to validate the authenticity and integrity of products, control supplier access, and assess supplier and product risks. Using these processes, organizations should vet suppliers and service providers to ascertain their capabilities, trustworthiness, the adequacy of their internal security practices, the effectiveness of their safeguards, their supply chain relationships, and any risks that may be associated with those relationships and dependencies.

Examples of key checks that the organization should validate include:

- Whether the products include any unauthorized components, software, suppliers, or regions for all acquisitions
- Remote access and on-site management requirements and mechanisms to audit and control access
- The existence of unauthorized communication devices (e.g., cellular modems)

Additionally, special consideration should be given to how difficult it may be to obtain 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.

Supplemental guidance for supply chain risk management can be found in the following documents:

- SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- IR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*
- CISA Software Acquisition Guide Fact Sheet
- CISA Software Bill of Materials (SBOM)
- CISA A Hardware Bill of Materials Framework for Supply Chain Risk Management Fact Sheet

3.4. OT Security Policy and Oversight (GV.PO)

Organizational leadership should develop and disseminate policies that establish security requirements for their environments. These policies may include the identification and assignment of roles, responsibilities, management commitment, and compliance. The policies may also reflect coordination among the organizational entities responsible for the different aspects of security (e.g., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring).

Where possible, OT-specific security policies and procedures should be compatible and coordinated with other groups and existing policies and procedures throughout the organization. This includes coordination with IT management, human resources, and

organizational governance teams. Examples of where policy coordination is necessary across groups include:

- **IT:** When IT infrastructure is used to provide user access to OT infrastructure or protect OT data along with processes to investigate and respond to security incidents that potentially span both OT and IT networks
- **Human resources:** The investigation or remediation of security issues regarding organizational personnel
- **Organization governance:** The incorporation of necessary regulatory requirements, decision authorities, and reporting to facilitate awareness

The development of cybersecurity policies should be based on a risk assessment that will set the security priorities and goals for the organization. Procedures that support the policies should be developed so that the policies are implemented fully and properly for OT. Cybersecurity procedures should also be documented, tested, and updated periodically in response to changes in policy, technology, and threats.

Supplemental guidance for cybersecurity policy can be found in the following documents:

- SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- SP 800-37r2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- SP 800-100, *Information Security Handbook: A Guide for Managers*
- IR 8286r1, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8183Av2, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide*

3.4.1. Program Performance Measurement

The OT cybersecurity program should be continually observed to determine its overall effectiveness. This may include evaluating the current charter and related policies to determine whether they remain the most appropriate components.

The organization should define both key performance indicators (KPIs) and key risk indicators (KRIs), analyzing them over time to gauge the program's performance and the organization's risk posture. While KPIs are quantitative measures of the program's operational efficiency, KRIs may result from shortcomings in the governance program.

Examples of KPIs include:

- Percentage of OT assets with applied system hardening
- Mean time to detect incidents (MTTD)
- Mean time to respond to incidents (MTTR)

- Percentage of security policies reviewed and reapproved in the past 12 months
- Personnel security awareness training completion rate
- Percentage of personnel who reported phishing simulations

Examples of KRIs include:

- Percentage of production assets deemed end-of-service (EOS) or end-of-life (EOL) by vendors
- Percentage of personnel who have not completed security awareness training
- Percentage of personnel who failed phishing simulations
- Number of open, critical vulnerabilities yet to be remediated

The organization should define KPI targets and KRI thresholds to better manage the program throughout its life cycle. While a KPI target is a numerical value that the organization hopes to meet or exceed (e.g., 90 % of OT assets are hardened), a KRI threshold is an expression of the maximum numerical value before risk is deemed unacceptable (e.g., no more than 5 % of staff should have missed or failed their security awareness training).

3.4.2. Organizational Oversight

Organizations must establish oversight capabilities and teams to monitor risk management activities and make necessary decisions, investments, and strategies. These teams should help review key artifacts and indicators from the risk management process, including incidents, vulnerabilities, audit findings, and assessments to track the status of the security program.

An organization-wide risk management strategy is foundational to developing an OT cybersecurity strategy.[5] The OT cybersecurity strategy leverages the organization-wide risk management strategy — including organization-defined risk tolerance, threats, assumptions, constraints, priorities, and trade-offs — to further tailor the strategy to apply to the OT cybersecurity program. By consciously choosing to develop and implement a cybersecurity strategy, an organization establishes a disciplined approach that considers all aspects of the system life cycle, from procurement to decommissioning, with cybersecurity in mind. As a result, the organization can ensure that cybersecurity goals are realized in its systems. The adoption of a cybersecurity strategy can result in a more systematic implementation of risk decisions into system development and operation. Decisions on cybersecurity strategy should flow from a high-level understanding of the organization's operations, objectives, and cybersecurity goals. A comprehensive and accepted cybersecurity strategy can assist an organization with consistently maintaining acceptable risk management throughout the life cycle of an OT system.

The OT cybersecurity strategy should:

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

- Refine the OT operation's organizational risk tolerance, which drives the OT cybersecurity operation's priorities
- Refine and supplement guidance from the organization-wide risk management strategy to address OT-specific constraints and requirements
- Identify the OT cybersecurity team and personnel and the associated OT-specific cybersecurity training and awareness necessary
- Address the OT cybersecurity operation model (e.g., insource, outsource, use managed security services)
- Outline the appropriate cybersecurity architecture for the various OT sites within the OT program.
- Address both IT and OT concerns and requirements; while IT may prioritize data loss or system availability, OT may prioritize system safety, production efficiency, and environmental protection
- Incorporate critical infrastructure standards and regulatory requirements, which are typically designed to protect critical cyber assets to support reliability and may carry additional legal obligations for the organization
- State the need for sound cybersecurity practices, such as patching or monitoring

The strategy should provide guidance on how the organization will make key cybersecurity decisions, including:

- Architectural decisions informed by a cybersecurity to increase the likelihood that high-level cybersecurity goals will be reflected in the cybersecurity of individual systems, including the approach to securing integration with other networks and systems (e.g., business networks, cloud, IIoT technologies)
- The management of OT systems across the life cycle, including the approach to addressing products that pass end-of-life status or have identified cybersecurity or supply chain concerns
- The required approval, evaluation, or restrictions necessary to inform the adoption and use of new technologies (e.g., crypto agility, artificial intelligence [AI], and machine learning [ML] technologies, digital twins)
- Data governance issues, especially those associated with data hosted on IT environments, and any third parties (e.g., contractors, integrators)

Supplemental guidance for establishing an OT cybersecurity strategy can be found in IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide*.

3.5. OT Cybersecurity Awareness and Training (PR.AT)

This section addresses governance and workforce considerations for OT cybersecurity awareness and training with a particular focus on preparing personnel to carry out their security-related responsibilities in OT environments. Because human actions can directly affect the safety, reliability, and security of OT systems, organizations should incorporate cybersecurity into personnel security practices, access management processes, and role-based training programs. This includes coordinating with human resources, IT, physical security, and OT leadership to ensure that personnel in critical roles are appropriately screened, trained, and authorized and that they maintain the knowledge needed to recognize and respond to cybersecurity issues relevant to their job functions.

A general personnel security program should address policy, position risk designations, personnel screening, terminations, transfers, access agreements, and third-party roles and responsibilities. OT personnel should communicate with human resources, IT, and physical security to ensure that personnel security requirements are being met. Cybersecurity should also be included in human resources practices to reduce the risk of human error, theft, fraud, or other intentional or unintentional misuse of information systems.

Organizations should consider establishing an access agreement and request form to manage physical and/or logical access to OT equipment. Organizations should also screen the personnel assigned to critical positions who control and maintain the OT. Additionally, each employee should receive training that is relevant to and necessary for their job functions. Organizations should require personnel to 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.

Supplemental guidance on personnel security controls can be found in the following documents:

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

4. OT Cybersecurity Outcomes and Objectives (CSF 2.0 – ID, PR, DE, RS, RC)

4.1. Identify (ID)

This section discusses the unique opportunities and challenges of identifying assets and risks within an OT environment. It will first explore the asset management category, which is critical to ensuring that an organization broadly understands its assets and their functions. It will then discuss the risk assessment process to understand the resulting risks in the OT environment.

4.1.1. Asset Management (ID.AM)

Asset management depends on understanding individual assets, their architecture, data flows, and associated operational functions. Accurate inventory information supports multiple risk management objectives, including risk assessment, vulnerability management, and obsolescence tracking. Asset inventories are also critical to supporting other security functions, including detection and response/recovery.

This section will explore key challenges and recommendations for establishing an asset inventory. While asset management also encompasses the security configuration and maintenance associated with assets, the discussion of these topics is included in Sec. 4.2.3.

4.1.1.1. Establishing an Asset Inventory

An accurate asset inventory is the foundation of an asset management program. Organizations need to maintain a process to identify all of their assets and understand key information and configurations for those assets, their communication needs, functions, and their criticality to the overall process. Organizations should consider including the following to support their asset management capability:

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

Additionally, updating inventory information when components are added, removed, or changed (e.g., patched, new firmware installed, component swapped during maintenance) helps organizations accurately manage their overall environmental risks. Establishing an asset inventory typically depends on a combination of automated tools that continually discover changes in the environment along with manual processes to validate the completeness and accuracy of the collected data. Various tools are available to support automated discovery and the collection of asset data. While automated tools provide many benefits for maintaining an updated inventory, organizations should consider how the tool collects information and whether the collection method (e.g., active scanning) may negatively impact their OT systems.

While each approach has some benefits, there are also challenges associated with each, such as:

- **Vendor management tools.** Many vendors provide engineering tools to discover devices and manage configurations. These often use vendor-provided dedicated network services and are usually designed primarily for operational functionality rather than security. Vendor management tools may have access to very detailed information about devices (e.g., configurations, model and serial numbers, firmware versions), which feed directly into an asset inventory. One drawback is that these tools typically work with a single vendor's product line and cannot read information from other vendors' products. The asset owner must then maintain multiple vendor tools if they want to incorporate all of the information into an inventory, and there is no guarantee that each tool will consistently provide that information.
- **Passive network monitoring.** Passive network monitoring tools are often designed to monitor networks for cybersecurity threats. As part of this process, they also provide the ability to identify assets based on passively monitoring and analyzing network traffic to discern identifying information about devices. As these tools listen to more network traffic, they build a broader and more extensive database of assets and network data flows. These tools can be valuable for identifying all devices communicating on the network, not just the ones that are known. However, the tools are highly dependent on the placement of the listening sensors. Unlike typical IT designs, it is not uncommon for large amounts of communication in an OT network to be isolated to a single switch buried within the architecture, where a listening sensor would not detect them. Asset owners need to evaluate their network architecture to determine the optimal placement of listening sensors to avoid gaps.
- **OT-aware network scanning.** Some network scanning tools, whether specifically designed for asset management or security monitoring, can interrogate devices for identifying information using native OT protocols. These tools act in similar ways to vendor management tools by using the native capabilities of the OT devices to report configuration information, model and serial numbers, or firmware versions. These tools may be able to gather information from multi-vendor, multi-protocol environments, potentially reducing the number of tools that an asset owner needs to manage. Asset owners may want to consult with their vendors and should perform testing before implementing them in the production environment.

- **Independent active network scanning.** These tools establish network connections to various services on network devices to identify device profiles without using the native OT protocols. They perform more independent, extensive scans of devices to interrogate all available resources, sometimes requiring credentials to fully collect the information. These types of tools may be designed more for compliance or vulnerability management rather than just asset management. These independent active-scanning tools can often provide a more comprehensive view of devices by revealing both published and unpublished information. However, active scanning tools can also negatively impact device availability and functionality, potentially leading to unwanted operations. It may be possible to configure these types of scanners to limit their potential to overload the resources of OT devices. Asset owners may want to consult with their vendors, assess the scope of networks and systems in which these tools are used, and test them before implementing them in the production environment.
- **Software agents.** Many asset management tools that are common in the IT environment operate using software agents installed on devices. While these can provide broad visibility into a device's software and configuration, they are not typically deployed across the OT environment for various reasons. First, many devices in the OT environment (e.g., PLCs, sensors, other embedded devices) do not run common OSs that are capable of supporting these software agents. Next, if devices do run common OSs, there may be contractual or warranty-related reasons for why vendors may not permit these agents from being installed (e.g., incompatibilities, operational impacts). When considering a software agent to collect asset information, asset owners should consult with the appropriate vendors prior to installation and test their implementation to understand the potential risks.

The appropriate discovery method for a given asset is often determined by the equipment's age and capabilities. Modern devices with sufficient processing resources, and network connectivity can generally tolerate more active forms of discovery. Older or more resource-constrained devices may not tolerate active interrogation and are better-suited to passive monitoring, which collects information without sending traffic to the device. Legacy or isolated devices that lack network connectivity or cannot be reached by automated tools require manual processes (e.g., physical inspection, direct console access) to capture accurate inventory information. Organizations should evaluate the age and capabilities of their assets when selecting discovery methods and should not apply a single approach uniformly across environments with a mix of modern and legacy equipment.

The deployment of asset management infrastructure must also incorporate network architecture challenges. Tools that perform active network scanning must have routable connections to all deployed devices. Passive monitoring tools must have access to switch SPAN or TAP ports that provide access. Software agents must deal with the configuration management of deployed agents across the devices in which they are installed. Further, asset management tools typically require server infrastructure to aggregate data from various remote monitoring tools and agents.

Organizations may face multiple challenges in establishing an asset inventory, especially when adopting and integrating automated tools. For example:

- Many OT environments contain isolated systems, components, or systems that are connected on non-IP networks and cannot be remotely accessed to support the discovery or management of assets.
- The use of incompatible or untested automated asset discovery and management tools can negatively impact OT operations.

Asset owners may also want to consider how automated scanning activities could 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. Performing tests using automated asset management tools on offline systems or components is recommended before deployment into the OT production environment. When automated tools are not feasible due to network architecture or other OT environment issues, the organization should consider manual processes to maintain a current inventory.

While automated tools are useful for building inventory, they may not be able to discover or collect relevant data from all assets. Therefore, organizations should consider physically inspecting OT network connections or analyzing network logs to document the OT network architecture.

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

- SP 1800-5, *IT Asset Management*
- SP 800-53r5, *Security and Privacy Controls for Information Systems and Organizations*

4.1.1.2. Establishing Asset Criticality and Function

Asset inventories should also include information on the organization or individual responsible for managing the device, the device's operational criticality, and any regulatory oversight of that asset. This information is critical to ensuring that the asset is adequately protected and that any decisions associated with it involve the correct groups and are documented appropriately. Information about the device's criticality can include the key safety functions supported as well as its role in maintaining key operations. This information can be obtained from the results of risk assessment processes (ID.RA) and broader decisions on the governance context (GV.OC).

4.1.2. Architectures and Baselines

A comprehensive understanding and baseline of the data flows associated with the assets is critical for the successful deployment of cybersecurity controls. This information is also important for other security functions, including network monitoring and incident response.

To establish a baseline, organizations should begin by understanding which devices a specific asset communicates with; which addresses, ports, and protocols it uses; and the functional purpose of the communication. This information should be documented within a broad network diagram to ensure that it can be broadly shared and communicated with individuals across the organization. While establishing baselines for all devices across an organization may not be feasible, organizations should prioritize focusing on critical assets, network segments, and areas in which communications cross key boundaries, such as connectivity with the DMZ, internet, and external parties.

Numerous tools can support the development of an architecture document, including tools to perform asset discovery and management (Sec. 4.1.1) and network detection tools (Sec. 4.3.1.4). These tools can help an organization identify, document, and diagram the interconnections between devices, enterprise networks, and other external connections.

Organizations should pay particular attention to cloud conduits when documenting their architecture. Cloud conduits are connections between OT systems and cloud-based services or platforms that may bypass traditional network boundaries and introduce exposure that is not immediately visible in standard network diagrams. These connections should be explicitly identified, documented, and assessed as part of the baseline process.

Organizations should also treat the discovery of unknown assets and undocumented connections as a core objective of the architecture and baseline process. Unauthorized or undocumented devices and connections, sometimes referred to as Shadow IT/OT, can introduce unmanaged risks into the OT environment. Any device or connection that cannot be attributed to a known, authorized function should be investigated and either formally documented or removed.

4.1.3. System-Level Risk and Vulnerability Assessment (ID.RA)

Cybersecurity risk assessments are performed to identify risks and estimate the magnitude of harm to operations, assets, or individuals that might result from cyber incidents, such as unauthorized access, use, disclosure, disruption, modification, or destruction of an information system or data. Risk assessments require understanding the impacts (i.e., consequences) and methods (e.g., threats and vulnerabilities) that cause them. Risk assessments leverage the risk management strategy (e.g., acceptable risk assessment methodologies, risk tolerance) and facilitate efforts to identify, estimate, and prioritize risks to operations, assets, individuals, and other organizations.

Risk assessments help organizations understand how cybersecurity events could affect safety, reliability, and operations so that resources (e.g., people, money, technology) can be applied in a manner that reduces the most significant risks. Results from a risk assessment can be used to generate scenarios that inform decisions around controls, system design, maintenance, incident response, tabletop exercises, vendor management, and data collection management strategies. It also helps in identifying critical assets, functions, dependencies, and cascading impacts.

The objective of a risk assessment is to determine how a cybersecurity event could affect the organization’s ability to accomplish its mission safely and reliably. This includes the loss of view

and/or control, which can lead to an inability to produce products, a degradation of product quality, damage to equipment, environmental damage, or a health and safety incident.

Organizations may need to evaluate the potential physical impacts across all parts of an OT system. Organizations may also need to determine how OT systems interact with or depend on IT to support risk decisions. These processes may require organizations to identify a common framework for evaluating impacts that incorporates OT considerations. One approach is based on NIST Federal Information Processing Standards (FIPS) publication 199 [FIPS199], which specifies that systems are categorized as low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability. Another approach based on ISA 62443-3-2 [ISA62443] provides example definitions for determining system categorization based on OT impacts.

Risk assessments are typically point-in-time reports. As a result, organizations should ensure that they are up to date and that their security levels remain adequate.

Supplemental guidance for risk assessments can be found in the following documents:

- SP 800-30r1, *Guide for Conducting Risk Assessments*
- SP 800-37r2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- CISA Risk Assessments Resources
- ISA/IEC 62443-3-2, Security for industrial automation and control systems, Part 3-2: Security risk assessment for design
- ISA Global Cybersecurity Alliance, Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies

4.1.3.1. Understanding OT Impacts

In OT environments, impacts may relate to safety, health, and the environment as well as business and financial impacts. Organizations should use existing analyses (e.g., PHA, FMEA) or past events (e.g., power outages, control failures, upstream feed disruptions, downstream capacity issues, major equipment failures) to understand the potential impacts of a cyber incident.

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

on their services. More specifically, organizations should consider identifying interdependent OT systems that pose cybersecurity risks that threaten system availability.

OT systems often rely on supporting services that reside in the enterprise network (e.g., billing, maintenance), remote access solutions (internal and third-party), identity infrastructure, time synchronization, and backup infrastructure or cloud-based services, which may introduce risk. Organizations should identify both logical and physical dependencies and evaluate failures and the impacts they can have across those relationships.

The impact of a cyber incident in an OT environment may include both physical and digital effects that risk assessments need to incorporate, including:

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

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

Table 5. Categories of non-digital OT control components

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

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

4.1.3.2. Threat Characterizations

There are three factors for a threat to be applicable: capability, intent, and vulnerability. Capability and intent information can be obtained from OSINT and external intelligence-sharing sources (e.g., Information Sharing and Analysis Centers [ISACs], threat feeds). Organizations should consider participating in cyber threat information sharing [SP800-150]. Threats can be external (e.g., APTs) or internal (i.e., insiders).

Organizations may want to consider incorporating resources (e.g., the MITRE ATT&CK for Industrial Control Systems [ICS] framework [ATTACK-ICS]) into their processes for assessing risks to the mission and OT systems. ATT&CK for ICS categorizes adversarial tactics, techniques, and procedures (TTPs) that have been used to target ICS environments across real-world threat events. It provides a strong understanding of how threat actors are currently targeting OT environments, which is critical to ensuring that the organization's risk management processes adequately incorporate realistic threat behavior.

Supplemental guidance for threat characterization can be found in the following documents:

- MITRE ATT&CK for ICS
- National Council of ISACs

4.1.3.3. Assessing Vulnerabilities

A key part of risk assessment is the identification of vulnerabilities and associated predisposing conditions within the OT environment. A list of common vulnerabilities and predisposing conditions is defined in Appendix C. While vulnerabilities are often associated with the products and services used by the organization, others depend on the device's unique architecture or implementation details.

Understanding vulnerabilities associated with vendor products and services depends on an accurate inventory of IT and OT assets within the operating environment, including the vendor, model numbers, firmware, OSs, and software versions installed on the assets. This inventory facilitates the identification, tracking, and remediation of vulnerabilities. OT-specific vulnerability information is available through multiple methods, including:

- Using OT-specific tools to automate asset inventory creation, cross-correlation of the inventory with known vulnerabilities and threats, and regular updates
- Monitoring security groups, associations, and vendors for security alerts and advisories

- Reviewing the NIST National Vulnerability Database (NVD) and CISA Known Exploited Vulnerabilities (KEV) Catalog for detailed information on known vulnerabilities for hardware and software assets

In addition to understanding the vulnerabilities across products and services, organizations must also examine their architectures, deployed security controls, configurations, and any custom infrastructure that may introduce additional vulnerabilities. While organizations often execute vulnerability assessments in their environments, these can be problematic in OT environments. Specifically, both vulnerability scanning tools and vulnerability assessment methods can potentially disrupt systems. Therefore, organizations should use caution when performing this assessment on production systems. They may instead want to test in representative lab environments.

Vulnerabilities can be identified through a combination of automated and manual techniques. These vulnerability scans should be performed on an ongoing basis to capture newly discovered vulnerabilities. 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 affect OT components and communications by testing them in an offline environment before implementing them in production.
    - Passive scanning tools typically use network traffic analyzers to detect assets and identify potential vulnerabilities affecting them.
    - Active scanning tools typically use an agent to connect to networked assets and perform detailed queries and analyses of components to identify 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.

4.1.3.4. Evaluating Risk

As discussed in Sec. 3, the organization needs to define risk tolerances and add findings to the risk register. For risks that exceed the organization's tolerance, implemented remediations or mitigations should align with Sec. 4.2 *Protect (PR)*, Sec. 4.3 *Detect (DE)*, Sec. 4.4 *Respond (RS)*, and Sec. 4.5 *Recover (RC)*.

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. [SP800-30r1] provides guidelines on developing likelihood-weighted risk factors. Organizations should consider weighting risk factors based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities), that the threat event will be initiated, and that the threat event will result in adverse impacts.

For adversarial threats, the likelihood of occurrence is typically assessed based on the adversary's intent, capability, and targeting. For other-than-adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, and other factors. If organizations find that their historical data is minimal, they may want to extend their analysis to include industry-specific data on cybersecurity events reported by similar organizations.

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

Organizations that establish definitions for event likelihood may want to review Appendix G of SP 800-30r1 for more detailed guidance and suggestions. Based on this guidance, organizations should consider defining five levels of likelihood, from Very Low to Very High, for both adversarial (i.e., intentional threat actors) and non-adversarial (e.g., errors, accidents, acts of nature) events. Additionally, organizations may want to establish definitions for the likelihood that an event may result in an adverse impact. Using these two factors, organizations can establish a heat map like the one shown in Table 6 to determine the likelihood of supporting the risk analysis.

Table 6. Event likelihood evaluation

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

4.2. Protect (PR)

Within OT environments, the primary objective of the CSF 2.0 PROTECT (PR) function is to develop, implement, and sustain appropriate safeguards to manage the organization's cybersecurity risk without compromising the safety, reliability, or availability of continuous physical processes. Achieving this requires organizations to carefully tailor and apply four core control families: identity, authentication, and access control (PR.AA); data security (PR.DS); platform security (PR.PS); and technology infrastructure resilience (PR.IR). This section provides specific guidelines on implementing these control objectives and addressing the unique

operational constraints, legacy system limitations, and safety imperatives inherent to OT environments.[6]

4.2.1. Identity, Authentication, and Access Control (PR.AA)

The CSF 2.0 Identity Management, Authentication, and Access Control (PR.AA) controls ensure that access to physical and logical assets is strictly limited to authorized users, services, and hardware and is managed commensurate with the assessed risk of unauthorized access. Establishing a robust access control architecture in an operational environment is a multi-step process that encompasses the full life cycle of an identity. It begins with foundational identity and access management (IAM) to administer accounts and assign permissions, followed by the deployment of appropriate authentication mechanisms to reliably verify those identities. Once verified, authorization and logical access controls ensure that local and remote users are granted only the minimum privileges necessary to perform their duties. Furthermore, because gaining physical access to an OT control room or component often implies gaining logical access to the system, these digital safeguards must be seamlessly integrated with comprehensive physical access controls.

While enterprise IT environments typically rely on stringent, ubiquitous access controls, implementing these capabilities in OT environments requires careful tailoring to avoid adversely impacting continuous physical processes. Organizations must balance the need to secure systems against the imperative for immediate operator access during emergency situations. In critical situations, the time required to enter a user's credentials may impede rapid response or intervention, resulting in negative consequences for safety, health, or the environment. When legacy OT equipment cannot natively support modern IAM capabilities, or when strict access controls introduce unacceptable latency or safety risks, organizations should select compensating countermeasures to provide an equivalent level of protection for the OT environment.

To navigate these complexities, the following subsections outline key considerations and recommendations for evaluating IAM processes, selecting appropriate authentication mechanisms, and adapting logical, remote, and physical access controls to fit the operational realities of their OT environments.

4.2.1.1. Identity and Access Management

Identity and access management (IAM) addresses the administration of accounts, the deployment of authentication, and the assignment of access rights or permissions for both users and systems.

When OT equipment cannot support IAM or the organization determines that it is not advisable due to adverse impacts on performance, safety, or reliability, the organization should select

[6] Awareness and training (PR.AT) is discussed in Sec. 3.5 due to the importance that training has with the broader roles and responsibilities within the organization.

compensating countermeasures to provide an equivalent security capability or level of protection for the OT.

An example of a unique challenge in OT is the need for immediate access to systems and interfaces during emergencies. The time required to enter a user's credentials may impede the operator's response or intervention, resulting in negative consequences for safety, health, or the environment.

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

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

The following sections describe some areas in which protections may need to be augmented to support identity and access management in the OT environment.

4.2.1.2. Identity Life Cycle Management and Provisioning

Coordinating the organization's processes for authenticating and authorizing users to access the OT environment can be difficult when systems are not connected. Having a process to remove a user's access to physical locations and the computer systems they use may require multiple steps and involve both automated and manual processes. It can also be complicated when OT systems are disconnected or have local accounts.

Written processes and checklists can help organizations ensure that, as personnel join, change job roles, or leave the organization, their associated user accounts are properly modified to reflect their appropriate access needs. These written processes will help ensure that linkages between departments within the organization are not overlooked.

4.2.1.3. Separation of Duties and Dual Approval

The ability to create, modify, or delete user accounts needs to be managed within an organization. Separating the approver of these changes from the implementor provides an additional layer of protection, ensuring that no single person can compromise the system.

Multiple approvers may be required for accounts with higher levels of privilege. For example, creating a normal user account may only require their manager's approval, but creating a system administrator may require their direct manager and a security officer to confirm that additional background checks have been performed.

4.2.1.4. System, Device, and Service Accounts

In OT environments, many systems communicate automatically without the need for a human user. These may be controllers talking to HMI, data aggregators talking to historians, or software talking to a license server. In many cases, these use some form of user account as one layer of protection for the information being communicated. While these user accounts are not inherently different from human user accounts, they may have some different requirements since they are often not changed once established. If the devices are capable, these accounts should use the most complex credentials possible. These accounts are usually tied to automated processes. Modifying the credentials for these accounts can cause operational downtime if the change is made in one location but not the other. Therefore, procedures to change credentials should be developed and validated to ensure credentials can be changed if necessary.

4.2.1.5. IT/OT Identity Convergence and Centralization

As organizations modernize their industrial environments, they may find opportunities to streamline account administration by centralizing user, device, and process identification and authentication. Utilizing common network technologies, such as Active Directory or Lightweight Directory Access Protocol (LDAP), can support centralizing identity management across both IT and OT environments. This centralization enables the convergence of physical and logical access controls. For example, standardizing on federal PIV smart cards allows an organization to use the same credential mechanism for both physical entry into a facility and logical authentication into OT assets, adjusting the required authentication factors (e.g., Card-Only vs. Card+PIN) based on the risk level of the protected resource. However, while unified credentialing improves monitoring capabilities and reduces administrative overhead, organizations must carefully weigh the operational benefits of centralized accounts against the increased cybersecurity risks of allowing authenticated accounts from the IT environment to access the OT environment.

4.2.1.6. Authentication Mechanisms

There are several possible factors for determining the authenticity of a person, device, or system, including something you know (e.g., PIN, password), something you have (e.g., key, dongle, smart card), something you are (i.e., a biological characteristic, such as a fingerprint or retinal signature), and where you are (e.g., geofencing).

OT organizations must manage user accounts and authentication mechanisms across diverse environments, and many device manufacturers and legacy devices lack support for modern authentication mechanisms. Therefore, organizations are often forced to share user accounts, which limits both the accountability of user access and the ability to have individual user credentials. Organizations must also often provide accounts and credentials for manufacturers, integrators, or contractors that require remote or on-site access.

4.2.1.6.1. Password Authentication

While password authentication schemes are extremely common, they present challenges in OT environments. Device protocols may transmit passwords in plaintext, and complex passwords could pose safety issues if operators are locked out during critical events.

Organizations should consider the following password recommendations:

- **Change default passwords.** Always change default passwords on OT equipment to prevent trivial exploitation.
- **Balance complexity and safety.** Enforce appropriate password length and complexity, balancing security requirements with the operational necessity for rapid access during safety-critical functions.
- **Protect privileged accounts.** Administrative accounts require stronger complexity, more frequent rotation, and additional physical safeguards.
- **Secure transmission and storage.** Passwords should never be transmitted over the network unless protected by FIPS-approved encryption. Organizations should also consider using a secure, centralized password management tool.
- **Life cycle management.** Implement procedures to rotate passwords periodically, when a compromise is suspected, or when an individual leaves the organization

4.2.1.6.2. Multi-Factor Authentication

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

4.2.1.6.3. Token Authentication

Traditional passwords can become lost or stolen without notice, leaving credentials more vulnerable to exploitation. Token authentication primarily addresses this issue by requiring physical possession of the token. If a security token is lost or stolen, the token owner is typically aware of its absence and can notify security personnel to disable access.

Physical token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used alongside the token. Common forms of physical token authentication include:

- 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)

When token authentication uses cryptographic verification, the access control system should conform to the requirements of NIST SP 800-78-5.

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

4.2.1.6.4. Biometric Authentication

Biometric authentication enhances software-only solutions (e.g., password-based authentication) by providing an additional authentication factor and eliminating 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 provide a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases security.

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

- Handling environmental factors (e.g., temperature, humidity) to which some biometric devices are sensitive.
- Addressing industrial applications for which employees may have to wear safety glasses and/or gloves and industrial chemicals are present
- Denying needed access to the OT system because of a temporary inability of the sensing device to acknowledge a legitimate user

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

4.2.1.7. Authorization and Logical Access Controls

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

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

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

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

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

Solutions that provide credential management, authentication, authorization, and system use monitoring can help manage risks associated with OT devices and protocols by offering a secure platform for authorized personnel to access OT devices.

Access control systems should verify the identity of individuals, processes, or devices before granting access while minimizing latency and delays in processing OT system access or commands.

Systems should also be highly reliable and not interfere with OT personnel's routine or emergency duties. Solutions should be designed to reduce the impact of identity and authorization checks on OT operations and safety.

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

- SP 800-63-3, *Digital Identity Guidelines*
- SP 800-73-4, *Interfaces for Personal Identity Verification*
- SP 800-76-2, *Biometric Specifications for Personal Identity Verification*
- SP 800-78-5, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*
- SP 800-96, *PIV Card to Reader Interoperability Guidelines*
- SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

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, RBAC on engineering workstations and servers, and ABAC integrated into physical security for sensitive areas may meet an organization's risk-based access control requirements.

4.2.1.7.1. Privileged Access Management

Privileged access management (PAM) is a set of technologies and processes used to control, secure, and monitor accounts with elevated permissions (e.g., administrator, engineer, and service accounts) so that critical systems can only be accessed by authorized users for approved purposes. One feature often found in PAM solutions is to rotate shared or embedded credentials, which are commonly found in OT. Additionally, PAM solutions can provide audited session recording for remote vendor and maintenance access, creating clear accountability for privileged actions.

4.2.1.8. Remote Access Controls

OT environments often require access from remote users or devices, including those external to the company. Access requirements and accounts for remote access should be maintained for all external access. A process should be developed and communicated to the organization for requesting and enabling remote access. This should include the business justification for the access and document the expected security controls and the responsibilities of the external organization and device. Further, ensure mechanisms exist to revoke access rights and accounts associated with external users along with mechanisms to audit their access.

Deploying secure remote access technologies requires the deployment of various technologies and devices to authenticate and secure access sessions. Remote access often requires the use of the following devices:

- **TLS/SSL VPNs.** VPN appliances are often used to establish secure tunnels to a VPN appliance within an OT DMZ. The use of VPNs should be complemented with additional tools to help manage access to OT devices.
- **Access management tools.** Access management solutions (including privileged access management) manage credentials and sessions across heterogeneous OT devices. They can enforce strong authentication (including MFA), enable least-privilege access, and improve auditing of OT access.
- **Jump hosts.** Jump hosts or servers can also be used to broker user access to remote OT devices, including to control and monitor access.
- **Authentication servers.** OT environments often require dedicated and segmented authentication services (e.g., LDAP, Active Directory) to keep OT credential stores and authentication workflows separate from those used in IT networks.

Remote access methods include remote agents, jump hosts, site-to-site direct connections, and, most commonly, VPNs. These technologies must be carefully managed to minimize the organization's attack surface. For example, persistent VPN tunnels with poor authentication factors may be exploited by attackers to gain network access using trivial techniques.

4.2.1.9. Physical Access Controls

Defense in depth is a multifaceted strategy that integrates people, technology, and operational capabilities to establish variable barriers across multiple layers and dimensions of the organization. Physical security should be included in a comprehensive defense-in-depth strategy. Physical security measures are designed to reduce the risk of accidental or deliberate loss or damage to assets and the surrounding environment. Limiting physical access to assets helps prevent undesirable effects, including unauthorized physical access to sensitive locations; the unauthorized introduction of new systems, infrastructure, communications interfaces, or removable media; and the unauthorized disruption of the physical process. Physical access controls include controls for managing and monitoring physical access, maintaining logs, and handling visitors.

Safeguarded assets may include control systems, tools, equipment, the environment, the surrounding community, and intellectual property, including proprietary data (e.g., process settings and customer information). Organizations may also need to consider additional environmental, safety, regulatory, legal, and other requirements when implementing physical security.

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

The initial layers of physical access control are often determined based on the risk of access to the overall facility, not just OT components. Some regulations may also determine the strength and quantity of barriers used for the physical protection of a facility, such as the North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP), or those from the Nuclear Regulatory Commission (NRC).

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

- **Protection of physical locations.** Classic physical security considerations typically include a layered architecture of security measures that create multiple physical barriers around buildings, facilities, rooms, equipment, and other information assets. Physical security controls should be implemented to protect physical locations and may include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, door and cabinet locks, guards, or other measures.
- **Physical access control.** Equipment cabinets should be locked when not required for operation or safety, and wiring should be neat and contained within cabinets or under floors. Additionally, consider keeping all computing and networking equipment in secured areas.

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

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

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

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

Providing physical security for control centers and control rooms can reduce the potential of many threats, including unauthorized access. Access to these areas should be limited to authorized personnel due to the increased probability of finding sensitive servers, network components, control systems, and consoles that support continuous monitoring and rapid response. Gaining physical access to a control room or OT system components often implies gaining logical access to the system or system components. In extreme cases, organizations

may need to consider designing control centers to be blast-proof or provide an off-site emergency control center to maintain control if the primary control center becomes uninhabitable.

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

- CISA, Cybersecurity and Physical Security Convergence Action Guide
- UFC 4-020-01, Security Engineering Facilities Planning Manual

4.2.2. Data Security and Cryptography (PR.DS)

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. The protection of data should also extend to backup images and data stores to ensure they remain available and free from tampering. This section will explore the key technologies needed to protect data, including the deployment of cryptography in OT environments.

4.2.2.1. Data Classification

Different types of OT system data can be found in the OT network, such as control data (e.g., setpoints, recipes, interlocks, alarm settings), process data (e.g., sensor readings, batch records, quality measurements), and identity and access data (e.g., accounts, roles, remote access logs). Additionally, information related to the OT system data can be found on the IT network, such as engineering data (e.g., Piping and Instrument Drawings [P&IDs], electrical diagrams, robot programs, operating manuals, Programmable Logic Controller [PLC]/Distributed Control System [DCS] code, firmware, network diagrams), asset data (e.g., inventories, firmware versions, vulnerability/patch status), environmental data (e.g., emission records, compliance evidence), and maintenance data (e.g., work orders, service reports).

OT data needs to be classified based on its impact on the organization due to loss or modification. Some of the criteria to be considered include the safety/operational impact if the data is altered or lost, how difficult recovery would be, who currently has access to the data, whether the data is exported and to whom, and whether an adversary reviewing the data would gain an understanding of the organization's system or be able to use it to help plan a campaign. Data control considerations can include data access, handling rules (e.g., storage, transmission, access, retention), sharing with vendors/third parties, and compliance requirements. These considerations apply to data at rest and in transit.

4.2.2.2. Use of Cryptography

Cryptography can support data security requirements. Encryption, digital signatures, hashing, and other cryptographic functions are available to prevent unauthorized access or the modification of data at rest and in transit. Encrypting data that flows over networks (i.e., in transit) or data stored in memory and local storage (i.e., at rest) can also be used in defending OT. Encryption prevents an attacker from viewing or modifying cleartext data streams.

OT applications often focus on data availability. Before deploying cryptography in OT, ensure that confidentiality or integrity is the goal of applying the security. Understanding the advantages and disadvantages of cryptography can help organizations make an informed decision about where to incorporate it into the defense-in-depth strategy.

Organizations should deliberately scope where encryption is applied across their OT environment rather than treating it as uniformly deployable. Not all OT systems can support encryption since legacy devices may lack native cryptographic capabilities, sufficient processing capacity, or the ability to tolerate the latency introduced by encryption. The concept of encryption exposure radius refers to organizations identifying which systems, data flows, and storage locations carry the highest risk if exposed and prioritizing encryption there while documenting where encryption is not feasible and implementing compensating controls accordingly.

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

When cryptography is selected, organizations should use a certified cryptographic system. Additionally, cryptographic hardware should be protected from physical tampering and uncontrolled electronic connections.

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.

4.2.2.2.1. Post-Quantum Cryptography (PQC) Considerations

The emergence of quantum computing presents a long-term threat to current public-key cryptographic algorithms (e.g., RSA, elliptic-curve cryptography), which could be rendered vulnerable by a sufficiently capable quantum computer. OT environments face a particular challenge in transitioning to post-quantum cryptographic standards since many OT devices have life cycles measured in decades and cannot be easily patched or replaced. Organizations should begin assessing their cryptographic inventory now, which involves identifying the systems that rely on public-key cryptography, understanding the vendor's roadmap for PQC support, and prioritizing migration planning for the highest-risk systems.

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

- SP 800-47r1, *Managing the Security of Information Exchanges*
- SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*
- SP 800-209, *Security Guidelines for Storage Infrastructure*

4.2.2.3. Protecting Data at Rest

Identify critical physical and electronic file types and data to protect while at rest. This may include personally identifiable information and sensitive, proprietary, or trade secret information. Organizations should consider centralizing critical data within secure storage locations. When OT data is stored in the cloud or on vendor servers, organizations should consider conducting a risk analysis to assess how the service provider protects the data and whether additional countermeasures are needed to manage risk to an acceptable level.

4.2.2.3.1. Cryptographic Protection for Data-at-Rest

Encryption can also be used on hard local storage to protect information at rest. Full disk encryption is recommended for portable laptops, devices, and removable media. Organizations may also want to consider encrypting folders that contain sensitive files. When using disk or file encryption, organizations should ensure that appropriate backup keys are maintained and securely stored to support recovery if the primary encryption key is lost or forgotten.

4.2.2.3.2. Access Control and Enforcement

Access to data should be restricted to authorized users and services through the implementation of access enforcement to critical data. Organizations should ensure that logical access controls are deployed to restrict access based on the defined authorization policy. If devices or software do not support modern access control mechanisms, compensating controls may be necessary, such as restricting access to a secure workstation or placing the system behind a protected network boundary.

4.2.2.3.3. Media Protection

Processes and procedures for handling media assets should be developed and followed. This includes labeling media for distribution and handling requirements, storage, transport, sanitization, destruction, and disposal. Media assets include removable media and devices, such as floppy disks, Compact Disks (CDs), Digital Video Disks (DVDs), Secure Digital (SD) cards, Universal Serial Bus (USB) memory sticks, and printed reports and documents. Physical security controls should address specific requirements for the safe and secure maintenance of these assets and provide guidance for transporting, handling, 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. Organizations should apply a verification process that includes, at a minimum, scanning devices (e.g., laptops, USB storage devices) for malicious code prior to allowing them to connect to OT devices or networks.

Physically protecting media or encrypting the data on media is critical to protecting the OT environment. Access to media containing OT data could provide a malicious actor with valuable information to launch an attack.

Supplemental guidance can be found in the following documents:

- SP 800-88r1, *Guidelines for Media Sanitization*
- SP 800-100, *Information Security Handbook: A Guide for Managers*
- SP 800-209, *Security Guidelines for Storage Infrastructure*

4.2.2.4. Protecting Data in Transit

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).

4.2.2.4.1. Cryptographic Protection for Data in Transit

Organizations should consider using encryption and authentication to support secure connections or conduits for OT environments when connections must pass over non-OT network segments (e.g., enterprise networks, the internet, wireless).

Many modern automation protocols incorporate cryptographic protections and can be used to establish secure communication to OT devices, including OPC-UA and DNP3-SAv6. However, many devices utilize either unencrypted automation protocols (e.g., DNP3, Modbus) or unprotected management protocols (e.g., Telnet, HTTP). If OT devices lack cryptographic support, it may be necessary to encapsulate communication using other protocols to protect communications between network segments, such as a virtual private network (VPN). For example, a remote site might have a boundary protection device on-site that uses a VPN to establish a secure tunnel over an untrusted network (e.g., the internet) to a VPN-enabled device in the main control center at a different location.

Deploying cryptography on OT presents numerous challenges, including:

- The use of cryptography could introduce communications latency. Therefore, solutions should be tested to determine whether latency is acceptable for the application.
- Various cryptographic protocols depend on pre-shared keys or certificates across devices. However, certificates need to be signed by a common authority, or devices need to be configured to only accept authorized certificates (i.e., pinning). Certificates also have a limited validity period and may expire well before the OT environment reaches the end of its operational life. Organizations should ensure that they consider these challenges and validate that deployed technologies adequately address these challenges.

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

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

- SP 800-52r2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*
- SP 800-77r1, *Guide to IPsec VPNs*
- SP 800-113, *Guide to SSL VPNs*
- Cybersecurity and Infrastructure Security Agency (CISA) Barriers to Secure OT Communication: Why Johnny Can't Authenticate

4.2.2.4.2. Protecting Wireless Communications

Wireless communication can be used for local-area communication (e.g., wireless LANs, field networks) and wide-area communication using cellular, microwave, or satellite-based systems. While radio frequency (RF)-based communications provide enhanced flexibility over traditional physical (i.e., wired) communication capabilities, they are also more susceptible to interference, unauthorized access, eavesdropping, and reliability issues (e.g., signal jamming, distance limitations, line-of-sight requirements). Prior to installation, a wireless survey should be performed to identify antenna locations and signal strength for adequate coverage and to minimize the exposure of the wireless network to interference from OT environmental factors and eavesdropping.

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

- 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 failover of the network. Organizations should also consider the performance and security implications of using 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.
- Selecting a standard, non-proprietary protocol (e.g., IEEE 802.15.x).
- Allowlisting devices in the wireless device manager to prevent rogue devices from connecting.
- Implementing appropriately complex passwords and join keys.

- Consider implementing network access control mechanisms to strengthen authentication.

While encrypting and securing the data transmitted over wireless networks is critical, these data-level protections must be paired with network boundary defenses. For specific guidance on safely segmenting, isolating, and integrating wireless technologies within the broader OT environment, refer to Sec. 4.2.2.4.

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

- SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11*
- SP 800-121r2, *Guide to Bluetooth Security*
- SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*
- SP 800-187, *Guide to LTE Security*

4.2.2.4.3. Third-Party Communication Providers

OT environments often depend on third-party communication providers for connectivity to geographically remote sites and with external partners. These providers may lack adequate network protection, leaving them vulnerable to threats that degrade their availability and integrity. Therefore, organizations should deploy technical redundancies and contingency plans to support operations if these providers are compromised and unavailable, including establishing backup and contingency communications capabilities (e.g., PACE plans) or establishing procedures to operate in an isolated or manual mode if these communications are unavailable.

4.2.3. Platform Security and Infrastructure Resilience (PR.PS / PR.IR)

Platform security is a broad topic that encompasses many aspects of deploying, operating, maintaining, and decommissioning systems and devices in an asset owner's facility. Even the most secure device can be configured and/or maintained in such a way that renders its security ineffective.

4.2.3.1. Platform Configuration and Maintenance

4.2.3.1.1. Developing a Maintenance Tracking Capability

Establish processes and implement tools to ensure that routine and preventative maintenance and repairs (both local and remote) of OT assets are performed consistently with OT organizational policies and procedures.

Ensure that the processes and tools allow for scheduling, authorizing, tracking, monitoring, and auditing maintenance and repair activities for OT assets. 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.

Any maintenance performed on an OT device can inadvertently modify its configuration and result in an increased attack surface. The OT device should remain in a hardened state, 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.

Maintenance tracking tools enable an organization to schedule, track, authorize, monitor, and audit maintenance and repair activities to OT and ensure that maintenance logs or changes are properly documented. The software used for OT maintenance activities should be approved and controlled by the organization. Approved software should be obtained directly from vendors and its authenticity verified (e.g., validate certificates, compare the hashes of installers). If the ability for remote maintenance is required, ensure that the remote access tool supports the authentication of maintenance personnel, connection establishment at the beginning of maintenance activities, and immediate teardown once the maintenance activities are complete. Additionally, ensure that the tool can log the remote maintenance activities that are performed.

Maintenance devices that remain secure within the OT environment reduce their exposure. Using maintenance devices outside of the OT environment or connecting the devices to non-OT networks should be restricted or minimized. 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). Any devices that are connected to the OT system should be disconnected after the maintenance activities are completed, and any temporary connections should be removed. Vendor documentation should be thoroughly reviewed to understand these capabilities.

4.2.3.1.2. Configuration Management

Applying configuration management practices (e.g., setting access controls, enabling encryption) that support secure configurations and application hardening is important to meet organizational and regulatory security requirements. Application hardening procedures may also include disabling or blocking specific network communication ports, application features, or unnecessary services that run on the system.

Configuration management helps ensure that systems are deployed and maintained in a secure, consistent state and reduces the risk of outages by improving visibility and the tracking of system changes. In addition, configuration management can detect improper configurations before they negatively impact performance, safety, or security. Organizations should document the approved baseline configuration for their OT devices and establish the system development life cycle (SDLC) approach to document, test, and approve changes before deploying them to the OT environment. Organizations should also verify that default configurations align with the

predetermined safe states defined for each system to ensure that a device restored to its baseline configuration does not inadvertently place the physical process in an unsafe operating condition.

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

Configuration management tools enable an asset owner to establish and maintain the integrity of system hardware and software components by controlling the processes for initializing, changing, monitoring, and auditing the configurations of the components throughout the system life cycle. If the use of automated configuration management tools is deemed to be appropriate, processes should be in place to validate configurations prior to deployment. Many OT changes can be made only during scheduled maintenance downtime to minimize impact. When considering automated configuration management tools, organizations should also consider potential impacts on the OT system. In some cases, these tools transfer numerous types of data, potentially in large amounts, over the manufacturing system network. Additionally, some tools may also have the potential to impact OT system operations by attempting to change device configurations or manipulating active files. Keys for OT assets (e.g., PLCs, safety systems) should be in the "Run" position at all times unless they are actively being programmed.

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

- SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- SP 1800-5, *IT Asset Management*
- IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide*

4.2.3.1.3. Software/Firmware Patch Management

Organizations should implement an OT patch management process that defines how it will monitor for patches, when to apply them, how to test them (e.g., with vendors, on offline systems), and how to select compensating controls to limit exposure of the vulnerable system when patching is delayed. The process should be designed to not only reduce cybersecurity risks but also account for OT reliability, availability, and safety needs.

Organizations are responsible for staying informed and determining when patches should be applied as part of their documented patch management process. Many OT vulnerabilities are published to CISA as advisories or CVEs. However, not all vendors report known vulnerabilities to CISA or CVE. Organizations can often stay informed by subscribing to vendor-specific notifications in addition to CISA alerts and advisories. Private cybersecurity companies also

offer services to help organizations stay informed about known vulnerabilities in their OT environments.

OT environments present numerous challenges that constrain the deployment of patches. Patch management decisions should account for the following considerations:

- Many OT environments must run nearly continuously for extended periods or have small maintenance windows to apply approved updates. This limits the frequency with which patches can be applied.
- A patch may remove a vulnerability, but it can also introduce greater reliability or safety risks. Patching the vulnerability may also change the way the OS or application behaves, potentially resulting in some loss of functionality.
- Legacy devices and software often lack vendor support and may no longer receive patches for identified flaws and vulnerabilities.

OT patching decisions should factor in operational requirements and potential adverse effects of installing the patch and be determined by knowledgeable OT personnel. Many organizations define decision frameworks (e.g., Now/Next/Never, Now/Next/Later) to triage and inform patching decisions:

- **Now.** Patches that pose immediate risks and can be installed without impacting operations may be applied immediately. These may include patches for components within DMZ environments, network segments that are more exposed, or vulnerabilities that allow unauthorized remote access to the OT environment.
- **Next.** Vulnerabilities that pose a significant risk to operations but cannot be feasibly patched may need to be scheduled during the next scheduled maintenance period.
- **Later (or Never).** Other vulnerabilities that present reduced or minimal risk may be scheduled for a future time. Additional information about this approach is defined here.

An organization's patch management process should also define processes to prevent or recover from any unintended consequences of deployed patches. For example:

- Consider separating the automated OT patch management process from the automated non-OT application process.
- Patches should be adequately tested (e.g., offline system testing) to assess the acceptability of any performance impacts before being deployed into a production system.
- Have a recovery plan for the OT component or system being patched in case the patch causes an unexpected issue.

If patches cannot be deployed, the organization should explore appropriate compensating controls. Security tools (e.g., web application firewalls, IDSs) could be configured to provide additional protection to detect or prevent attacks exploiting unpatched vulnerabilities while the organization waits for an opportunity to apply the updates. Other tools (e.g., bump-in-the-wire

security devices) can be installed in line with devices that cannot be updated or are using obsolete operating systems.

Organizations may be required to follow industry-specific patch management guidance. Otherwise, they may develop patch management procedures based on existing standards.

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

- SP 800-40r4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- ISA 62443-2-3, Patch Management in the IACS Environment

4.2.3.2. 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.

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 DHS recommends it as a best practice. When considering application allowlisting within an OT environment, organizations should coordinate with their vendors and review available implementation guidance, such as SP 800-167, *Guide to Application Whitelisting*, or relevant guidance for their industry. The configurations and policies should be thoroughly tested before being deployed to ensure that the rules and settings properly support organizational security objectives.

4.2.3.3. Hardware Management

Hardware must also be managed securely throughout its life cycle, especially during decommissioning and disposal.

4.2.3.3.1. Decommissioning Systems

Managing OT hardware throughout the system life cycle is essential to ensuring operational efficiency and reducing the organization's attack surface. When OT devices are decommissioned, associated risks may manifest as many devices participate in tightly coupled control and safety functions. These devices may also have dependencies that are unknown to the maintenance staff (e.g., time synchronization, OPC links, software licensing).

When the decision is made to decommission a system, a thorough review must be conducted to ensure that the asset's removal from production has no negative or otherwise adverse effects on normal operations (e.g., no impact on system functionality, overall monitoring, or operator visibility). If the review yields no findings of note, staff may proceed and remove the system from production. It is recommended that operators revoke devices' certificates or other

keys, disable device-related and service accounts, remove firewall and ACL entries, and ensure that the device is no longer reachable via the network or other logical means upon removal.

4.2.3.3.2. System Disposal

Upon the completion of system decommissioning, secure disposal is necessary. OT devices may contain proprietary information (e.g., PLC logic, product recipes, product batch records, calibration information, other artifacts) that could enable process replication, thereby compromising an organization's competitive advantage.

To establish a paper trail during the disposal process, organizations should leverage a chain of custody from removal through storage and transportation to the decommissioned device's final disposition. Additionally, the organization should note whether the equipment is being destroyed, returned to its vendor, or retained as a spare. Retained in-scope assets should be inventoried, securely stored, and — if applicable — reintroduced in a secure manner in keeping with defined policy.

Some OT devices may be environmentally hazardous or subject to e-waste statutes, depending on jurisdiction, and must be handled accordingly. Should the organization handle destruction, careful steps must be taken to purge all media and leave no trace of its past production state unless data retention is required by policy or law. Proprietary process data or secrets may persist on devices even after decommissioning, so performing and validating a factory reset is imperative.

If devices are to be destroyed by a third party, the organization must require that party to follow its expected media sanitization procedures and obtain proof of completion.

4.2.3.4. Software Development Life Cycle

Organizations that develop in-house systems and components should incorporate policies and procedures that support and validate secure code development practices into the cybersecurity program. The software development life cycle (SDLC) should consider security during each phase, including 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, these same practices should be reviewed prior to executing contracts with vendors. Organizations can help industries move toward more secure products by incorporating security requirements into their procurement decisions and vendor agreements. This approach is known as secure-by-design procurement and shifts the burden of security from the asset owner back to the manufacturer, where it can be addressed most efficiently and at scale. Prior to procurement, organizations should evaluate prospective OT products against key security criteria, including secure-by-

default configurations, strong authentication, baseline logging, commitment to vulnerability management, and support for open standards.

The SDLC is especially critical for programmable automation devices (e.g., PLCs) because unauthorized or untested changes to device logic can cause operational disruptions or safety incidents. Organizations should follow applicable industry guidance for secure coding practices for automation logic, including PLC programming.

Supplemental guidance for secure-by-design procurement and secure coding practices for automation logic can be found in the following documents:

- Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products, U.S. Cybersecurity and Infrastructure Security Agency, Jan. 2025.
- Top 20 Secure PLC Coding Practices, PLC Security, admeritia GmbH. 2026

4.2.3.5. Resilience of Technology Infrastructure (PR.IR)

Managing the physical operating environment includes emergency protection controls, such as emergency shutdown of the system, backup power and lighting, temperature and humidity controls, and protection against fire and water damage. Organizations should develop policies and procedures to ensure that environmental operating requirements for assets are achieved. To this end, organizations should consider the following factors when identifying potential countermeasures to protect the operating environment:

- **Environmental factors.** Environmental factors can be important. For example, if a site is dusty, systems should be placed in a filtered environment, especially if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems.
- **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 risks of operating HVAC systems (e.g., air intakes) in an occupied shelter during a toxic release as well as the risks of continued operation during a power outage (e.g., using an uninterruptible power supply in critical environments). Additionally, fire systems must be carefully designed to avoid causing more harm than good (e.g., avoid mixing water with incompatible products). HVAC and fire systems play significant roles arising 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. In addition, environments that contain systems and media (e.g., backup tapes, floppy disks) should maintain stable temperature and humidity. An alarm should be generated in the OT system when environmental specifications (e.g., temperature, humidity) are exceeded.

- **Backup power.** Reliable power for OT is essential so backup power should be provided for critical systems. Depending on the site's needs, this can be something that lasts for seconds to minutes (e.g., UPS) or for hours to days (e.g., generator). The backup power should be sized to support operational needs, which can range from just long enough for a safe shutdown to supporting continued operations for an extended period.
- **Cabling.** While unshielded twisted-pair communications cables may be acceptable in an office environment, they may not be suitable for some OT environments due to their susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Organizations should consider using alternative cabling or shielding that provides suitable protection against environmental threats. Additionally, organizations should consider color-coded cables, connectors, conduits, and labeling to clearly delineate OT and IT network segments and reduce the risk of potential cross-connections. Organizations should also consider running spare cables during the initial commissioning.

4.3. Detect (DE)

Situational awareness of the OT system is imperative for understanding its current state, validating that it is operating as intended, and ensuring that no policy violations or cyber incidents have hindered its operation. To detect security incidents across the OT environment, the organization should deploy infrastructure to monitor and collect data from networks, hosts, users, and physical access systems. In addition to collecting this data, the organization should ensure that it is properly collected, stored, and reviewed by security analysts to help identify and investigate potential intrusions.

4.3.1. Continuous Monitoring (DE.CM)

The goal of continuous monitoring is to observe systems and user activities to detect anomalies, indicators of compromise, and other potentially adverse events. Monitoring includes collecting and analyzing digital artifacts from devices, network traffic, and user interactions, such as physical access and system use.

4.3.1.1. System and Device Monitoring

OT environments contain a diverse set of services, endpoints, and devices that should be monitored for potential malicious activity. This includes identifying and collecting logs, detecting the presence of malware across endpoints and servers, and aggregating and correlating user access records across the environment.

4.3.1.1.1. Device Logging

Network and computing devices (e.g., routers, gateways, switches, firewalls, servers, 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. Logging should also be configured and collected from any external computing platforms used by the organization, such as cloud services.

Capturing log events is critical to maintaining situational awareness of the OT system. Organizations should review their available logging capabilities and configure them to record the operational and cybersecurity events that are appropriate for their environment. Typical events include maintenance functions (e.g., access control, configuration changes, backup, 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 device's capabilities and the desired events to capture. In general, each log entry should also include where the event occurred, the type of event, when it occurred, the source of the event, the identities of any users or system accounts involved, and the outcome of the event.

To support log correlation, each log entry should identify the device that generated the event, the timestamp of the event, and the user or system account that generated the event. 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. Each device's internal clock should be synchronized with a primary clock to support event correlation across devices. Log entries should also use a consistent timestamp format (e.g., time zone format, string format, daylight saving). Organizations should verify timestamp consistency after log collection since device clock drift or loss of time synchronization can introduce discrepancies that affect the accuracy of event correlation and incident reconstruction.

Organizations should establish how long event logs should be retained and ensure that adequate storage is available to support log retention requirements. Many sector-specific regulations require data retention for a specific length of time. Depending on the frequency of events being logged, the log size may grow quickly and result in increasing space utilization. Disk space and memory are limited on most OT devices, so adequate storage should be provided locally or remotely to reduce the likelihood of exceeding device capacity, which could ultimately result in the loss of logging capability. Transferring logs from OT devices to alternate storage should be considered to free up device storage and ensure logs remain available for monitoring, analysis, and incident response.

Many OT devices either lack mechanisms to store logs or do not provide a network service that supports remote log collection (e.g., syslog). If device-level logs are unavailable, organizations should identify compensating data sources that can partially reconstruct activity on those devices. In this scenario, the engineering workstation or other programming terminal used to interact with the device is often the most valuable log source, as it may record engineering sessions, project file access, and maintenance activity even when the device itself cannot. Network infrastructure devices (e.g., switches, routers, firewalls) that sit adjacent to OT devices may also provide partial visibility through their own logs and capture connection activity and traffic patterns associated with those devices. Organizations should document which devices in their environment are incapable of generating or exporting logs and define compensating monitoring strategies for those device classes.

Organizations that use unidirectional gateways, data diodes, or similar devices to enforce highly segregated boundaries between OT and IT networks must explicitly design a security telemetry export path to ensure that security logs generated within the OT environment can still reach the IT SOC. These devices enforce one-way data flow by design, which can create a detection blind spot if this export path is not deliberately accounted for.

Supplemental guidance can be found in SP 800-92, *Guide to Computer Security Log Management*.

4.3.1.1.2. Service Logging

If cloud-based or hosted services (e.g., remote access platforms, cloud-based historians, vendor remote monitoring services) are present in the OT architecture, the log sources they generate should be included in the organization's host-based logging inventory. Unlike device-level logs, which originate from hardware within the OT environment, service logs are generated and may be retained by an external platform. This introduces considerations around log accessibility, retention controls, and data sovereignty that organizations should account for when defining their overall logging requirements.

4.3.1.1.3. Time Synchronization

Time synchronization solutions enable an organization to synchronize time across many devices. This is important for a variety of functions, including event and log correlation, authentication mechanisms, access control, and quality of service. Synchronizing the internal clocks of OT systems and devices is critical for cyber event correlation and other OT functions (e.g., motion control). If a device or system clock is inaccurate, the timestamps generated by the clock for event and log entries will also be inaccurate, as will any other functions that use the clock.

A common time should be used across all OT devices. Utilizing multiple time sources can reduce clock error and compensate if the primary time source is lost or its time quality degrades. Authenticated Network Time Protocol (NTP) and secure Precision Time Protocol (PTP) (i.e., PTP with an authentication TLV [type, length, value]) can be used if there is a risk of malicious modification to the network time (e.g., RF jamming, packet spoofing, denial of service). Non-authenticated NTP is susceptible to spoofing and should be located behind the firewall.

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

Supplemental guidance can be found in the following documents:

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

4.3.1.2. Malicious Code and Endpoint Monitoring

Tools should be used to monitor for malicious code and cyber threats across the organization, including file transfer tools and endpoint devices for potential threat actor behavior. OT organizations should be especially cautious about the use of tools on OT endpoints, as they could potentially introduce reliability or performance concerns.

There are multiple approaches and tools to detect unauthorized behavior on endpoints. Traditional antivirus software, which relies on a combination of heuristic algorithms and known malware signatures to detect and block potentially malicious code, can often be ineffective against novel malware or more modern threat actor tactics. More recent endpoint detection and response (EDR) tools focus on endpoint behavior analysis and telemetry collection, which can improve the ability to detect these threats.

The use of malicious code and endpoint monitoring within OT may require adopting special practices, including compatibility checks, change management, and performance impact metrics. These tools may consume significant CPU usage when running manual scans and signature updates, which could have negative impacts on OT computers and servers. Some OT vendors recommend and even support the use of vendor-specific malicious code and endpoint monitoring tools. In some cases, OT system vendors may have performed regression testing across their product line to support a particular malicious code or endpoint monitoring tool and provide associated installation and configuration documentation.

The decision to deploy these tools to an endpoint should be determined by both its functional role and the associated software it deploys. Generally:

- General-purpose Windows, Unix, and Linux systems used as engineering workstations, data historians, maintenance laptops, and backup servers can be secured like commercial IT equipment by installing push- or auto-updated malicious code and endpoint monitoring software with updates distributed via an update server located within the process control network. Follow organization-developed procedures for transferring the latest updates from known vendor sites to the OT platform servers and other OT computers and servers.
- Follow vendor recommendations on all other servers and computers (e.g., DCS, PLC, instruments) that have time-dependent code, modified or extended OSs, or any other change that makes them different from a standard PC. Test the malicious code and endpoint monitoring 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).

Before deploying malicious code and endpoint monitoring, software organizations should validate that they are compatible with the target platform and do not introduce any reliability or performance issues. Key checks include:

- The configuration of the antivirus software should be tested on an offline system, if possible.

- Manual scanning and signature updates should be performed while the system is not critical for operations.
- Redundancy should be considered for critical systems that require ongoing tool updates such that signature updates can be performed without impacting operations (e.g., consoles, HMIs).
- When configuring file exclusion lists, determine which control application files should not be scanned during production to avoid potential OT system malfunctions or performance degradation.

Malicious code protection tools only function effectively when they are installed, configured, run full-time, and properly maintained in light of known attack methods and payloads.

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

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

- SP 800-83r1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- SP 1058, *Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts*
- IR-18-214 - Recommended Practice: Updating Antivirus in an Industrial Control Systems. U.S. Department of Homeland Security. 2018

4.3.1.3. User Behavior Monitoring

User behavior monitoring focuses on observing and analyzing the actions performed by operators, engineers, administrators, and third-party personnel within the OT environment. Monitoring user activity requires collecting and correlating events from host devices, engineering software, and authentication servers to build a complete picture of personnel actions across the OT environment. Organizations should establish baselines of expected behavior for individual users or user groups, including normal working hours, expected privilege/access levels, typical systems accessed, expected software usage, and routine operational tasks. This will provide a reference point against which deviations can be identified. Anomalous activity (e.g., access outside of normal hours, privilege escalation, use of unauthorized accounts, configuration changes outside of approved maintenance windows) may indicate policy violations or potential security incidents.

User attribution in OT environments can be difficult for several reasons, including the use of shared accounts, limited device-level logging capabilities, legacy systems that do not support authentication, local access to devices that may bypass authentication and logging entirely, and automated processes that operate under generic service accounts. If individual attribution is not directly available, compensating controls (e.g., work orders, physical access logs, network infrastructure logs, session recording, personnel sign-in procedures) should be used to attribute actions to specific individuals. Network monitoring data and packet captures may also contain

user identity information if protocols transmit usernames or session context in clear text, providing an additional source for user attribution.

Third-party and vendor access warrants particular attention, as these users operate outside of the organization's normal oversight structures while often having elevated access to OT devices for maintenance and support purposes. Third-party sessions should be monitored against approved work orders and maintenance schedules, and activities should be logged and reviewed for any actions outside of the approved scope.

4.3.1.4. Network Monitoring

Network monitoring can greatly enhance the ability to detect attacks that are entering or leaving OT networks. It can also improve network efficiency by detecting non-essential traffic. OT cybersecurity personnel must be part of the diagnostic process for interpreting alerts from network monitoring tools. Careful monitoring and an understanding of the OT network's normal state can help distinguish transient conditions from legitimate attacks and provide insight into events outside of the normal state.

Network monitoring involves the continuous observation and analysis of traffic that traverses OT network segments to detect anomalous activity, identify potential cybersecurity incidents, and maintain situational awareness of the OT environment. Unlike host-based monitoring, which focuses on activities that occur on individual devices, network monitoring provides visibility into communications between devices across the OT architecture.

OT system traffic is typically more deterministic (i.e., repeatable, predictable, and designed) than IT network traffic, which can be leveraged to support network monitoring for anomaly and error detection. Organizations should refer to Sec. 5 for guidelines on OT network architecture, including network segmentation and zone design, which can directly inform sensor placement and monitoring strategy.

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

4.3.1.4.1. Monitoring Tools and Capabilities

Tools and capabilities that support behavior anomaly detection (BAD), SIEM, intrusion detection systems (IDS), and intrusion prevention systems (IPS) can assist organizations in monitoring network traffic and generating alarms when anomalous or suspicious traffic is detected.

Effective network monitoring in OT requires tools that can parse and interpret OT-specific industrial protocols. Organizations should ensure that their monitoring tools support the specific protocols in use within their environment, which may include Modbus, DNP3, IEC 61850, Ethernet/IP, PROFINET, OPC-DA/UA, and other vendor- or industry-specific protocols.

Some IDS and IPS vendors have incorporated attack signatures for common OT protocols to detect known attack patterns that target those protocols.

Organizations should carefully consider the impacts of automated response capabilities associated with IPS deployment in OT environments. Automated actions that are appropriate in IT environments may disrupt time-critical control processes or safety functions in OT. Organizations may consider limiting automated response capabilities to higher network levels (e.g., DMZ interfaces) if the risk of disrupting OT operations is lower while relying on alerts and manual responses at lower network levels that are closer to field devices.

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

4.3.1.4.2. Network Baselining

Careful monitoring and an understanding of the OT network's normal state can help distinguish transient conditions from legitimate attacks and provide insight into events outside of the normal state. A well-defined baseline differentiates between expected operational traffic and anomalous activity that may indicate a cybersecurity incident, misconfiguration, or equipment issue.

Building a network baseline involves observing and documenting the normal state of the OT network across several dimensions, including expected communication pairs, the protocols and port numbers in use, typical polling intervals and data volumes, and the function codes or command types used within OT protocols. Implementing network monitoring tools in a passive (e.g., listen or learning) mode and analyzing the information to differentiate between known and unknown communication may be a necessary first step in implementing network security monitoring. Organizations should also document expected communication flows between network zones, including traffic that crosses the OT/IT boundary or traverses the DMZ.

Once established, baseline information can be used as a reference point to identify deviations in network traffic. Not all deviations are malicious; for instance, equipment changes, software updates, and process modifications can all alter normal traffic patterns. Because of this, baseline maintenance should account for authorized changes to the environment. Baselines should also be reviewed and updated when significant changes are made to the OT environment, such as the addition of new devices, network reconfigurations, or changes to operational processes.

Supplemental guidance can be found in the following documents:

- SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*

- IR 8219, *Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection*

4.3.1.5. Physical and Environmental Monitoring

Physical access monitoring provides log sources for tracking personnel movement and detecting unauthorized access to sensitive areas. Monitoring the physical environment contributes to broader situational awareness and supports both safety and incident response activities across physical and cyber domains.

Organizations should also deploy systems to track and monitor physical access and activities across key sites and facilities. Examples of this include:

- **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 detecting unauthorized access.
- **People and asset tracking.** Locating people and vehicles within a facility can be important for both safety and security. Asset location technologies can be used to track the movements of people and vehicles to ensure that they remain in authorized areas, identify personnel who may need assistance, and support emergency response.

While these systems are critical to preventing unauthorized physical access to OT facilities, they also provide a key data source to support the investigation of cybersecurity incidents. Systems such as badge readers, biometric scanners, and electronic door controllers can generate timestamped access event logs that record who accessed a given area, when, and whether access was granted or denied. These logs are valuable not only for physical security purposes but also as a data source that can be correlated with cyber activity to detect threats that span both domains.

4.3.2. Anomalies and Events (DE.AE)

To effectively detect cyber threats, organizations must be able to collect and analyze diverse data from logs, devices, hosts, users, and network monitoring tools. This includes centralized data collection and storage, the ability to correlate and analyze information across multiple sources, the ability to assess activity against known adversary behaviors identified in current cyber threat intelligence (CTI), and properly staffed analysts who can investigate alerts and anomalies.

4.3.2.1. Data Aggregation and Analysis

Organizations should define how security events are integrated into their security operations center (SOC) or network operations center (NOC) functions. In some organizations, OT monitoring is handled by a dedicated OT security team, while in others it is integrated into an existing IT SOC or NOC. Regardless of the model, the roles and responsibilities for monitoring, triaging, and escalating OT network alerts should be clearly defined and documented.

Organizations should develop a plan to identify their available log sources and establish a centralized collection and aggregation capability that consolidates them into a unified platform for analysis, correlation, and retention. A SIEM platform can accomplish this by providing organizations with a single location to aggregate logs, apply correlation rules, and maintain a searchable record of security-relevant activities across the OT environment.

A significant challenge in SOC/NOC integration is the context gap between security analysts and OT operations personnel. Security analysts may have limited familiarity with OT protocols, equipment, and operational processes, which can make it difficult to accurately assess the significance of an alert without an operations context. Conversely, OT operations personnel may not have the security expertise to recognize threat patterns or assess the implications of anomalous network activity. Effective SOC/NOC integration requires close collaboration between security and operations teams, and organizations should establish clear escalation paths that involve operations personnel in the triage and assessment of OT network alerts before containment or response actions are taken.

Physical access, network, and host logs should be forwarded to the SIEM to enable this type of time-based correlation. Defining alert logic around physical-cyber event sequences adds a detection layer that is difficult for an adversary to avoid without simultaneously defeating physical access controls and operating within expected cyber behavioral patterns. Organizations should work with both physical security and OT operations teams to define what normal physical-cyber activity sequences look like so that anomalies can be identified with appropriate context.

4.3.2.2. Identifying Adverse Events and Anomalies

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

- **Information events**
    - Multiple failed logon attempts
    - Locked-out accounts
    - Unauthorized creation of new accounts

- Unexpected remote logons (e.g., logons of individuals who are on vacation, remote logon when the individual is expected to be local, remote logon for maintenance support when no support was requested)
- Cleared event logs
- Unexpectedly full event logs
- Antivirus or IDS alerts
- Disabled antivirus or other security controls
- Requests for information about the system or architecture (e.g., social engineering or phishing attempts)

- **Operational events**
  - Unauthorized configuration changes
  - Unauthorized patching of systems
  - Unplanned shutdowns
- **Physical access events**
  - Physical intrusions
- **Networking events**
  - Unexpected communication, including new ports or protocols being used without appropriate change management
  - Unusually heavy network traffic
  - Unauthorized devices connecting to the network
  - Unauthorized communication to external IPs

Organizations should consider that not all events and anomalies are malicious or require investigation. Organizations should define incident alerting thresholds and response requirements for the events and anomalies that affect their systems and environment to establish an efficient incident detection capability. To reduce false positive and nuisance alarms, organizations should establish their OT alerting thresholds based on baselines of normal network traffic, data flows, and human and OT process behavior.

Additionally, OT components are often physically remote and not continually staffed. Alerting thresholds may need to account for the alert response time as well as the speed of the physical process itself. Some OT processes can transition to an unsafe or damaging state within seconds of a malicious or anomalous command being executed. Alert prioritization and escalation paths should reflect these physical process response times to ensure that the most time-critical alerts are immediately routed to personnel with the authority and ability to take action.

Organizations should consider collecting and correlating event data from multiple sources and sensors using automated mechanisms to improve detecting and alerting capabilities. For example, a centralized intrusion detection system could accept data feeds and logs from

multiple devices and network segments to identify organization- or environment-specific events and sound an alarm. Detection tools should also be integrated with asset management tools. This integration can provide additional context to an event (e.g., system location, firmware version, system criticality) to help an organization determine the event's impact.

Supplemental guidance can be found in the following documents:

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

4.3.2.3. Integrating Cyber Threat Intelligence (CTI)

CTI provides analysts with external context about recent adversary behaviors, tactics, techniques, and procedures (TTPs) that can be used to enrich alert triage and improve detection capabilities. Organizations should identify and integrate CTI sources to ensure that they monitor for known threat actor behavior and indicators of compromise (IoCs). Organizations should identify and establish access to CTI sources relevant to their industry sector and the specific technologies deployed in their environment, including vendor feeds, sector-specific information-sharing and analysis centers (ISACs), and government advisories. Organizations should develop a process for evaluating incoming CTI for relevance and actionability, recognizing that not all intelligence will be immediately usable and that some may only inform longer-term detection improvements or patch planning.

The MITRE ATT&CK for ICS framework provides a structured knowledge base of adversary tactics and techniques observed in attacks against industrial control systems. Incorporating ATT&CK for ICS into analyst workflows provides a common language for describing and categorizing observed activity, enables analysts to map alerts and events to known adversary behavior patterns, and supports the identification of detection gaps where monitoring coverage is limited.

An event that appears benign in isolation may take on considerably more significance when mapped to known adversary techniques and considered alongside CTI relevant to the organization's sector and environment. Organizations should establish processes for routinely cross-referencing active alerts and observed anomalies against current CTI and relevant ATT&CK for ICS techniques so that individual events can be evaluated independently and with the broader threat context relevant to their environment. For example, an individual alert for a stop in controller operation may appear routine, but when observed in sequence with a program download followed by a transition back to run mode, this sequence can be associated with adversary efforts to impair process control.

4.3.2.4. Emerging Detection Capabilities

Technologies (e.g., AI, ML, digital twins) offer advanced detection capabilities that could complement traditional signature-based and threshold-based detection approaches in OT

environments. While adopting these technologies for OT anomaly detection remains limited in current industry practice, organizations should understand both their potential benefits and the security considerations associated with their implementation.

ML-based anomaly detection models could be trained on historical data from the OT environment to establish a baseline of normal behavior and help identify subtle deviations that conventional threshold-based alerts may miss. Digital twins, which maintain a synchronized virtual representation of physical OT assets or processes, could also be used to compare expected behavior with observed conditions and flag potentially anomalous activity.

Organizations should weigh several considerations before evaluating and implementing these technologies. Training and operating AI/ML models requires access to extensive historical and live process data, which expands data collection and retention needs beyond conventional monitoring. The integrity of the training data is also critical, as a model trained on an unrepresentative or compromised baseline may produce unreliable results. These models can also behave non-deterministically and produce different outputs across runs or model versions in ways that may complicate validation and consistency expectations.

Beyond AI/ML models specifically, digital twins carry their own distinct considerations. Their bidirectional connectivity to physical systems for synchronization creates a new attack surface that warrants additional boundary protections in the OT environment. If the twin's underlying model drifts out of sync with the physical asset's actual state, it may also fail to flag genuine anomalies or generate false positives. A compromised twin could further serve as a deception vector, allowing an adversary to manipulate its model or inputs to mask anomalies in the physical system it is meant to monitor.

4.4. Respond (RS)

The Respond Function supports activities for containing a cybersecurity incident when it occurs.

4.4.1. Incident Response

Organizations should establish an OT cybersecurity incident response (IR) function that includes planning, detection, analysis, containment, and reporting activities in the event of a cybersecurity incident. The IR function requires establishing several cybersecurity capabilities, including incident management, forensic analysis, vulnerability management, and response communication. Stakeholders should also review and approve the plan.

NIST IR 8428, *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*, provides a more tailored discussion of OT IR challenges and associated guidance. This includes guidance on the composition and roles of incident response teams, tools and resources needed to support IR activities, training requirements, and an overall framework for managing cybersecurity incidents. This resource can support and inform the development of IR capabilities within an organization.

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

- IR 8428, *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*
- SP 800-61r2, *Computer Security Incident Handling Guide*
- SP 800-83r1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
- SP 800-100, *Information Security Handbook: A Guide for Managers*
- CISA, Handling Destructive Malware
- Federal Emergency Management Agency (FEMA) National Incident Management System (NIMS)
- FEMA National Preparedness Goal
- SANS ICS Cybersecurity Field Manuals, Volume 3
- Patrick Kral. Incident Handler's Handbook. December 2011, SANS Institute
- ICS4ICS Incident Command System for Industrial Control Systems (https://www.ics4ics.org)

4.4.2. Incident Response Planning

As part of building the IR function, the OT cybersecurity department should create an incident response plan that applies to all OT personnel, networks, systems, and data. The purpose of the incident response capability is to determine the scope and risk of cybersecurity incidents, respond appropriately to them, communicate the incidents to all stakeholders, and reduce their future impacts. Response plans should be measured against the service being provided, not just the compromised system. 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].

During the preparation of the incident response plan, input should be obtained from various stakeholders, including operations, engineering, IT, system support vendors, management, organized labor, legal, and safety. Common IR planning steps include preparation, detection and analysis, containment, recovery, post-incident activity, communication, and coordination. . Personnel should be trained on where to find the response plan and the actions to take as part of an incident response. Organizations should also regularly review and update their response plans. Response plans should be documented on paper or on an offline system (e.g., air-gapped) that cannot be compromised during a cyber attack.

Response plans include personnel roles and responsibilities as well as:

- Identification and classification of incidents. Various types of OT incidents should be identified and classified based on their potential impact so that a proper response can

be formulated for each. This classification may inform who needs to be notified and what response and recovery actions should be taken. Additionally, many sectors have regulatory requirements regarding what constitutes a cybersecurity event and the necessary reporting that must be done when one occurs. Organizations should ensure that the classification procedures adequately address possible regulatory requirements.

- Response actions. Incident response can range from doing nothing to performing a full system shutdown, which could result in a shutdown of the physical process. The response taken will depend on the type of incident and its effect on the OT system and the physical process being controlled. A written plan documenting the response to each incident type should be prepared. This will provide guidance if confusion or stress arise due to the incident. This plan should include step-by-step actions to be taken by various stakeholders.
- Reporting requirements should be documented along with contact information and the reporting format to reduce confusion.
- Response actions should also include steps for detection, analysis, containment, eradication, recovery, and post-incident activity. Some considerations for OT may include:
    - Determining a priority, such as returning to normal operations as quickly as possible, or performing an investigation and preserving forensic data
    - Communicating with the incident response team
    - Disconnecting infected systems from the network
    - Physically isolating operationally independent networks (e.g., enterprise from control, 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
    - Defining appropriate approaches, procedures, and tools to eradicate threat actors from OT environments and devices
    - Identifying the necessary capabilities to collect evidence for OT devices, including what tools and systems would be used and what evidence would be collected
- Requirements for engaging external incident response teams to support the response efforts should be defined, and the plan should clarify who has the authority to bring in the external team and establish rules and procedures for providing access to organizational resources.

Even when preventive maintenance is performed, equipment malfunctions and failures remain common in industrial and OT environments. Because many systems were designed and deployed before current cybersecurity threats were widely considered, abnormal behavior or

equipment failure may initially be attributed to routine mechanical, electrical, software, or process-related causes rather than to potential malicious activity. In addition, OT incidents often lack clear initial cyber indicators (e.g., ransomware messages, malware IOCs), especially in organizations without strong OT monitoring and detection capabilities. When outages or disruptions occur with unknown root causes, organizations may suspect a cyber intrusion and begin initial incident analysis steps before a cyber incident has been clearly confirmed.

As a result, organizations may prioritize the rapid restoration, replacement, or rebuilding of affected components, inadvertently destroying or altering valuable forensic data. Operations, maintenance, engineering, and cybersecurity personnel should coordinate to establish practical procedures for identifying failures that may warrant additional cyber-related review, preserving relevant data where feasible, and supporting incident response while minimizing operational burden and unnecessary false positives. Historical failure data can serve as a useful starting point for establishing a baseline or normal failure threshold for critical devices. NIST IR 8428 provides additional guidance on event identification, particularly the need for situational awareness among both cybersecurity analysts and OT engineers when alerts or anomalies are detected. Figure 16 illustrates a workflow that demonstrates how incidents may originate from an SOC analyst or operational staff (referred to as the Facility Control Room in the figure), thereby requiring coordination between both groups to ensure that incidents are properly identified.

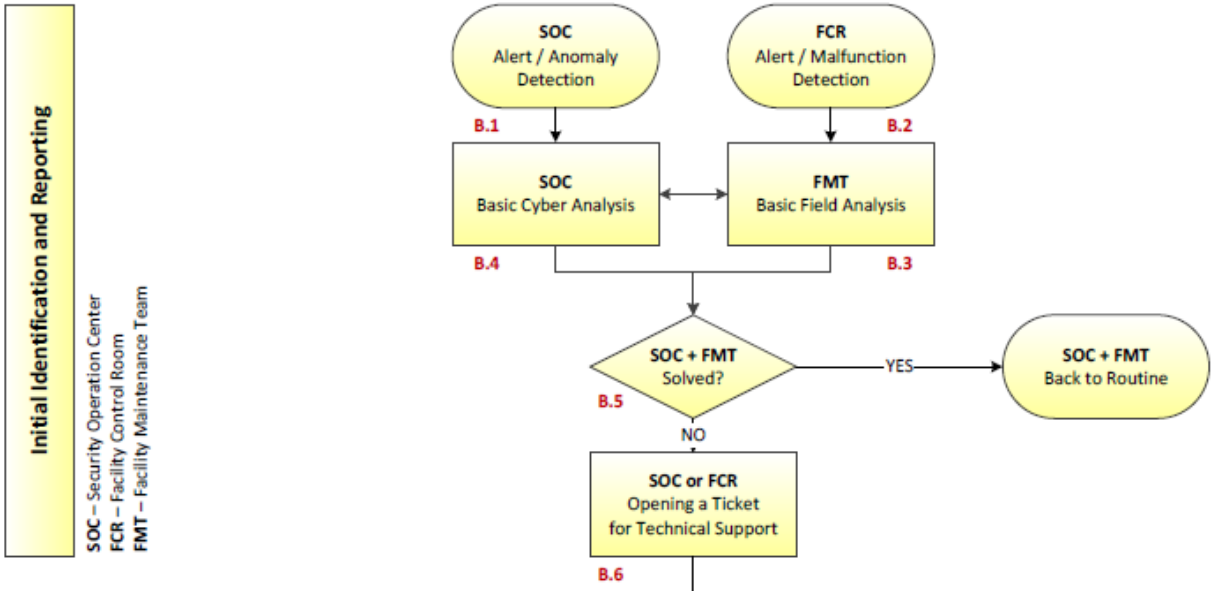

Fig. 16. Initial identification and reporting [IR8428]

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.

In addition to developing incident response plans, organizations may want to develop predefined playbooks for common OT scenarios, such as ransomware, insider threats, and malware on critical OT devices. Playbooks can provide more detailed, step-by-step guidance on

how to respond to specific scenarios, including processes for forensic analysis and threat eviction, which can improve response actions and minimize operational impacts.

IR plans are only effective if personnel know about them and receive periodic training. Tabletop exercises are important to ensure that staff understand the plan and to determine whether the plan effectively covers and informs key decisions and processes through a scenario. Periodic exercises should be performed across different hypothetical scenarios to evaluate the effectiveness of the IR plan and identify where the plan should be improved.

Additional information with specific examples for OT incident response is also provided in NIST IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide* [IR8183A], Sec. 6.2.4.5.

4.4.3. Incident Management (RS.MA)

If an incident is discovered, organizations should assess the risk to the OT environment to evaluate the attack's effects and available response options. For example, one possible response option is to physically isolate the system under attack. However, this may negatively affect the OT and may not be possible without compromising operational performance or safety. It may also affect the organization's ability to conduct incident response activities if the system is remote or if remote personnel are assisting.

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

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

4.4.4. Incident Analysis (RS.AN)

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

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 depend on IT for business applications, so an incident on the IT network can result in an OT disconnect or shutdown.

Traditional IT forensic tools may not work on OT systems and devices. Organizations should therefore establish and test procedures for performing necessary forensic activities in OT environments, including the collection of configuration data and the extraction and validation of programs. If an organization does not have adequate resources or capabilities to conduct OT forensics, consider engaging external organizations to perform forensic analysis.

Organizations should identify and classify cyber and non-cyber incidents that affect the OT environment in accordance with 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.

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

- SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- IR 8428, *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)*

4.4.5. Incident Response Reporting and Communication (RS.CO)

Responding to a cybersecurity incident includes coordinating with internal and external stakeholders. An incident response team should be assembled. Depending on the complexity and impact of the incident, the incident response team could consist of one or many individuals who have been trained on incident response.

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

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

The response plan should include a detailed list of organizations and personnel that should be contacted for incident response and reporting under various circumstances. Each individual should be assigned roles that are required for incident response, which could include incident commander; operations, planning, logistics, or finance/administration section chief or member; and public information, safety, or liaison officer. The personnel responsible for responding to an incident should be informed of and trained on their responsibilities.

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

- **Internal Resources**

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

- **External Industry Partners**
  - OT technical support (e.g., vendors, integrators)
  - Operational supply chain (e.g., suppliers, customers, distributors, business partners)
  - External incident response team
  - Surge support
  - Impacted community (e.g., facility neighbors)
  - Regulatory organizations

Organizations should establish procedures to identify and satisfy all applicable incident reporting requirements, including those necessary to support federal statutes, executive policy, agency directives, sector-specific regulations, contractual requirements, and other legal authorities. For organizations that support critical infrastructure, reporting procedures should align with the roles and responsibilities established under National Security Memorandum 22 (NSM-22) and applicable guidance from CISA and the appropriate Sector Risk Management Agency (SRMA).

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

4.4.6. Incident Mitigation (RS.MI)

Mitigation activities are meant to prevent the expansion of an incident, alleviate its effects, and resolve the incident, and they should be consistent with the response plan. 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 to minimize impacts until personnel arrive on-site (e.g., remote shutdowns, disconnects).

Cyber incident mitigation and eradication may involve process shutdowns, communication disconnects, or emergency isolation of affected systems that may impact operations and therefore require approval from senior leaders. The organization should explore these possible mitigation and eradication procedures, ensure that their broader impacts on operations are understood, and ensure that the processes and approvals required to authorize these decisions are well-defined. Human safety must take precedence over system preservation when implementing these mitigations, particularly during incidents that pressure system operators to isolate systems quickly (e.g., ransomware), increasing the risk of abrupt decisions that do not account for the physical process state. When implementing these mitigations, organizations should consider not only the core OT devices but also the devices and platforms used to manage the OT environment.

4.5. Recover (RC)

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

4.5.1. Recovery Planning

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

- Define recovery objectives when recovering from disruptions. For example, the recovery capability should prioritize human and environmental safety before restarting the OT operation impaired by the cybersecurity event.
- Develop a site disaster recovery plan (DRP) and business continuity plan (BCP) to prepare the OT organization to respond appropriately to significant disruptions in their operations due to the cybersecurity incident.
- Maintain an inventory of necessary spare devices to restore operations, including on-site spares and supplier contracts for expedited delivery.
- Establish processes for restoring relevant OT systems' state, data, configuration files, and programs from backups in a timely manner.
- Establish recovery processes and procedures that will be executed to restore the OT assets and services affected by cybersecurity incidents.
- Establish communication plans to coordinate restoration activities with internal and external stakeholders and the executive management team.

- Establish communication plans to manage public relations.
- Establish a lessons-learned task as part of the recovery process to continuously improve cybersecurity capabilities (e.g., vulnerability management, cybersecurity operations, incident response, recovery).
- Test these plans at reasonable intervals that are appropriate for the organization.

Business continuity planning addresses the overall issue of maintaining or reestablishing production in the case of an interruption. Recovery time can vary widely depending on the cause. For example, a natural disaster may take days, weeks, or months to recover from, while a malware infection or a mechanical or electrical failure may take only minutes or hours. BCPs are often written to cover many types of incidents that involve several different disciplines. The BCP for cybersecurity incidents should broadly cover long-term outages (e.g., disaster recovery) and short-term outages that require operational recovery. It is important to work with physical security to develop the BCP for cybersecurity incidents. This collaboration with physical security should include identifying critical equipment and the associated countermeasures in place to prevent incidents. Before creating a BCP to address potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs.

There are two distinct types of objectives: system recovery and data recovery. System recovery involves restoring communication links and processing capabilities and is usually specified in terms of a recovery time objective (RTO). Management should define the acceptable RTO, and technical personnel should work to achieve that target. Data recovery involves recovering data that describes past production or product conditions and is usually specified in terms of a recovery point objective (RPO). This is defined as the time for which an absence of data can be tolerated. The RTO and RPO may justify investment in spare inventory if recovery objectives cannot be met by other means. Once the recovery objectives are defined, a list of potential interruptions should be created, and the recovery procedure should be developed and described. A contingency plan is then created for the variety of potential interruptions. The contingency plan should be reviewed with managers to ensure that the cost of meeting the contingency plan is approved. For many smaller-scale interruptions, a critical spares inventory will likely prove adequate to meet the recovery objectives. For larger-scale recovery, vendor relationships will likely be leveraged. For all types of recovery, backups are critical.

A disaster recovery plan (DRP) is a documented process or set of procedures that comprises a comprehensive statement of recovery actions to be taken before, during, and after a disaster. The DRP is ordinarily documented in both electronic and paper form to ensure that it is readily available during any type of disaster (e.g., natural, environmental, caused by humans). Organizations should develop, maintain, and validate disaster recovery plans for their environments to help minimize the impact of an event by reducing the time required to restore capabilities. Organizations may already have some emergency response plans in place and should consider leveraging existing plans when developing a response plan for cybersecurity events.

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

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

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

- SP 800-184, *Guide for Cybersecurity Event Recovery*
- SP 800-209, *Security Guidelines for Storage Infrastructure*
- IR 8183A, *Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide*
- SP 800-34r1, *Contingency Planning Guide for Federal Information Systems*

4.5.2. Incident Recovery Execution (RC.RP)

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

OT systems often have strict sequencing and timing requirements for restart that must be followed to avoid unsafe conditions. Recovery plans should document these dependencies, including restart order and required validation checks. These plans should be developed in coordination with control engineers who understand the consequences of restoring systems out of sequence.

Organizations should also protect OT backups from tampering (e.g., encryption) or deletion by storing them in a production environment using immutable mechanisms that cannot be altered or destroyed by malware. Recovery plans should specify how backup integrity is validated before restoration begins to ensure that clean backups are not inadvertently replaced with compromised data during the recovery process.

4.5.3. Recovery Communication (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.

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

- **Internal Communications**
  - OT personnel
  - IT personnel
  - Procurement
  - Management with appropriate authority to approve the cost of recovery
  - Storage or warehouse personnel
- **External Communications**
  - OT vendors
  - Security companies that may be held on retainer for response and recovery efforts
  - Storage or warehouse personnel
  - Internet service providers
  - Owners of the attacking systems and potential victims

During or after a cyber incident, the primary communication infrastructure may be unavailable or compromised. Organizations should develop and maintain a backup communication plan to ensure that coordination can continue through alternative means. A PACE plan (Primary, Alternate, Contingency, and Emergency) provides a structured framework for defining communication methods at each level of degradation. Organizations should pair this with pre-established point-of-contact trees to ensure that personnel know who to reach and what mechanism to use when primary channels become unavailable. Supply chain partners and critical vendors should also be included in out-of-band communication planning, as their support may be essential to recovery and their primary communication channels may be similarly affected.

Supplemental guidance for recovery communications can be found in SP 800-184, *Guide for Cybersecurity Event Recovery*.

5. OT Cybersecurity Architecture

When designing a security architecture for an OT environment, it is generally recommended to separate the OT network from the enterprise network. The nature of network traffic on these two network types differs significantly. Internet access, email, and remote access are typically permitted on the enterprise network but not allowed on OT networks. There may also be differences in the degree of rigor associated with enterprise and OT environment change control procedures. Additionally, using the enterprise network for OT communication protocols could expose OT components to cyber attacks, such as the denial of service, adversary-in-the-middle, or other network-based attacks. Utilizing separate networks allows for greater flexibility to address the security and performance requirements of each environment independently.

This separation should extend beyond the boundary between enterprise and OT networks. Within the OT environment itself, networks that serve different functions and purposes warrant their own segmentation. Operational networks (i.e., those that carry process control traffic between supervisory systems and field devices) have fundamentally different traffic characteristics, availability requirements, and security properties than networks dedicated to management functions, such as configuration, patching, and access control. Combining these on a shared network infrastructure may introduce risk to operational traffic from management activity, limit the ability to apply independent security policies to each function, and create conditions in which a security event that affects one network type can propagate to the other. Additionally, external parties (e.g., vendors, other third parties) should have access paths that are architecturally separate from both operational and internal management traffic with their own credential stores, entry points, and enforcement boundaries so that the trust level extended to external access does not inadvertently reach internal functions through shared infrastructure.

Practical considerations (e.g., digital transformation, the cost of OT installation, maintaining a homogenous network infrastructure) often mean that connections are required between OT networks and other IT networks. These connections represent additional risk, and organizations should seek to minimize them and implement additional security controls where they exist. This section identifies a representative set of functions, security controls, and architecture patterns for organizations to consider when engineering their OT environments to support the cybersecurity objectives described in Sec. 4.

5.1. Summary of Cybersecurity Capabilities

This section presents the functions and architectural patterns that support a defensible OT cybersecurity architecture, organized into three categories.

OT/ICS system management (Table 7) and security controls (Table 8) are functions: discrete operational capabilities that produce a specific security-relevant outcome. System management functions establish and maintain visibility into managed assets and govern the introduction of change. Security controls enforce protection at points where access, transfer, or observation occurs. Architecture patterns (Table 9) are distinct from these functions. Rather than performing an operation, an architecture pattern defines the structural context in which

functions are deployed and enforced, determining where a given function applies and what it is permitted to reach.

Each function and pattern addresses one or more outcomes defined in the OT Cybersecurity Outcomes and Objectives framework referenced throughout this document and was selected for its role in mitigating risk characteristics of OT environments, including insufficient asset visibility, uncontrolled configuration drift, ungoverned content ingress, propagation of credential compromise across trust domains, and the absence of independent, tamper-resistant monitoring.

No individual function or pattern is sufficient in isolation. System management and security controls are interdependent: system management provides the visibility and governance records that security controls act on. Architecture patterns establish the structural conditions that require clearly defined boundaries, controlled and auditable access paths, and assurance that compromise of one component does not silently defeat protections implemented elsewhere.

Table 7 through Table 9 identify each function and architecture pattern, together with a description and reference to related guidance presented elsewhere in this document. Section 5.2 presents representative example architectures demonstrating how these may be composed, sequenced, and enforced in combination.

Not every item identified in Table 7 through Table 9 will be applicable to every environment. Asset owners and operators should evaluate applicability against the criticality of the assets being protected, the operational constraints of the environment, and organizational risk tolerance, consistent with the risk-informed approach described throughout this document.

Table 7. Example OT/ICS system management

Function	Description
Asset Management	Building on the asset inventory concepts addressed in Sec. 4.1.1.1, the asset management function maintains a continuously updated record of every managed device: its identity, firmware, configuration, and security state.
Industrial Code Management	Changes to industrial code should move through a defined workflow that includes authoring or receipt, review, approval, and controlled deployment, extending the secure coding and change-control practices discussed in Sec. 4.2.3.4.
Configuration Management Database	The CMDB is the governance record for the asset inventory, reflecting the configuration management concepts addressed in Sec. 4.2.3.1.
Work Order Integration	The work order function integrates with asset management, code management, and access management to create a complete audit record for every authorized touch to a managed asset, consistent with the maintenance tracking capability described in Sec. 4.2.3.1.
Update Services and Vendor Patch Delivery	Many vendors offer software update services (i.e., platforms that maintain a connection to a vendor server to retrieve approved firmware, software updates, and security patches on demand or on a schedule) following the patch management approach outlined in Sec. 4.2.3.1.

4129 **Table 8. Example security controls**

Function	Description
File Transfer — General Content Ingestion	Content should undergo antivirus scanning, file type validation, and integrity checking before it is permitted to proceed, mirroring the endpoint monitoring guidance in Sec. 4.3.1.2.
Bidirectional Transfer — Outbound Content and Vendor Data Access	Outbound content should be routed through the same controlled infrastructure used for inbound content in line with the remote access control principles introduced in Sec. 4.2.1.8.
Removable Media and Portable Devices — USB Kiosk Workflow	A USB scanning kiosk should serve as the mandatory entry point for removable media before it is permitted to connect to any field device, engineering workstation, or other asset, building on the media protection concepts addressed in Sec. 4.2.2.3.
Credential Separation	Credentials should be maintained separately across trust domains, as discussed in the identity convergence and centralization guidance in Sec. 4.2.1.5.
Privileged Access Management	Privileged access should be mediated through an access manager that enforces least-privilege entitlements, time-bounded session authorization, and session recording with live termination capability, as addressed in Sec. 4.2.1.7.
Passive Network Monitoring	Passive network monitoring sensors deployed via span ports or network taps extend the passive monitoring concepts introduced in Sec. 4.1.1.1.
Log Collection and Telemetry	Telemetry should flow one-way outbound to a central collection point, mirroring the device logging guidance discussed in Sec. 4.3.1.1.

4130 **Table 9. Example architectural patterns**

Architecture Pattern	Description
Access Architecture	The design and operation of a full access management architecture build on the remote access control principles introduced in Sec. 4.2.1.8.
DMZ and the Two-Firewall Architecture	A two-firewall DMZ architecture separates trusted infrastructure from untrusted external connections with traffic routed through it rather than crossing directly between planes, consistent with the boundary protection principles discussed in Sec. 4.2.1.8. Without this separation, a single set of firewall rules must accommodate both trust levels and is, therefore, necessarily broader than either requires.
VPN Gateways and Remote Site Connectivity	Remote sites and remote users should reach protected infrastructure through VPN gateways terminating in a DMZ rather than connecting directly, thus building on the data-in-transit protections described in Sec. 4.2.2.4. Persistent VPN tunnels with poor authentication can be exploited by attackers to gain network access using otherwise-blocked paths.
Intra-Site Segmentation and Field-Facing Gateways	Segmentation should separate distinct network zones from one another, each governed by its own access control list and firewall policy, to reflect the authorization and logical access control practices addressed in Sec. 4.2.1.7. Without this internal segmentation, a

Architecture Pattern	Description
	foothold gained anywhere on the site-level network has unrestricted reach across every zone.

5.2. Cybersecurity Architecture Models

Building on the concepts and guidance from Sec. 4, the following subsections expand on the management network described in Sec. 5.1 as well as the operational networks described in Sec. 2. They provide examples for how these environments might be adapted to incorporate the functions, security controls, and architecture patterns identified above.

5.2.1. Management Network Architecture

Separating OT from the enterprise network is a baseline architectural practice. The two networks carry fundamentally different traffic, tolerate different levels of risk, and are subject to different change control rigor. Combining them exposes OT components to network-based attacks that enterprise traffic would otherwise absorb. This same logic extends inside the OT environment itself. Operational traffic (i.e., supervisory-to-field-device communication) has different availability requirements and traffic characteristics than management traffic, such as configuration changes, patching, and access control sessions. Running both on shared infrastructure lets management activity introduce risk to operational traffic, prevents an independent security policy per function, and allows a security event on one to propagate to the other.

The management network exists to give these functions the isolation that separation requires. It provides the connectivity, credential domain, and audit posture that asset management, code management, and monitoring need without exposing that access on the operational network, where broad device connectivity would otherwise sit unguarded on infrastructure designed only for deterministic process traffic. An attacker seeking a physical impact must establish separate footholds in networks that each require their own credentials and have their own enforced boundary, which materially raises the cost and detectability of an attack. Vendor and third-party access follows the same principle: external connections use their own credential stores and entry points that are architecturally separate from internal management traffic so that the trust extended externally cannot reach internal functions through shared infrastructure.

Figure 17 illustrates the management network architecture relative to the operational network, the enterprise network, and external vendor connections, including asset and code management, configuration governance, patch and update management, identity and access management, and security monitoring.

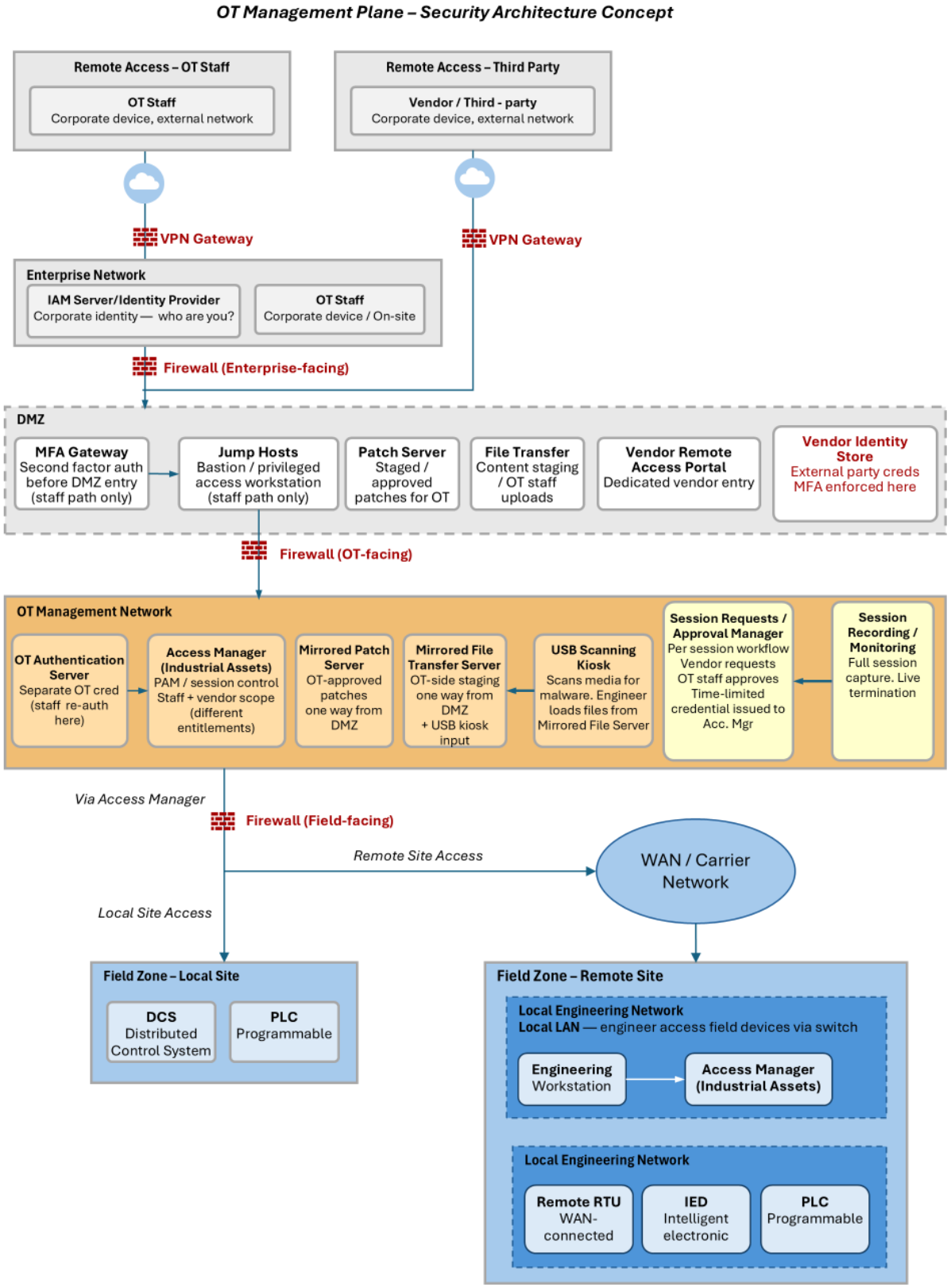

Fig. 17. Network management security architecture

Where connections between OT and enterprise or other IT networks are operationally necessary, they represent additional risk and should be minimized and controlled rather than treated as routine. For network security, the organization should consider incorporating the following capabilities into the security architecture:

- The management network is separated into zones based on function. Asset management, industrial code management, and the configuration management database occupy one zone; patch staging and file transfer occupy a second; identity and access management infrastructure occupies a third; and security monitoring occupies an isolated zone with no staff access path.
- Asset management and code management connectivity is restricted to the management network. Both functions require active, write-adjacent connectivity to read and validate device state or running logic. The asset management platform holds a complete inventory and vulnerability picture, and the code repository holds every authorized version of device logic, making both high-value targets that are not reachable from the operational network directly. Access to field devices for these functions routes through the engineering network and a field-facing gateway rather than a direct path.
- Boundary devices (e.g., firewalls) control and monitor communications between zones. Rules define authorized traffic per function rather than a shared rule set across the management network.
- A two-firewall DMZ architecture separates the management network from both the enterprise network and untrusted external connections. Vendor update services are staged in the DMZ rather than run directly in the management network. If DMZ staging is not available, the update client is restricted to a tightly scoped outbound rule that permits only the specific vendor endpoint, documented as a risk acceptance.
- All file transfers route through a DMZ-hosted file transfer server as the exclusive sanctioned ingestion path. Content is scanned for malicious code, validated by file type, and integrity-checked before reaching the management network. Content that fails validation is quarantined within the DMZ. Outbound content (e.g., logs, diagnostics, configuration exports) routes through the same DMZ infrastructure rather than a separate path.
- A USB scanning kiosk serves as the mandatory entry point for removable media and engineer laptops before either is permitted to connect to any field device, engineering workstation, or other management-network asset. Media that passes scanning may be loaded with content from the mirrored file transfer server so that files placed on it are the same files that passed DMZ validation, rather than files sourced externally.
- A dedicated OT authentication server resides within the management network, distinct from enterprise directory services, so that a compromised enterprise credential cannot grant access to the management infrastructure.
- All privileged access is mediated through an Access Manager who enforces least-privilege entitlements, time-bounded session authorization, and session recording with

live termination capability for every privileged session against a managed asset. Staff and vendor access paths are architecturally distinct (e.g., separate entry points, credential stores, firewall policy lanes, and entitlement profiles) with just-in-time approval required for vendor and third-party access before any session is established. Standing, always-on vendor access is avoided. If it cannot be eliminated, it is formally risk-accepted and continuously monitored. Because a compromise of this infrastructure affects the authorization layer for every managed device rather than any single one, it is treated as a high-value target in its own right.

- Security monitoring infrastructure resides in its own isolated zone that is reachable only via one-way telemetry feeds from the other management zones so that monitoring data and infrastructure are not accessible through the same paths used for management operations.

5.2.2. Operational Network Architecture

The operational network carries process control traffic (i.e., traffic that is deterministic, latency-sensitive, and essential to safe and reliable operation of the physical process) between supervisory systems, distributed field controllers, and the sensors and actuators they command. This traffic differs fundamentally from enterprise network traffic (e.g., internet access, email, remote access) and from management network traffic (e.g., configuration changes, patch delivery, administrative access). Running any of this alongside operational traffic exposes OT components to network-based attacks (e.g., denial of service, adversary-in-the-middle) that the operational network was never designed to withstand.

Isolating the operational network preserves the narrow, predictable traffic envelope that makes it a high-signal environment for anomaly detection. Deviations from expected process communication are easier to identify precisely because nothing else is competing for that bandwidth or introducing variable traffic patterns. It also directly limits the attacker's capabilities. Supervisory and field-level functions operate within a defined operating envelope (e.g., control logic, setpoints, process limits), and an adversary confined to the operational network is constrained by that same envelope. Changing the envelope itself requires reaching the management network, so an attacker seeking consequential physical impact must establish and maintain separate footholds in each, defeating a separately enforced boundary for each one.

The specific architecture of the operational network varies with the type of control system deployed. The following sections address these considerations as they apply to Distributed Control System (DCS)-Based OT Systems and SCADA-Based OT Environments.

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

A distributed control system (DCS) is used to control production systems within the same geographic location by organizing the network into separate functional areas, such as:

- A field level with devices typically associated with Purdue Levels 0, 1, and 2

- An operations management level with devices used to monitor and manage field devices and Purdue Level 3 components
- A DMZ with devices that support communication between the operations management level and enterprise systems

Additional network segments may also be used for systems, such as:

- Physical monitoring and access controls
- Doors
- Gates
- Cameras
- Voice over Internet Protocol (VoIP)
- Access card readers

Boundary devices (e.g., firewalls) can be placed between these areas to control and monitor communications. Industrial-class firewalls may be used between field devices and operations management systems to support OT-specific protocols or to operate in harsh environments. Inbound and outbound rules should be defined so that only authorized communication passes between adjacent areas.

A DMZ can be used to separate the OT environment from the enterprise network. Communications between enterprise systems and operations management systems should pass through services located in the DMZ rather than directly between the two environments. Because the DMZ connects to outside environments, the services within it should be monitored and protected to reduce the chance that a compromise in the DMZ could be used to reach the OT environment.

Some architectures may use separate authentication services for enterprise and OT users, such as:

- An IT authentication server in the enterprise network
- An OT authentication server in the operations management network

Devices in the field level, operations management level, and DMZ should be configured to only use the capabilities required for their purpose. Non-essential software, services, and ports should be identified and disabled. For example, if a PLC or HMI contains a web server or SSH server that is not needed, that service and its associated TCP/UDP ports should be disabled.

Figure 18 shows a security architecture example for a DCS system.

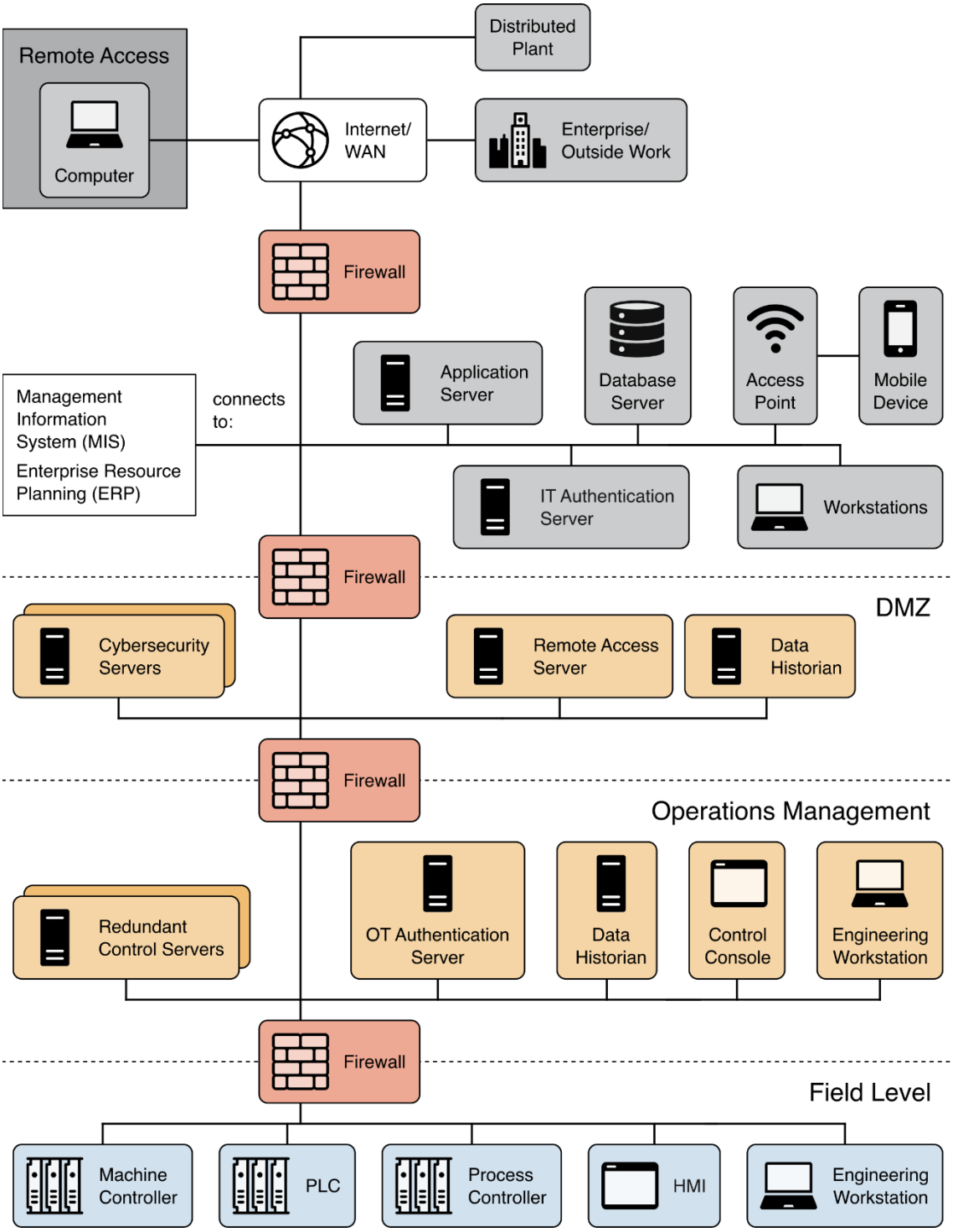

Fig. 18. A security architecture example for a DCS system

5.2.2.2. DCS- and PLC-Based OT With IIoT

When DCS- and PLC-based OT environments include IIoT devices, the architecture may be expanded to support the additional communication and processing needs of those devices. For example, IIoT devices may be connected to a local IIoT platform that provides computing capabilities. Because IIoT introduces different communication and architectural components, separate network segments may be used for those components.

Communication from the IIoT platform tier can be routed through a DMZ border firewall. This allows organizations to support data transmission to:

- Servers in the DMZ or
- The enterprise or internet, as needed for IIoT operational requirements.

This also allows cybersecurity services located in the DMZ to monitor the IIoT platform tier.

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.

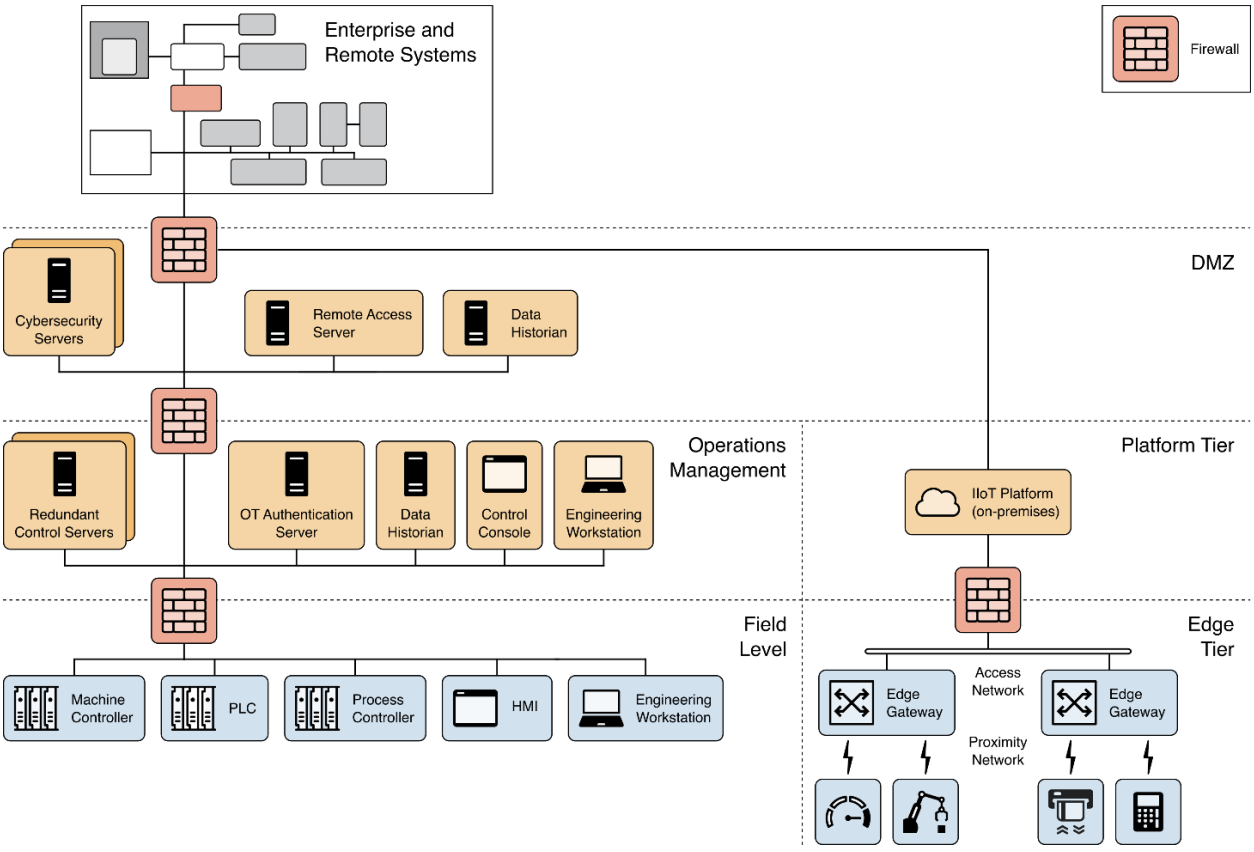

Fig. 19. A security architecture example for DCS system with IIoT devices

5.2.2.3. SCADA-Based OT Environments

A SCADA environment often includes primary and backup control centers, regional control centers, and remote stations in different geographic locations. Because these components are distributed, communication between locations often passes over external or WAN connections using wired or wireless media. The network can be divided into different zones or regions. Additional separation may also be used for systems, such as:

- Physical monitoring and access controls
- Doors
- Gates
- Cameras
- VoIP
- Access card readers

Boundary devices (e.g., firewalls) can be placed between regions to control and monitor communications between network segments. Industrial-class stateful firewalls may provide better support for OT-specific protocols and may enhance protection for OT devices, such as PLCs and controllers. Inbound and outbound rules should be defined so that only authorized communication passes between regions.

Secure connections should be used between network segments, such as:

- VPN tunnels
- Encrypted channels
- Point-to-point connections

These secure connections may be used:

- Between a regional center and primary control centers
- Between remote stations and control centers

For geographically distant locations, these secure connections may traverse the internet or a wide area network. Devices in each network segment should only connect to other segments through the secure connection, and direct internet access should be restricted.

A DMZ can also be used to separate control centers from the enterprise network. Communications between the enterprise network and control centers should pass through services within the DMZ. Those services should be monitored and protected to prevent them from becoming a path into the OT environment.

Remote station components, control center components, and DMZ devices should be configured to support only necessary functions. Non-essential software, services, and ports should be identified and disabled. For example, if a newer PLC or HMI includes a web server or SSH server that is not required, it should be disabled along with the associated TCP/UDP ports.

Fig. 20 shows an example implementation of the components and general configuration of a SCADA system.

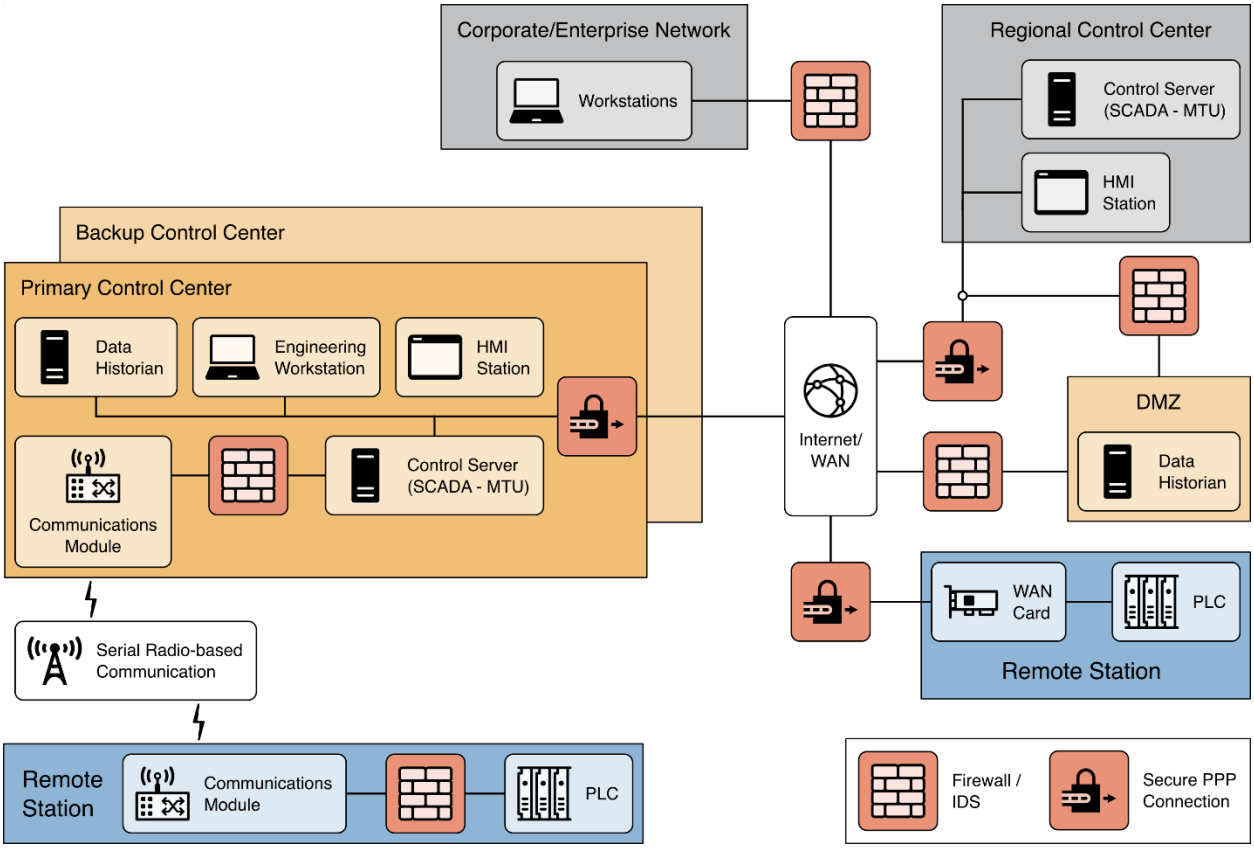

Fig. 20. A security architecture example for a SCADA system

5.3. Integrating Zero Trust Principles in OT

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

Several of the functions and controls described throughout this document already embody core zero trust principles and can serve as an organization's practical starting point for a broader ZTA implementation rather than requiring a separate initiative:

- Continuous, per-session authorization rather than implicit trust. Privileged access management (see Sec. 4.2.1.7) is the clearest expression of zero trust. The Access Manager evaluates and authorizes each privileged session individually to enforce least-privilege entitlements, time-bounded authorization, and live session termination rather than granting standing trust once a user reaches the network. Extending this same continuous-evaluation model to non-privileged access is a natural next step in a ZTA implementation.
- Strong, verifiable identity as the basis for authorization decisions. Credential separation (see Sec. 4.2.1.5) ensures that identity verification for OT network access does not inherit trust from the enterprise identity domain. A dedicated OT authentication server gives a ZTA policy engine an identity source that it can evaluate independently rather than one in which a compromised enterprise credential could satisfy an OT authorization check.
- Content-level verification rather than perimeter trust. File transfer controls (see Sec. 4.3.1.2) and removable media controls (see Sec. 4.2.2.3) apply zero trust logic to content rather than users. Nothing is trusted by virtue of having reached the DMZ or passing the USB kiosk once. Each artifact is scanned, validated, and quarantined on failure before it is trusted for use.
- Continuous monitoring as the enforcement feedback loop. Security monitoring (see Sec. 4.3.2.1) supplies the continuous observation that a ZTA model depends on to revoke or adjust trust in near real-time rather than relying on a one-time authorization decision made at the start of the session.

Some challenges to implementing a ZTA include:

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

5.3.1. OT-Specific Recommendations and Guidance

Many OT components (e.g., PLCs, controllers, HMIs) do not support the technologies or protocols required to fully integrate with a ZTA implementation. Therefore, organizations should consider applying a ZTA to compatible devices, such as those typically found at the functionally higher levels of the OT architecture (e.g., Purdue model Levels 3, 4, 5; OT DMZ). This corresponds closely with the functions addressed in Sec. 4.2.1.7, 4.2.1.5, 4.3.1.2, 4.2.2.3, and 4.3.2.1, where the controls already provide much of the necessary foundation.

Organizations may also want to consider whether any adverse impacts might occur, such as if the ZTA solution increases the latency to respond to resource requests or if one or more ZTA components become unavailable. Based on this analysis, organizations should consider adjusting the ZTA implementations to minimize latency and ensure adequate redundancy to minimize risks to OT and safety operations.

Another important aspect of ZTA implementations is the identity of person and non-person entities accessing resources. Within OT environments, shared credentials may be utilized, which could impact the ability to fully implement a ZTA solution. This reinforces the importance of credential separation control (see Sec. 4.2.1.5) and privileged access management control (see Sec. 4.2.1.7) as preconditions for meaningful ZTA adoption.

5.4. Designing for Security, Safety, and Resilience

The functions, security controls, and architectural patterns described in this section reduce the likelihood that a given threat will succeed. They do not, on their own, ensure that operations continue when a component fails or a control is defeated. The following design principles address that separate concern: ensuring that the OT environment degrades gracefully, recovers predictably, and remains manageable even when primary systems or paths are unavailable.

5.4.1. Fault Tolerance as an Architectural Design Principle

Fault tolerance is the property of a system to continue operating when a component fails rather than failing outright, potentially at a reduced level. In OT environments, fault tolerance is a design principle: a failed component should fail in a manner that does not generate unnecessary traffic, cascade to other systems, or leave the process in an unsafe state. This differs meaningfully from IT environments, in which momentary downtime is typically an acceptable and recoverable event. In OT, momentary downtime may be unacceptable because it could directly affect a physical process. Architectures should support graceful degradation (i.e., moving from full automation to increasingly manual modes of operation) so that a fault reduces functionality rather than availability entirely.

Guidelines on engineering resilient systems, including fault-tolerant design, are provided in SP 800-160v2r1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, which defines resilience techniques and design principles applicable to OT and other cyber-physical systems.

5.4.2. Redundancy Addressed as an Architecture-Level Design Principle

Redundancy supports fault tolerance by ensuring that no single point of failure can interrupt a critical function. Redundancy should be addressed at the architecture level rather than the component level. Critical components should have a redundant counterpart on a redundant network path, and any redundant communication path should be protected to the same security level as the primary path it backs up. Architecture-level redundancy also extends to identity and access infrastructure and monitoring infrastructure. A redundant authentication

server or monitoring collector that shares the same failure domain as its primary provides limited additional resilience.

Redundancy requirements should be scoped to the criticality of the asset or function being protected, consistent with an organization's risk tolerance, rather than applied uniformly across the environment. The architectural treatment of resilience and redundancy is addressed in SP 800-160v2r1.

5.4.3. Analog Backups

If a process can be safely operated using non-digital instrumentation and controls, maintaining an analog backup (e.g., hardwired instrumentation, physical gauges, manual control stations that do not depend on the digital control system) provides a recovery path that is unaffected by a cyber incident against the digital environment. Analog backups are most relevant for safety-critical or highly critical processes for which the consequences of extended digital system unavailability are unacceptable. They should be evaluated as a complement rather than a replacement for digital backup and restoration processes.

Digital backup and restoration practices (e.g., layered, time-sequenced "backup-in-depth" approach with local, facility, and disaster-recovery backups) are addressed at a general level in SP 800-82r3, Sec. 5.3.2.1. Broader contingency planning guidelines, including backup strategy selection and testing, is provided in SP 800-34r1, *Contingency Planning Guide for Federal Information Systems*.

5.4.4. Out-of-Band Management as an Architectural Concept

Out-of-band management provides an administrative access path that is physically or logically separate from the primary data path used for normal operations. Where implemented, management traffic (e.g., access to boundary devices, the Access Manager, and monitoring infrastructure) does not traverse the same network segments as operational or enterprise traffic, so a compromise of the in-band path does not also compromise the ability to administer or recover the environment. This separation is particularly relevant to the management network architecture since an out-of-band path preserves the ability to manage boundary devices and recover monitoring infrastructure even if the in-band management network is degraded or unavailable.

References

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

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

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

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

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

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

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

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

[CIE] Cyber-Informed Engineering (CIE). U.S. Department of Energy (DOE). Available at: https://www.energy.gov/ceser/cyber-informed-engineering

[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

[CISA-PACE] Cybersecurity and Infrastructure Security Agency (CISA), National Council of Statewide Interoperability Coordinators (NCSWIC) Planning, Training, and Exercise Committee (2024) Leveraging the PACE Plan into the Emergency Communications Ecosystem. Available at: https://www.cisa.gov/sites/default/files/2024-

10/2024_NCSWICPTE_Leveraging_PACE_Plan_Emergency_Comms_Ecosystems.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 (2024) The NIST Cybersecurity Framework (CSF), Version 2.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.29

[CSRC-PQC] National Institute of Standards and Technology. Post-Quantum Cryptography. Available at: https://csrc.nist.gov/topics/security-and-privacy/cryptography/post-quantum-cryptography

[DOE-AMI] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability (2016) Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investment Grant Program. Available at: https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf

[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) NIST 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) NIST 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) NIST FIPS 180-4. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS186] National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (U.S. Department of Commerce, Washington, DC), Federal

Information Processing Standards Publication (FIPS) NIST FIPS 186-5. https://doi.org/10.6028/NIST.FIPS.186-5

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

[FIPS199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) NIST 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) NIST FIPS 200. https://doi.org/10.6028/NIST.FIPS.200

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

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

[IIC1] Canavan L (2019) What is IIoT? The Industrial Internet of Things Primer Industrial IoT Consortium (IIC), Available at https://www.iiconsortium.org/2019/09/what-is-iiot-the-industrial-internet-of-things-primer/

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

[IICSMM] Security Maturity Model (2022) Industry IoT Consortium (IIC). Available at https://www.iiconsortium.org/smm/

[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) NIST IR 6859. Available at https://doi.org/10.6028/NIST.IR.6859

[IR8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal or Interagency Report (IR) NIST 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) NIST IR 8183Av1. 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) NIST IR 8183Av2. 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) NIST IR 8183Av3. https://doi.org/10.6028/NIST.IR.8183A-3

[IR8228] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, O'Rourke D, Piccarreta B, Scarfone K (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8228. https://doi.org/10.6028/NIST.IR.8228

[IR8428] Salfati E, Pease M (2022) Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT). (National Institute of Standards

and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8428. https://doi.org/10.6028/NIST.IR.8428

[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-iec-62443-series-of-standards

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

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

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

[NIST-DT] National Institute of Standards and Technology. Digital Twins. Available at https://www.nist.gov/digital-twins

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

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

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

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

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

[PPD-41] Presidential Policy Directive 41 (2016) United States Cyber Incident Coordination. (The White House, Washington, DC), July 26, 2016. Available at

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

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

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

[SP1058] Falco JA, Hurd S, Teumim D (2006) Using Host-Based Anti-Virus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST 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) NIST 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) NIST SP 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP800-160v2r1] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v2r1. https://doi.org/10.6028/NIST.SP.800-160v2r1

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

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

[SP800-175A] Barker E, Barker W (2016) Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-175A. https://doi.org/10.6028/NIST.SP.800-175A

[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) NIST SP 800-18r1. 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) NIST SP 800-207. https://doi.org/10.6028/NIST.SP.800-207

[SP800-213] Fagan M, Marron J, Brady K, Cuthill B, Megas K, Herold R, Lemire D, Hoehn B (2021) IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-213. https://doi.org/10.6028/NIST.SP.800-213

[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) NIST SP 800-28ver2. 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) NIST SP 800-30r1. 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) NIST SP 800-34r1, 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) NIST SP 800-37r2. 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) NIST 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) NIST SP 800-40r4. 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) NIST SP 800-41r1. https://doi.org/10.6028/NIST.SP.800-41r1

[SP800-47r1] Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-47r1. https://doi.org/10.6028/NIST.SP.800-47r1

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

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

[SP800-55v1] Schroeder K, Trinh H, Pillitteri VY (2024) Measurement Guide for Information Security: Volume 1 – Identifying and Selecting Measures. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-55v1. https://doi.org/10.6028/NIST.SP.800-55v1

[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) NIST SP 800-60v1r1. 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) NIST SP 800-60v2r1. 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) NIST SP 800-61. https://doi.org/10.6028/NIST.SP.800-61

[SP800-61r3] Nelson A, Rekhi S, Souppaya M, Scarfone KA (2012) Incident Response Recommendations and Considerations for Cybersecurity Risk Management.

(National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3

[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) NIST 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) NIST 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) NIST SP 800-78-4. https://doi.org/10.6028/NIST.SP.800-78-4

[SP1800-45] Tang C, Marron J, Saravia S, Fenimore P, Stea B, White C, Wiltberger J (2026) Cybersecurity for the Water and Wastewater Sector. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1800-45. https://doi.org/10.6028/NIST.SP.1800-45

[UFC4-010-06] U.S. Army Corps of Engineers, Naval Facilities Engineering Systems Command, Air Force Civil Engineer Center (2023) Cybersecurity of Facility-Related Control Systems (FRCS). Unified Facilities Criteria (UFC) 4-010-06. Available a: https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

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

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

Appendix A. List of Symbols, Abbreviations, and Acronyms

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

A3
Association for Advancing Automation

ABAC
Attribute-Based Access Control

ACC
American Chemistry Council

ACI
Aviation Cyber Initiative

ACL
Access Control List

AES
Advanced Encryption Standard

AFPM
American Fuel and Petrochemical Manufacturers

AGA
American Gas Association

AHA
American Hospital Association

AI
Artificial Intelligence

AMA
American Medical Association

AMI
Advanced Metering Infrastructure

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

APT
Advanced Persistent Threat

ASDSO
Association of State Dam Safety Officials

ASHRAE
American Society of Heating, Refrigerating and Air-Conditioning Engineers

ATO
Air Traffic Organization

AWWA
American Water Works Association

BAD
Behavioral Anomaly Detection

BACS
Building Automation and Control 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

CCTV
Closed-Circuit Television

CD
Compact Disc

CDC
Cybersecurity Defense Community

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

CSET
Cyber Security Evaluation Tool

CSF
Cybersecurity Framework

CSO
Chief Security Officer

CSRC
Computer Security Resource Center

CSRIC
Communications Security, Reliability, and Interoperability Council

CTI
Cyber Threat Intelligence

CVE
Common Vulnerabilities and Exposures

CyTRICS
Cyber Testing for Resilient Industrial Control Systems

DCS
Distributed Control System

DDC
Direct Digital Control

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

EDR
Endpoint Detection and Response

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

EOL
End of Life

EOS
End of Support

EPA
United States Environmental Protection Agency

EPRI
Electric Power Research Institute

ERM
Enterprise Risk Management

ERP
Enterprise Resource Planning

ESD
Emergency Shutdown

ESS
Electronic Security Systems

FAA
Federal Aviation Administration

FCC
Federal Communications Commission

FDA
United States Food and Drug Administration

FEMA
Federal Emergency Management Agency

FGS
Fire and Gas System

FHWA
Federal Highway Administration

FIPS
Federal Information Processing Standards

FISMA
Federal Information Security Modernization Act

FMCSA
Federal Motor Carrier Safety Administration

FMEA
Failure Mode and Effects Analysis

FRA
Federal Railroad Administration

FRCS
Facility-Related Control Systems

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

HSE
Health, Safety, and Environment

HSIN
Homeland Security Information Network

HSIN-CI
Homeland Security Information Network - Critical Infrastructure

HSPD
Homeland Security Presidential Directive

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol Secure

HVAC
Heating, Ventilation, and Air Conditioning

I/O
Input/Output

IAARC
International Association for Automation and Robotics in Construction

IACS
Industrial Automation and Control System

IAEA
International Atomic Energy Agency

IAM
Identity and Access Management

ICCP
Inter-Control Center Communications Protocol

ICS
Industrial Control System

ICSS
Integrated Control and Safety Systems

ID
Identification

IDS
Intrusion Detection System

IEC
International Electrotechnical Commission

IED
Intelligent Electronic Device

IEEE
Institute of Electrical and Electronics Engineers

IES
IEEE Industrial Electronics Society

IETF
Internet Engineering Task Force

IFIP
International Federation for Information Processing

IIC
Industry IoT Consortium, Industrial Internet of Things Consortium

IIoT
Industrial Internet of Things

INL
Idaho National Laboratory

IoT
Internet of Things

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

IR
Incident Response

ISA
International Society of Automation

ISAC
International Sharing and Analysis Center

ISCM
Information Security Continuous Monitoring

ISO
International Organization for Standardization

IT
Information Technology

ITL
Information Technology Laboratory

KPI
Key Performance Indicator

KRI
Key Risk Indicator

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

LTE
Long-Term Evolution

MAC
Media Access Control

MARAD
Maritime Administration

MBR
Master Boot Record

MCAA
Measurement, Control, & Automation Association

MES
Manufacturing Execution System

MFA
Multi-Factor Authentication

MIB
Management Information Base

ML
Machine Learning

MTTD
Mean Time to Detect

MTTR
Mean Time to Respond

MTU
Master Terminal Unit

NAM
National Association of Manufacturers

NAWC
National Association of Water Companies

NCC
National Coordinating Center for Communications

NEA
Nuclear Energy Agency

NEI
Nuclear Energy Institute

NERC
North American Electric Reliability Corporation

NESCOR
National Electric Sector Cybersecurity Resource

NFS
Network File System

NFU
National Farmers Union

NGFW
Next Generation Firewall

NHTSA
National Highway Traffic Safety Administration

NICE
National Initiative for Cybersecurity Education

NIH
National Institutes of Health

NIMS
National Incident Management System

NIST
National Institute of Standards and Technology

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

NITAAC
National Institutes of Health Information Technology Acquisition and Assessment Center

NLR
National Laboratory of the Rockies

NOC
Network Operations Center

NRC
United States Nuclear Regulatory Commission

NTAS
National Terrorism Advisory System

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

OSINT
Open-Source Intelligence

OT
Operational Technology

PACE
Primary, Alternate, Contingency, and Emergency

PACS
Physical Access Control System, Picture Archiving and Communications Systems

PAM
Privileged Access Management

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

PQC
Post-Quantum Cryptography

PRAM
Privacy Risk Assessment Methodology

PSCCC
IEEE Power System Communications and Cybersecurity

PSS
Process Safety Shutdown

PT
Pressure Transmitter

PTP
Precision Time Protocol

R&D
Research and Development

RAS
IEEE Robotics and Automation Society

RBAC
Role-Based Access Control

RDP
Remote Desktop Protocol

RF
Radio Frequency

RFC
Request for Comments

RFID
Radio Frequency Identification

RMF
Risk Management Framework

RPC
Remote Procedure Call

RPO
Recovery Point Objective

RTO
Recovery Time Objective

RTOS
Real-Time Operating System

RTU
Remote Terminal Unit

S4
SCADA Security Scientific Symposium

SANS
SysAdmin, Audit, Network, and Security

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

TAP
Test Access Point

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

UFC
Unified Facilities Criteria

UPS
Uninterruptible Power Supply

U.S.
United States

USB
Universal Serial Bus

USDA
United States Department of Agriculture

VAV
Variable Air Volume

VDP
Vulnerability Disclosure Policy

VLAN
Virtual Local Area Network

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

VTS
IEEE Vehicular Technology Society

WAF
Web Application Firewall

WAN
Wide Area Network

WG
Working Group

Wi-Fi
Wireless Fidelity

WINS
World Institute of Nuclear Security

ZTA
Zero Trust Architecture

ZTNA
Zero Trust Network Access

Appendix B. Glossary

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

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

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

advanced metering infrastructure
An integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers. [DOE-AMI]

advanced persistent threat
An adversary with sophisticated levels of expertise and significant resources that pursues its objectives repeatedly over an extended period, adapting to defenders' efforts to resist it. [SP800-39] (adapted)

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

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

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

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

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

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

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

building automation and control system
A type of OT system used to manage critical building infrastructure and optimize facility operations, overseeing systems such as heating, ventilation, and air conditioning (HVAC), fire safety, electrical and lighting, physical security and access control, and energy management.

cleartext
Information that is not encrypted.

closed-circuit television
A system of video cameras used to transmit signals to a specific, limited set of monitors for surveillance and monitoring purposes.

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

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

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

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

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

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

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

control loop
A control loop consists of sensors for measurement, controller hardware (e.g., PLCs), actuators (e.g., control valves, breakers, switches, and motors), and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.

control network
Those networks of an enterprise typically connected to equipment that controls physical processes and that is time- or safety-critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.

control server
A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as remote terminal units (RTUs) and programmable logic controllers (PLCs), over an OT network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.

control system
A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs, BAS, and other types of OT measurement and control systems.

controlled variable
The variable that the control system attempts to keep at the set point value. The set point may be constant or variable. [ISADICT]

controller
A device or program that operates automatically to regulate a controlled variable. [ANSI-ISA-51-1]

cyber threat intelligence
Cyber threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. [SP800-61r3] (adapted)

cycle time
The time, usually expressed in seconds, for a controller to complete one control loop where sensor signals are read into memory, control algorithms are executed, and corresponding control signals are transmitted to actuators that create changes to the process resulting in new sensor signals. [ISADICT]

data diode
A network appliance or device that allows data to travel only in one direction. Also referred to as a *unidirectional gateway*, deterministic one-way boundary device, or unidirectional network.

data historian
A centralized database that supports data analysis using statistical process control techniques.

database
A repository of information that usually holds plant-wide information including process data, recipes, personnel data, and financial data. [IR6859] (adapted)

demilitarized zone
An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. [SP800-41r1]

denial of service
The prevention of authorized access to a system resource or the delaying of system operations and functions. [RFC4949]

diagnostics
Information concerning known failure modes and their characteristics. Such information can be used in troubleshooting and failure analysis to help pinpoint the cause of a failure and help define suitable corrective measures. [ISADICT]

digital twin
A computer model of a physical system, such as a machine or building, used to monitor status, detect anomalies, and predict system behavior. [NIST-DT] (adapted)

direct digital control
A control approach in which a digital computer or controller directly manages building equipment (e.g., HVAC components) through software logic rather than analog control loops.

disaster recovery plan
A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. [SP800-34r1] (adapted)

discrete process
A type of process where a specified quantity of material moves as a unit (part or group of parts) between workstations, and each unit maintains its unique identity. [ISADICT]

distributed control system
In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit. [ISADICT]

disturbance
An undesired change in a variable being applied to a system that tends to adversely affect the value of a controlled variable. [ANSI-ISA-51-1]

domain
An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. [RFC4949] (adapted)

electronic security systems
Systems used to monitor and control access to a facility, such as intrusion detection, video surveillance, and physical access control systems.

encryption
Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state. [RFC4949] (adapted)

endpoint detection and response
A category of tools that continuously monitor endpoint behavior and collect telemetry to detect and respond to threats.

end of life
The point at which a vendor stops selling or actively supporting a product, often signaling that security patches and updates will no longer be provided.

end of support
The point at which a vendor ceases all technical support and maintenance for a product, including security updates.

enterprise
An organization that coordinates the operation of one or more processing sites.

enterprise resource planning
A category of business management software that integrates core organizational processes, such as finance, procurement, and supply chain, into a unified system.

facility-related control systems
A subset of control systems used to monitor and control equipment and systems related to DoD real property facilities, such as building control systems, utility control systems, electronic security systems, and fire and life safety systems. [UFC 4-010-06]

fault tolerant
A system having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault.

field device
Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

field site
A subsystem that is identified by physical, geographical, or logical segmentation within the ICS. A field site may contain RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

fieldbus
A digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment, such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network, and each message identifies a particular sensor on the network.

firewall
An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). [RFC4949]

health, safety, and environment
A category of risk impact involving potential harm to personnel, the public, or the environment.

human-machine interface
The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software. [IR6859]

identification
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

identity and access management
Broadly refers to the administration of individual identities within a system, such as a company, a network, or even a country. [SP800-175A] (adapted)

incident
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [FIPS200]

industrial control system
A general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as programmable logic controllers (PLC). An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

information security program plan
A formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. [OMB-A130]

input/output
A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications. [ISADICT]

insider
An entity inside the security perimeter that is authorized to access system resources but uses them in a way that is not approved by those who granted the authorization.

integrity
Guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity. [USC44-3552] (adapted)

intelligent electronic device
Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers). [AGA12]

internet
The single interconnected worldwide system of commercial, government, educational, and other computer networks that share the set of protocols specified by the Internet Architecture Board (IAB) and the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). [RFC4949] (adapted)

intrusion detection system
A security service that monitors and analyzes network or system events for the purpose of finding and providing real-time or near-real-time warning of attempts to access system resources in an unauthorized manner. [RFC4949] (adapted)

intrusion prevention system
A system that can detect an intrusive activity and also attempt to stop the activity, ideally before it reaches its targets.

jitter
The time or phase difference between the data signal and the ideal clock.

key performance indicator
A measurable value that demonstrates how effectively an organization is achieving key business or security objectives.

key risk indicator
A metric used to signal an increasing exposure to risk in various areas of an organization, providing early warning of potential issues.

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.

long-term evolution
A standard for wireless broadband communication for mobile devices and data terminals, sometimes used for remote or cellular-based OT connectivity.

machine controller
A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage. [IR6859]

machine learning
The development and use of computer systems that adapt and learn from data with the goal of improving accuracy. [SP800-55v1]

maintenance
Any act that either prevents the failure or malfunction of equipment or restores its operating capability. [ISADICT]

malware
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. [SP800-53r5] (adapted)

manipulated variable
In a process that is intended to regulate some condition, a quantity or a condition that the control alters to initiate a change in the value of the regulated condition. [ISADICT]

manufacturing execution system
A system that uses network computing to automate production control and process automation. By downloading recipes and work schedules and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems. [IR6859]

master terminal unit
See *Control Server*.

mean time to detect
A metric that tracks the average amount of time that a problem exists before it is found. [SP800-55v1]

mean time to respond
The average time it takes an organization to respond to a security incident after detection.

network operations center
A centralized location from which an organization monitors, manages, and maintains its network infrastructure.

open-source intelligence
Information collected from publicly available sources and analyzed to produce actionable intelligence.

operating system
An integrated collection of service routines for supervising the sequencing of programs by a computer. An operating system may perform the functions of input/output control, resource scheduling, and data management. It provides application programs with the fundamental commands for controlling the computer. [ISADICT]

operational controls
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). [FIPS200]

operational technology
A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

password
A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. [FIPS140-2]

phishing
Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet websites).

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.

post-quantum cryptography
An area of cryptography focused on quantum-resistant primitives, with the goal of keeping existing public key

infrastructure intact in a future era of quantum computing. Also referred to as quantum-resistant cryptography. [CSRC-PQC]

predisposing condition
A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation. [SP800-30r1]

pressure regulator
A device used to control the pressure of a gas or liquid. [IR6859]

pressure sensor
A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium. Pressure sensors can also use differential pressure to obtain level and flow measurements. [IR6859] (adapted)

primary, alternate, contingency, and emergency
A methodology that helps organizations prepare backup communications capabilities and establish options for redundant communications if primary capabilities are disrupted or degraded. [CISA-PACE] (adapted)

privileged access management
The policies, processes, and technologies used to control, monitor, and secure access to an organization's most sensitive accounts and systems.

process controller
A type of computer system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs. [IR6859] (adapted)

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

protocol
A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [RFC4949]

protocol analyzer
A device or software application that enables the user to analyze the performance of network data so as to ensure that the network and its associated hardware/software are operating within network specifications. [ISADICT]

real time
Pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process.

redundant control server
A backup to the control server that maintains the current state of the control server at all times. [IR6859]

relay
An electromechanical device that completes or interrupts an electrical circuit by physically moving conductive contacts. The resultant motion can be coupled to another mechanism such as a valve or breaker. [ISADICT]

remote access
Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. [SP800-53r5]

remote diagnostics
Diagnostic activities conducted by individuals who are outside of an information system security perimeter.

remote maintenance
Maintenance activities conducted by individuals communicating through an external network. [SP800-53r5]

remote terminal unit
A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs. [IR6859]

risk
The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. [FIPS200] (adapted)

risk assessment
The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [SP800-39] (adapted)

risk management
The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. [FIPS200] (adapted)

router
A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. [RFC4949] (adapted)

safety instrumented system
A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated. Other terms commonly used include emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS). [ANSI-ISA-84]

SCADA server
The device that acts as the master in a SCADA system.

security audit
Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. [ISO7498-1]

security controls
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS199]

security plan
A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [SP800-18r1]

security policy
Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.

sensor
A device that produces a voltage or current output that is representative of some physical property being measured (e.g., speed, temperature, flow). [ISADICT]

set point
An input variable that sets the desired value of the controlled variable. This variable may be manually set, automatically set, or programmed. [ISADICT]

single loop controller
A controller that controls a very small process or a critical process. [IR6859]

social engineering
An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. [800-115]

supervisory control
A term that is used to imply that the output of a controller or computer program is used as input to other controllers. See *Control Server*. [ISADICT]

supervisory control and data acquisition
A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. [ISADICT]

technical controls
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. [FIPS200]

test access point
A hardware device inserted into a network to passively capture and monitor traffic without disrupting the flow of data.

threat
Any circumstance or event with the potential to adversely impact agency operations (including safety, mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [FIPS200] (adapted)

threat event
An event or situation that has the potential for causing undesirable consequences or impact. [SP800-30r1]

threat source
The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. *Synonymous with threat agent.* [FIPS200]

Trojan horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. [RFC4949]

unauthorized access
A person gains logical or physical access without permission to a network, system, application, data, or other resource. [SP800-61]

unidirectional gateway
Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information back to the source network. The software replicates databases and emulates protocol servers and devices.

valve
An in-line device in a fluid-flow system that can interrupt flow, regulate the rate of flow, or divert flow to another branch of the system. [ISADICT]

virtual private network
A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. [RFC4949] (adapted)

virus
A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. [RFC4949] (adapted)

vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [FIPS200]

wide area network
A physical or logical network that provides data communications to a larger number of independent users than are typically served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

wireless device
Any device that can connect to an OT network via radio or infrared waves, usually to collect or monitor data but also to modify control set points in some cases.

workstation
A computer used for tasks such as programming, engineering, and design. [IR6859]

worm
A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. [RFC4949] (adapted)

zero trust architecture
A security model and cybersecurity strategy based on the premise that threats exist both inside and outside traditional network boundaries. It eliminates implicit trust in any element, component, or service, requiring continuous verification before granting access. [SP800-160v2r1]

zero trust network access
A security model and set of technologies that grant access to applications and services based on defined access control policies, rather than implicit trust based on network location.

Appendix C. Threat Sources, Vulnerabilities, and Incidents

Several terms are used to describe the interrelated concepts of threat, threat source, threat event, and incident. A *threat* is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats have some intent or method that may exploit a vulnerability through either intentional or unintentional means. This intent or method is referred to as the *threat source*. A *vulnerability* is a weakness in an information system (including an OT), system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A *threat event* is an event or situation that has the potential to cause undesirable consequences or impacts. When a threat event occurs, it becomes an *incident* that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

This appendix explores OT-specific threat sources, vulnerabilities, and incidents. It also cites examples of OT-specific incidents to illustrate their potential impacts. Each organization calculates risk based on the specific threats, vulnerabilities, impacts, and likelihood of incidents within its environment.

C.1. Threat Sources

Threats to OT can come from numerous sources that can be classified as adversarial, accidental, structural, or environmental. These threat sources should be well-understood and considered part of the risk management strategy to define and implement adequate protection. For example, environmental events (e.g., floods, earthquakes) are well-understood but may vary in magnitude, frequency, and their ability to compound with other interconnected events. However, adversarial threats depend on the resources available to the adversary and the emergence of previously unknown vulnerabilities or attacks. Table 10 lists and defines known threat sources to OT.

Table 10. 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

Type of Threat Source	Description	Characteristics
ACCIDENTAL • User • Privileged user or administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities (e.g., operator accidentally typing 100 instead of 10 as a set point; engineer making a change in the production environment while thinking that they are in the development environment).	Range of effects
STRUCTURAL • Hardware failure o Processors, input/output cards, communications cards o Networking equipment o Power supply o Sensor, final element o HMI, displays • Software failure o OS o General-purpose applications o Mission-specific applications • Environmental controls failure o Temperature control o Humidity control • Communications degradation o Wireless o Wired	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters, including failures of critical infrastructures within the control of the organization.	Range of effects
ENVIRONMENTAL • Natural or human-caused disaster o Fire o Flood/tsunami o Windstorm/tornado o Hurricane o Earthquake o Bombing o Animal interference o Solar flares, meteorites • Critical infrastructure failure o Telecommunications o Electrical power o Transportation o Water/wastewater	Natural disasters and failures of critical infrastructures on which the organization depends but that are outside of the control of the organization. Natural and human-caused disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities that house mission-critical systems, making those systems unavailable for three weeks).	Range of effects

C.2. Vulnerabilities and Predisposing Conditions

Vulnerabilities are weaknesses in information systems, system procedures, controls, or implementations that can be exploited by a threat source. *Predisposing conditions* are properties of the organization, mission, or business process, architecture, or information systems that contribute to the likelihood of a threat event. The order of these vulnerabilities and predisposing conditions does not reflect priority in terms of likelihood of occurrence or severity of impact. Additionally, the vulnerabilities and predisposing conditions identified in this appendix should not be considered a complete list, nor should they be assumed to occur in every OT environment.

Vulnerabilities and predisposing conditions are grouped according to where they exist (e.g., in the organization's policy and procedures) or the inadequacy of security mechanisms implemented in hardware, firmware, and software. The former is referred to as being "in the organization" and the latter as being "in the system." Understanding the source of vulnerabilities and predisposing conditions can help identify optimal mitigation strategies. Deeper analysis may uncover that causes and observations are not one-to-one. That is, some underlying causes may exhibit multiple symptoms, and some symptoms may come from more than one cause.

Any given OT will usually exhibit a subset of the identified vulnerabilities in this appendix, but may also contain additional vulnerabilities and predisposing conditions that are unique to a particular technology or implementation. Specific current information on OT vulnerabilities can be found on the CISA website, though many vendors publish notifications and patches that are not always found on the CISA website. It is beneficial to maintain relationships with vendors in order to stay up to date with known vulnerabilities.

Some vulnerabilities and predisposing conditions can be mitigated. Others can only be accepted and controlled by appropriate countermeasures but will result in some residual risk to the OT environment. For example, some existing policies and procedures may be changed with a level of effort that the organization considers acceptable, while others may be addressed more expeditiously by instituting additional policies and procedures.

Vulnerabilities in the products and services acquired from outside of the organization are rarely under the direct control of the organization. Changes may be influenced by market forces, but this is a slow and indirect approach. Instead, the organization may change predisposing conditions to reduce the likelihood that a systemic vulnerability will be exploited.

C.2.1. Policy and Procedure Vulnerabilities and Predisposing Conditions

Vulnerabilities and predisposing conditions are often introduced into the OT environment due to incomplete, inappropriate, or nonexistent security policies, including documentation, implementation guides (e.g., procedures), and enforcement. Management support of security policy and procedures is the cornerstone of any security program. An organization's security policy can reduce vulnerabilities by mandating and enforcing proper conduct. Written policies and procedures are mechanisms for informing staff and stakeholders of decisions regarding

behaviors that benefit the organization. From this perspective, policy is an educational and instructive way to reduce vulnerabilities. Enforcement is a partner to policy and encourages people to do the proper thing. Various forms of corrective action are the usual consequences to personnel not following policy and procedures. Policies should be explicit about the consequences to individuals or organizations that do not conform.

There is usually a complex policy and procedure environment that includes laws, regulations, overlapping jurisdictions and spheres of influence, economics, customs, and history. Larger enterprises are often subdivided into organizational units that work together to reduce vulnerabilities. The scope and hierarchical relationship among policies and procedures need to be managed for maximum effectiveness.

Table 11 presents examples of observed policy and procedure vulnerabilities and predisposing conditions for OT.

Table 11. Policy and procedure vulnerabilities and predisposing conditions

Vulnerability	Description
Inadequate organizational ownership of risk assessments	Risk assessments should be performed with acknowledgement from appropriate levels within the organization. The lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
Inadequate security policy for OT	Vulnerabilities are often introduced into the OT environment due to inadequate policies or the lack of policies specifically for OT system security. Controls and countermeasures should be derived from a risk assessment or policy to ensure uniformity and accountability.
Inadequate OT security training and awareness program	A documented formal OT security training and awareness program is designed to keep staff up to date on organizational security policies and procedures, threats, industry cybersecurity standards, and recommended practices. Without adequate ongoing training on specific OT policies and procedures, staff cannot be expected to maintain a secure OT environment.
Lack of inventory management policy	Inventory policy and procedures should include installation, removal, and changes made to hardware, firmware, and software. An incomplete inventory could lead to unmanaged and unprotected devices within the OT environment.
Lack of configuration management policy	Lack of policy and procedures for OT configuration management can lead to an unmanageable and highly vulnerable inventory of hardware, firmware, and software.
Inadequate OT equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an OT malfunction.
Lack of administrative mechanisms for security policy enforcement	Without accountability for enforcing policy, there is limited ability to ensure that security policies are followed adequately. Administrative mechanisms should be in place to ensure accountability.
Inadequate review of the effectiveness of the OT security controls	Procedures and schedules should exist to determine the extent to which the security program and its constituent controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the OT. The examination is sometimes called an “audit,” “evaluation,” or “assessment.” Policy should address the stage of the life cycle, purpose, technical expertise, methodology, and level of independence.

Vulnerability	Description
No OT-specific contingency plan	A contingency plan (e.g., business continuity plan, disaster recovery plan) should be prepared, tested, and available in the event of a major hardware or software failure or destruction of facilities. The lack of a specific plan for the OT could lead to extended downtimes and production losses.
Lack of adequate access control policy	Access control enforcement depends on policy that correctly models roles, responsibilities, and authorizations. The policy model must enable the way the organization functions.
Lack of adequate authentication policy	Authentication policies are needed to define when authentication mechanisms (e.g., passwords, smart cards) must be used, how strong they must be, and how they must be maintained. Without this policy, systems may not have appropriate authentication controls, making unauthorized access to systems more likely. Authentication policies should be developed as part of an overall OT security program, taking into account the capabilities of the OT and its personnel to handle more complex passwords and other mechanisms.
Inadequate incident detection and response plan and procedures	Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods for collecting, analyzing, and reporting data.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single-point-of-failure possibilities.
Lack of policies and procedures for AI-enhanced social engineering	Generative AI enables adversaries to craft highly targeted and convincing phishing emails, voice calls, and video communications that are indistinguishable from legitimate correspondence. Unlike traditional social engineering awareness training, addressing this threat requires organizations to establish and enforce procedural verification mechanisms for sensitive requests that do not rely solely on perceived legitimacy.
Lack of supply chain security policy	OT hardware, software, and firmware sourced from vendors, integrators, and third-party suppliers may contain compromised, counterfeit, or vulnerable components. Without policies governing vendor vetting, component integrity verification, and oversight of third-party access, organizations may unknowingly introduce malicious code or exploitable vulnerabilities into critical systems. Vendors and integrators often require privileged access to OT systems for installation and maintenance, making unvetted third-party involvement a significant supply chain risk.

C.2.2. System Vulnerabilities and Predisposing Conditions

Security controls must clearly identify the systems to which they apply. Systems range widely in size, scope, and capability. At the small end of the spectrum, a system may be an individual hardware or software product or service. At the other end of the spectrum are large and complex systems, systems-of-systems, and networks, all of which incorporate hardware architectures and software frameworks (including application frameworks) to support operations. An organization may choose to identify security zones such that security controls may be applied to all systems within the security zone.

System vulnerabilities can occur in the hardware, firmware, and software used to build the OT. Sources of vulnerabilities include design flaws, development flaws, misconfigurations, poor maintenance, poor administration, and connections with other systems and networks. Many of the controls in the SP 800-53 and the OT overlay in Appendix E specify what the system must do to mitigate these vulnerabilities.

Vulnerabilities can also exist in the auxiliary components that support the OT systems. The potential vulnerabilities and predisposing conditions commonly found within OT systems are categorized into the following tables:

- Table 12. Architecture and design vulnerabilities and predisposing conditions
- Table 13. Configuration and maintenance vulnerabilities and predisposing conditions
- Table 14. Physical vulnerabilities and predisposing conditions
- Table 15. Software development vulnerabilities and predisposing conditions
- Table 16. Communication and network configuration vulnerabilities and predisposing conditions
- Table 17. Sensor, final element, and asset management vulnerabilities and predisposing conditions

Table 12. Architecture and design vulnerabilities and predisposing conditions

Vulnerability	Description
Inadequate incorporation of security into architecture and design	Incorporating security into the OT architecture and design must start with a budget and schedule designated for OT. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
Inadequate management of change that allows insecure architecture to evolve	The network infrastructure within the OT environment has often been developed and modified based on business and operational requirements with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within the infrastructure. Without remediation, these gaps may represent backdoors into the OT. Sensors and controllers that were historically simple devices are now often manufactured as intelligent devices. In some cases, sensors and controllers may be replaced with IIoT devices that allow direct internet connections. Security should be incorporated into change management for all OT devices, not just traditional IT components.
No security perimeter defined	If the OT does not have a security perimeter clearly defined, it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability. Having both types of traffic on a single network creates challenges for meeting the requirements of control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in OT functions.

Vulnerability	Description
Control network services dependent on a non-control network	When IT services (e.g., DNS, DHCP) are used by control networks, they are often implemented in the IT network. This causes the OT network to become dependent on the IT network, which may not have the reliability and availability requirements needed by OT.
Inadequate collection of event data history	Forensic analysis depends on the collection and retention of sufficient data. Without proper and accurate data collection, it may be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures. Event data for an OT environment could include physical process data, system use data, and network data.
Inadequate security architecture considerations for IoT and IIoT device integration	IoT and IIoT devices often have limited built-in security capabilities and may introduce new network pathways and communication channels that have not been accounted for. Without adequate network segmentation and access controls, the integration of these devices can significantly expand the OT attack surface and provide adversaries with additional entry points into the environment.
Inadequate security architecture considerations for cloud-connected OT environments	When cloud integration is not adequately accounted for in the OT security architecture, it introduces dependencies on external infrastructure outside of the organization's direct control and may create network pathways that bypass existing perimeter controls.
Lack of post-quantum cryptography consideration in OT architecture	Advances in quantum computing are expected to render widely used asymmetric encryption algorithms obsolete, posing a long-term risk to OT systems that cannot be updated or replaced. Organizations should consider cryptographic agility as a requirement when procuring new OT systems to ensure that cryptographic standards can be updated without requiring full hardware replacement.
Inadequate security considerations for AI systems integrated into OT environments	AI systems are susceptible to manipulation through prompt injection and compromised training data, which can cause models to produce incorrect outputs, develop blind spots that allow unsafe conditions or malicious activity to go undetected, or reveal sensitive information to unauthorized users. The data pipelines and external connectivity required to support AI systems can also introduce new network pathways into the OT environment that may not be properly secured.
Inadequate consideration of AI behavior in deterministic OT environments	OT control systems are designed around deterministic logic, meaning that a given input reliably produces the same expected output. AI systems operate probabilistically, meaning that outputs are based on statistical inference and may vary under different conditions. Deploying AI in safety-critical OT environments without accounting for this fundamental difference introduces the risk of unpredictable outputs that could result in incorrect process recommendations, missed anomalies, or unsafe operational decisions.

5965 **Table 13. Configuration and maintenance vulnerabilities and predisposing conditions**

Vulnerability	Description
Hardware, firmware, and software that are not under asset management	The organization does not know what it has (e.g., make, model), where they are, or what version it is, resulting in an inconsistent and ineffective defense posture. To properly secure an OT, there should be an accurate inventory of the assets in the environment. Procedures should be in place to manage additions, deletions, and modifications of assets, which include asset inventory management. These procedures are critical to executing business continuity and disaster recovery plans.
Hardware, firmware, and software are not under configuration management	The organization does not know the patch management status, security settings, or configuration versions that it has, resulting in an inconsistent and ineffective defense posture. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure that an OT is protected against inadequate or improper modifications before, during, and after system implementation. To properly secure an OT, there should be an accurate listing or repository of the current configurations.
OS and vendor software patches may not be developed until long after security vulnerabilities are found	Because of the tight coupling between OT software and the underlying OT, changes must undergo expensive and time-consuming comprehensive regression testing. The elapsed time for such testing and the subsequent distribution of updated software provides a long window of vulnerability. Vulnerability management procedures should include flexibility for interim alternative mitigations.
Vendor declines to develop patches for vulnerability	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Security patch support may not be available for legacy OT, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where patches may never be available or replacement plans.
Lack of a vulnerability management program	Vulnerability management procedures should be in place to determine a plan of action or inaction upon the discovery of a vulnerability. Some OT-specific considerations regarding patching include general availability (e.g., patching delayed to the next planned operational downtime), security patch support being unavailable for OT systems that use outdated OSs, isolated systems that may not require immediate patching, and prioritizing patching for OT that is exposed to the internet.
Inadequate testing of security changes	Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the OT. Documented procedures should be developed for testing all changes for security impacts. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
Poor remote access controls	There are many reasons why an OT may need to be remotely accessed, including vendors and system integrators performing system maintenance functions or OT engineers accessing geographically remote system components. The concept of least privilege should be applied to remote access controls. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access or authorized individuals from gaining excessive access to the OT.

Vulnerability	Description
Poor configurations are used	Improperly configured systems may leave unnecessary ports and protocols open. These unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.
Critical configurations are not stored or backed up	Procedures should be available for restoring OT configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent the loss of data. Documented procedures should be developed for maintaining configuration settings.
Data unprotected on portable device	System security could be compromised if sensitive data (e.g., passwords, dial-up numbers) is stored in cleartext on lost or stolen portable devices, such as laptops and mobile devices. Policy, procedures, and mechanisms are required for protection.
Vendor default passwords are used	Most vendor default passwords are easy to discover within vendor product manuals, which are also available to adversaries. Using the default password can drastically increase OT vulnerability.
Password generation, use, and protection do not comply with policy	Password policy and procedures must be followed to be effective. Violations of password policy and procedures can increase OT vulnerability.
Inadequate access controls applied	Access controls must match how the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in an OT user having too many or too few privileges. For example: • System configured with default access control settings gives an operator administrative privileges. • System configured improperly results in an operator being unable to take corrective actions in an emergency situation.
Improper data linking	OT data storage systems may be linked to non-OT data sources. For example, database links allow data from one database (e.g., data historian) to be automatically replicated on others. Data linkage may create a vulnerability if it is not properly configured and may allow unauthorized data access or manipulation.
Malware protection is not installed or up to date	The installation of malware (i.e., malicious software) is a common attack. Malware protection software (e.g., antivirus software) should be kept current in a dynamic environment. Outdated malware protection software and definitions leave the system open to malware threats.
Malware protection implemented without sufficient testing	Malware protection software that is deployed without sufficient testing could impact the normal operation of the OT and block the system from performing necessary control actions.
Denial of service (DoS)	OT software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.
Intrusion detection and prevention software is not installed	Incidents can result in the loss of system availability and integrity; the capture, modification, and deletion of data; and the incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to ensure that it does not compromise normal operation of the OT.
Logs are not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur and perform adequate forensics.

Vulnerability	Description
Inadequate security configuration management for IoT and IIoT devices	Unlike traditional OT devices that support centralized configuration management, many IoT and IIoT devices run proprietary embedded firmware that can only be configured through vendor-specific interfaces, making it difficult to consistently enforce security settings or audit device configurations at scale. These devices are also often deployed with vendor default credentials and unnecessary services enabled that cannot be disabled due to device limitations.
Limited organizational control over cloud platforms and services in OT environments	Cloud-connected OT systems introduce gaps that organizations have limited visibility into and control over (e.g., specific security settings and configurations within the cloud platform). These gaps increase the risk of misconfigured services, inadequate access controls, and limited visibility that could hinder monitoring and detection, expose operational data, or provide adversaries with unintended access pathways into the OT environment.

5966 **Table 14. Physical vulnerabilities and predisposing conditions**

Vulnerability	Description
Unauthorized personnel have physical access to equipment	Physical access to OT equipment should be restricted to only the necessary personnel while taking safety requirements into account, such as emergency shutdown or restarts. Improper access to OT equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage to or destruction of data and hardware • Modification of the operational process • Unauthorized changes to the functional environment (e.g., data connections, unauthorized use of removable media, adding/removing resources) • Disconnection of physical data links • Undetectable interception of data (e.g., keystroke, other input logging)
Radio frequency, electromagnetic pulse (EMP), static discharge, brownouts, and voltage spikes	Some hardware used for OT systems is vulnerable to radio frequency, electromagnetic pulses (EMP), static discharge, brownouts, and voltage spikes. The impacts can range from the temporary disruption of command and control to permanent damage to circuit boards. Proper shielding, grounding, power conditioning, and/or surge suppression is recommended.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the OT and could create an unsafe situation. Loss of power could also lead to insecure default settings. If the program file or data is stored in volatile memory, the process may not be able to restart after a power outage without appropriate backup power.
Loss of environmental control	The loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, such as processors overheating. Some processors will shut down to protect themselves. Others may continue to operate in a minimal capacity and produce intermittent errors, continually reboot, or become permanently inoperable.
Unsecured physical ports	Unsecured universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives or keystroke loggers.

5967 **Table 15. Software development vulnerabilities and predisposing conditions**

Vulnerability	Description
Improper data validation	OT software may not properly validate user inputs or received data to ensure validity. Invalid data may result in numerous vulnerabilities, including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities are not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.

5968 **Table 16. Communication and network configuration vulnerabilities and predisposing conditions**

Vulnerability	Description
Data flow controls are not employed	Data flow controls based on data characteristics are needed to restrict the information that is permitted between systems. These controls can prevent the exfiltration of information and illegal operations.
Firewalls are nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and enterprise networks, thus allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping, and providing individuals with unauthorized access to systems.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
Standard, well-documented communication protocols are used in plaintext	Adversaries that can monitor the OT network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols, such as telnet, FTP, HTTP, and NFS. The use of such protocols also makes it easier for adversaries to perform attacks against the OT and manipulate OT network activity.
Authentication of users, data, or devices is substandard or nonexistent	Many OT protocols have no authentication at any level. Without authentication, there is the potential to replay, modify, or spoof data or devices, such as sensors and user identities.
Use of unsecure OT protocols	OT protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. The incorrect implementation of the protocols can also lead to additional vulnerabilities.
Lack of integrity checking for communications	Integrity checks are not built into most OT protocols, so adversaries could manipulate communications undetected. To ensure integrity, the OT can use lower-layer protocols (e.g., IPsec) that offer data integrity protection when traversing untrusted physical media.
Inadequate authentication between wireless clients and access points	Strong mutual authentication between wireless clients and access points is needed to ensure that legitimate OT clients do not connect to a rogue access point deployed by an adversary and that adversary clients do not connect to any of the OT wireless networks.
Inadequate data protection between wireless clients and access points	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.

Vulnerability	Description
Insecure or unnecessary communications between OT systems and cloud platforms	Communications between OT systems and cloud platforms may lack adequate encryption, authentication, or integrity verification, leaving operational data susceptible to interception and unauthorized access. Unnecessary outbound connections to external domains initiated by cloud platform agents or services may not be accounted for in existing firewall rules or network monitoring configurations, creating uncontrolled pathways outside the OT environment.
Overreliance on third-party communication infrastructure for OT connectivity	Many OT environments rely on third-party carrier networks such as cellular and private LTE for communications between remote sites and central control systems. Third-party communication links are subject to outages, degraded performance, and compromise events outside the organization's control. Organizations that have not accounted for the unavailability or compromise of third-party communication links may find themselves unable to monitor or control remote sites during an incident.

5969 **Table 17. 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 loop should be managed to prevent incidents.
Unauthorized wireless access to sensors or final elements	Wireless access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices allow for wireless configuration (e.g., Bluetooth, Wi-Fi, WirelessHART). Wireless access should be securely configured or disabled using hardware write-protect where possible to prevent unauthorized modification of the sensors and final elements that are connected to both the physical process and the OT environment.
Inappropriate segmentation of the asset management system	Most architectures are designed for PLCs, RTUs, DCS, and SCADA controllers to manipulate the process and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

5970

5971 C.3. Threat Events and Incidents

5972 A threat event is an event or situation that could potentially cause an undesirable consequence
5973 or impact to operations resulting from some threat source. [SP800-30r1] Appendix E identifies a
5974 broad set of threat events that could potentially impact information systems. The properties of
5975 OT may also present unique threat events, such as how the threat events can manipulate OT
5976 processes to cause physical damage.

5977 Understanding how these threat events manifest in OT environments can be informed by
5978 MITRE ATT&CK for ICS, which is a knowledge base of adversary tactics and techniques observed
5979 in threat events targeting ICS [ATTACK-ICS]. ATT&CK for ICS provides detailed insight into the
5980 activities and software that threat actors have used in prior attacks against ICS environments.

The knowledge base catalogs common ICS assets found in ICS environments, including control servers, PLCs, and remote terminal units. It maps observed adversarial techniques to those assets based on their technical capabilities and operational functions [ATTACK-ICS]. This mapping helps organizations identify which techniques are most likely to target a given asset and prioritize defensive measures accordingly.

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. The four broad categories of threat sources are adversarial, accidental, structural, and environmental (see Appendix C.1). Often, an incident can be the result of multiple threat sources (e.g., an environmental event causes a system failure that an operator incorrectly responds to, leading to an accidental event).

Below is a limited selection of reported incidents that fall into each of the four categories. The incidents have been additionally categorized into malicious or non-malicious and direct or indirect to further distinguish the possible causes of OT incidents.

- **M = Malicious.** The event was initiated by someone for a harmful purpose. The initiator may or may not have been targeting the OT or known the potential consequences.
- **N = Non-malicious.** There does not appear to be evidence that the initiating event was intended to cause an incident.
- **D = Direct.** The event was designed to discover, inhibit, impair, or otherwise impact the OT system.
- **I = Indirect.** The event was not believed to be designed to discover, inhibit, impair, or otherwise impact the OT system. The OT system shut down or caused disruption as a result of an impact on the supporting infrastructure.

C.3.1. Adversarial Events

Adversarial events include:

- **[M][D] Marconi wireless hack.**[7] In 1903, Italian radio pioneer Guglielmo Marconi was preparing for his first public demonstration of long-distance secure wireless communications from Cornwall to Professor Fleming at the Royal Institution of London. Inventor and magician Nevil Maskelyne hacked the system and sent a comical message in Morse code referencing “rats.” Maskelyne then published an explanation of his hack in the trade journal *The Electrician*.
- **[M][I] Worcester air traffic communications.**[8] In March 1997, a teenager in Worcester, Massachusetts, disabled part of the public switched telephone network using a dial-up modem connected to the system. This disabled phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use

[7] Additional information on the Marconi wireless hack incident can be found at https://www.osti.gov/biblio/1505628.
[8] 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

the airport. The tower's main radio transmitter and another transmitter that activated runway lights were also shut down as well as a printer that controllers used to monitor flight progress. The attack also disabled phone service to 600 homes and businesses in the nearby town of Rutland.

- **[M][D] Maroochy Shire sewage spill.**[9] In the spring of 2000, a former employee of an Australian organization that developed manufacturing software applied for a job with the local government but was rejected. Over a two-month period, the disgruntled employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for specific sewerage pumping stations, causing malfunctions in their operations and ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.
- **[M][I] Night Dragon.**[10] McAfee reported a series of attacks that were designed to steal sensitive data from global oil, energy, and petrochemical industries. Adversaries exfiltrated proprietary operations data and project financing information with regard to oil and gas field bids and operations.
- **[M][D] Iranian centrifuge, Stuxnet.**[11] 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 target only particular SCADA systems that were configured to control and monitor specific industrial processes.
- **[M][D] German steel mill attack.**[12] In 2014, hackers manipulated and disrupted control systems to such a degree that a blast furnace could not be properly shut down, resulting in unspecified "massive" damage.
- **[M][I] Shamoon.**[13] In 2012, Saudi Aramco experienced a malware attack that targeted its 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.**[14] In 2013, an Iranian computer security company obtained remote access to a computer that controlled the SCADA system for the Bowman Dam located in Rye, New York. The adversary was able to view water levels, temperature, and the status of the sluice gate. The sluice gate control was disconnected for maintenance at the time of adversarial remote access, so the dam could not be remotely controlled.

[9] 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/.
[10] Additional information on Night Dragon was published as a McAfee white paper at https://www.mcafee.com/blogs/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf?msockid=073127cb95da6704354e31b3940f661e.
[11] Additional information on the Stuxnet worm can be found at https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[12] Additional information on the German steel mill incident can be found at http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.
[13] Additional information on the Saudi Aramco incident can be found at https://www.ibm.com/think/x-force/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks.
[14] The U.S. Department of Justice indictment for the New York dam attacks can be found at https://www.justice.gov/opa/file/834996/download.

- **[M][D] Dragonfly campaign, Havex.**[15] The energy sector was targeted during a multi-year cyber-espionage campaign that primarily used Havex malware. Havex was a remote access Trojan that used the Open Platform Communications (OPC) standard to gather information about connected ICS devices on a network. The campaigns were exploratory.
- **[M][D] Ukrainian power grid, BlackEnergy3.**[16] On December 23, 2015, Ukrainian power companies experienced a cyber attack that caused power outages affecting over 225,000 customers in Ukraine. Over 50 regional substations experienced malicious remote operation of their breakers. KillDisk malware was used to erase files on targeted systems, including at least one Windows-based HMI. The actors also corrupted the firmware of serial-to-Ethernet devices at the substations. This was the first known cyber attack on a power grid.
- **[M][D] Ukrainian power grid, Industroyer.**[17] On December 17, 2016, a cyber attack occurred at a substation outside Kyiv, Ukraine, resulting in an outage for customers of that substation for approximately one hour. This attack was the first known malware specifically designed to attack the power grid.
- **[M][I] Maersk, NotPetya.** In 2017, the NotPetya malware encrypted computers worldwide with no known decryption method. Although the malware initially targeted Ukrainian companies, it spread throughout the world with significant impacts to Maersk, FedEx, Merck, and Saint-Gobain. The malware destroyed data and disrupted shipping operations for Maersk, costing the company over $300 million in repairs and recovery efforts.
- **[M][D] Saudi Petrochem, TRITON.**[18] A petrochemical facility in Saudi Arabia was attacked using malicious software that targeted the industrial SIS. The SIS initiated a safe shutdown of the petrochemical process in 2017 when the triple-redundant processors identified mismatched code among the processors.
- **[M][I] Norsk Hydro, LockerGoga.**[19] In March 2019, Norsk Hydro experienced a cyber attack that used LockerGoga ransomware to encrypt its computer files. The aluminum and renewable energy company transitioned to manual operations and was transparent with the public on its progress to recovery. Norsk Hydro's transparency throughout the discovery and recovery process is well regarded by the security industry.
- **[M][I] Talman Software Ransomware Attack.**[20] In February 2020, a ransomware attack encrypted the central production systems of Talman Software, the primary technology

[15] Additional information on the Dragonfly/Energetic Bear Campaign can be found at https://www.osti.gov/servlets/purl/1505628.
[16] Additional information about the first Ukrainian power grid attack can be found at https://info.publicintelligence.net/NCCIC-UkrainianPowerAttack.pdf.
[17] Additional information on Industroyer malware can be found at https://us-cert.cisa.gov/ncas/alerts/TA17-163A.
[18] Additional information on the TRITON attack can be found at https://www.mandiant.com/resources/triton-actor-ttp-profile-custom-attack-tools-detections.
[19] 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.
[20] Additional information on Talman Software Ransomware attack can be found at https://theconversation.com/ransomware-attack-on-sheep-farmers-shows-theres-no-room-for-woolly-thinking-in-cyber-security-132882

provider for the Australasian textile sector. Because more than 75 % of the wool trade across Australia and New Zealand relied on Talman's proprietary platform, the blackout created a systemic single point of failure. The Australian Wool Exchange was forced to abruptly cancel regional auctions, freezing sales and stranding an estimated 70,000 bales of wool worth tens of millions of dollars.

- **[M][I] Colonial Pipeline.**[21] In May 2021, over 5,500 miles of pipeline transporting more than 100 million gallons per day of refined products to the East Coast of the U.S. shut down operations because of a ransomware attack. Colonial Pipeline was a victim of a ransomware cyber attack that encrypted its IT systems by exploiting a legacy VPN profile. Colonial made the decision to shut down the physical operations on the pipeline to contain any potential damage. Colonial Pipeline also decided to pay the ransom to the 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.[22]
- **[M][I] Ransomware targeting healthcare.**[23] A string of malware delivered via phishing attacks targeted the healthcare and public health sectors to disrupt services and steal data. In fall 2020, a CISA Alert (AA20-302A) was issued to warn healthcare and public health sector companies of the prevalence of these attacks.
- **[M][I] NEW Cooperative, BlackMatter.**[24] In September 2021, Iowa-based agricultural cooperative NEW Cooperative was targeted by a ransomware attack from the Russia-linked BlackMatter group. The hackers demanded a $5.9 million payment and disrupted IT systems used to manage food supply chains and livestock feeding schedules across many locations. The cooperative proactively took its networks offline to contain the malware and refused to pay the ransom. During the digital outage, growers and operators successfully maintained food supply continuity by reverting to manual paper hand tickets to weigh grain and track moisture. Investigators later determined the adversaries gained access by exploiting weak, shared employee credentials.
- **[M][I] Viasat KA-SAT, AcidRain.**[25] In February 2022, a destructive cyber attack targeted the ground management infrastructure of Viasat's KA-SAT satellite network to coincide with the Russian invasion of Ukraine. Adversaries deployed a novel data-wiping malware called "AcidRain" to overwrite the flash storage of tens of thousands of satellite modems, blinding communications. While intended to degrade military command-and-control, the attack caused massive collateral damage to European critical infrastructure. It knocked out remote monitoring, telemetry tracking, and automated SCADA controls

[21] Additional information on the Colonial Pipeline incident can be found at https://www.c-span.org/video/?512247-1/senate-homeland-security-hearing-colonial-pipeline-cyber-attack and https://www.hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf.
[22] Additional information can be found at https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
[23] Additional information on the series of malware targeting healthcare can be found at https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a.
[24] Additional information on the NEW Cooperative BlackMatter ransomware attack can be found at https://www.msspalert.com/news/new-cooperative-ransomware-attack-timeline-status-updates
[25] Additional information on the Viasat KA-SAT AcidRain attack can be found at https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

for 5,800 Enercon wind turbines in Germany. Additionally, the widespread network blackout halted satellite-linked precision tracking, automated machinery, and data feeds for thousands of regional agricultural operations dependent on the network.

- **[M][D] Ukrainian power grid, Industroyer2.**[26] In April 2022, Sandworm deployed Industroyer2 against a Ukrainian high-voltage electrical substation operator in a coordinated attack. Unlike the original Industroyer, which used multiple protocol modules, Industroyer2 was a single executable targeting the IEC 104 protocol used to communicate with industrial equipment. The attack also deployed CaddyWiper malware to destroy data on Windows systems and erase evidence of the intrusion. Ukrainian CERT and ESET identified and disrupted the attack before the substation outage could be fully executed, preventing a larger-scale power disruption.
- **[M][D] Unitronics defacement campaign.**[27] In November 2023, an Iranian-linked threat actor group known as CyberAv3ngers targeted internet-exposed Unitronics Vision Series PLCs across multiple countries, primarily at water and wastewater facilities, but also affecting other critical infrastructure sectors. The attackers exploited default credentials to gain access and used the legitimate Unitronics VisiLogic engineering software to download malicious projects to the devices, defacing HMI screens with politically motivated messaging and causing operational disruptions at multiple facilities.
- **[M][D] Ukrainian municipal district heating, FrostyGoop.**[28] In January 2024, a Russia-linked threat actor group targeted a municipal district energy company in Ukraine using FrostyGoop, the first known ICS malware to directly interact with OT systems via the Modbus TCP protocol. The attackers deployed malware that directly communicated with ENCO heating system controllers using the Modbus protocol to manipulate temperature measurements and cause system malfunctions. The attack left over 600 apartment buildings without heat during sub-zero temperatures for nearly two days before remediation was complete. The incident highlighted the risks of internet-exposed ICS devices communicating over Modbus and the limitations of traditional antivirus tools in detecting ICS-specific malware.
- **[M][I] Swiss Dairy Farm Robotic Milking Ransomware Attack.**[29] In August 2024, a ransomware attack encrypted the on-site computer systems of a dairy operation in Hagendorn, Switzerland. While the facility's automated milking robots continued functioning offline, the ransomware locked the farmer out of the localized server tracking the herd's vital signs and reproductive timelines. Because this critical data layer was blinded, the farmer failed to identify a pregnant cow in labor distress. The unborn calf died, and the mother cow suffered irreversible health deterioration and was euthanized.

[26] Additional information on Industroyer2 can be found at https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
[27] Additional information on Unitronics Defacement Campaign can be found at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
[28] Additional information on FrostyGoop can be found at https://www.sans.org/blog/whats-the-scoop-on-frostygoop-the-latest-ics-malware-and-ics-controls-considerations
[29] Additional information on Swiss Farm Ransomware attack can be found at https://www.csoonline.com/article/3484349/ransomware-attack-paralyzes-milking-robots-cow-dead.html

- **[M][D] Poland energy sector cyber incident.**[30] In December 2025, coordinated cyber attacks targeted over 30 distributed energy resources in Poland, including wind and solar farms, a combined heat and power plant, and a manufacturing company. Attackers gained initial access through internet-facing edge devices that lacked multi-factor authentication and used a combination of default-credential exploitation and wiper malware to corrupt firmware, destroy data, and disrupt visibility and communications between facilities and distribution system operators. The activity is attributed to a Russian state-sponsored threat cluster and represents the first publicly described destructive attack targeting distributed renewable energy resources at scale.

C.3.2. Structural Events

- **[N][D] Bellingham, Washington, gasoline pipeline failure.**[31] In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline and ignited 1.5 hours later, causing three deaths, eight injuries, and extensive property damage. The pipeline failure was exacerbated by control systems that were unable to perform control and monitoring functions. Immediately prior to and during the incident, the SCADA system exhibited poor performance, inhibiting the pipeline controllers from recognizing and responding to the development of an abnormal pipeline operation. A key recommendation from the NTSB report issued in October 2002 was to use an offline development and testing system to implement and test changes to the SCADA database.
- **[M][I] CSX train signaling system.**[32] In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the East Coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida, headquarters and shut down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, 10 Amtrak trains were affected in the morning. Trains between Pittsburgh, Pennsylvania, and Florence, South Carolina, were halted due to dark signals, and one regional Amtrak train from Richmond, Virginia, to Washington and New York was delayed by more than two hours. Long-distance trains were also delayed between four and six hours.
- **[N][D] Browns Ferry-3 PLC failure.**[33] In August 2006, TVA was forced to manually shut down one of its plant's two reactors after unresponsive PLC problems caused two water pumps to fail and threatened the stability of the plant itself. Although there were dual redundant PLCs, they were connected to the same Ethernet network. Later testing on the failed devices discovered that they would crash when they encountered excessive network traffic.

[30] Additional information on Poland Energy Sector Cyber Incident can be found at https://cert.pl/uploads/docs/CERT_Polska_Energy_Sector_Incident_Report_2025.pdf
[31] Additional information on the Bellingham, Washington, gasoline pipeline failure incident can be found at https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.
[32] Additional information on the CSX train signaling system incident can be found at https://www.informationweek.com/cyber-resilience/computer-virus-brings-down-train-signals.
[33] Additional information on the Browns Ferry -3 PLC failure incident can be found at https://www.informationweek.com/cyber-resilience/2006-shutdown-spurs-call-for-investigation-of-nuclear-cybersecurity.

C.3.3. Environmental Events

- **[N][I] Fukushima Daiichi nuclear disaster.**[34] The Great East Japan Earthquake on March 11, 2011, struck off the coast of Japan and sent a massive tsunami inland toward the nuclear plant. The tsunami compromised the plant's seawall, flooding much of the plant, including the location housing the emergency generators. This emergency power was critical for operating the control rooms and providing coolant water for the reactors. The loss of coolant caused the reactor cores to overheat to the point where the fuel's zirconium cladding reacted with water, releasing hydrogen gas and fueling large explosions in three of the four reactor buildings. This resulted in large-scale radiation leakage that has impacted plant employees, nearby citizens, and the local environment. Post-event analysis found that the plant's emergency response center lacked sufficient secure communication lines to provide information to other areas of the plant on key safety-related instrumentation.
- **[N][I] Global Navigation Satellite Systems (GNSS), Gannon Storm.**[35] On May 10, 2024, an extreme G5 geomagnetic storm impacted Earth's atmosphere, creating severe plasma disturbances in the ionosphere. The resulting space-weather anomalies severely degraded or entirely knocked out the Real-Time Kinematic (RTK) GPS tracking networks relied upon by modern precision agriculture. During the height of the spring corn-planting season, autonomous tractors and automated seeding machinery across the U.S. Midwest and Canada lost positional accuracy as RTK receivers drifted several feet off course, causing steering equipment to drive in circles. Because precision rows require sub-inch mapping to prevent crop gaps or fertilizer overlap, thousands of farmers were forced to completely suspend fieldwork and park their fleets. The non-cyber signal blackout ultimately caused an estimated $500 million in cumulative field damages and economic operational losses due to delayed planting windows.

C.3.4. Accidental Events

- **[N][I] NERC Enforcement Action.**[36] In 2019, a U.S. energy company was fined $10 million by NERC for cybersecurity violations that took place between 2015 and 2018. The inability to comply with U.S. standards for cybersecurity was seen as a risk to the security and reliability of the overall power system.
- **[N][D] NASA fire.**[37] 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.

[34] 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.
[35] Additional information on Gannon Storm can be found at https://www.agmanager.info/sites/default/files/pdf/Gannon_Corn_03-05-25.pdf
[36] For additional information about fines imposed on energy companies, see Enforcement Actions 2019 (nerc.com).
[37] For additional information on accidental OT losses from applying IT security controls in NASA, see Final Report - IG-17-011 (nasa.gov).

- **[N][D] Hatch Nuclear Power Plant.**[38] In 2008, the Hatch nuclear power plant in Georgia was forced into an emergency shutdown for forty-eight hours after a software update was installed on a single Windows computer. When the updated computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, the plant's automated safety systems triggered a shutdown.

[38] Additional information can be found at https://www.homelandsecuritynewswire.com/cyber-mishap-causes-nuclear-power-plant-shutdown

Appendix D. OT Security Organizations, Research, and Activities

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

D.1. Consortia and Standards

D.1.1. 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, users, and all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries. Below are relevant IEC Technical Committees (TCs) that contribute to the field of OT security.

https://www.iec.ch

D.1.1.1. IEC Technical Committee 57

The scope of TC 57 is to prepare international standards for power systems control equipment and systems, including energy management systems (EMSs), SCADA, 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.

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

The list of current working groups (WGs) within TC 57 includes:

- 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.1.1.2. IEC Technical Committee 65

The scope of TC 65 is to prepare international standards for the systems and elements used for industrial process measurement, control, and automation to coordinate standardization activities that affect the 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.

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

D.1.2. Institute of Electrical and Electronics Engineers, Inc. (IEEE)

IEEE inspires the global community to innovate for a better tomorrow through its more than 400,000 members in over 160 countries and its highly cited publications, conferences, technology standards, and professional and educational activities.

https://www.ieee.org/

Below are relevant IEEE subsocieties that contribute to the field of OT security.

D.1.2.1. IEEE Engineering in Medicine and Biology Security (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.1.2.2. IEEE Industrial Electronics Society (IES)

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

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

D.1.2.3. IEEE Power and 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.1.2.4. 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.

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.1.2.5. 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.1.2.6. 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, and maritime mobile services.

https://vtsociety.org

D.1.3. 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. It 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.1.3.1. 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.

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

D.1.3.2. 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 used by the International Electrotechnical Commission to produce the multi-standard ISA/IEC 62443 series, which are currently organized into four categories: General, Policies and Procedures, System, and Component.

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

D.1.3.3. ISASecure

The ISASecure program is a certification scheme certifying off-the-shelf automation and control systems to the ISA/IEC 62443 series of standards.

https://isasecure.org/

D.1.3.4. ISAGCA

ISAGCA is a collaborative forum to advance cybersecurity awareness, education, readiness, and knowledge sharing. The objectives of ISAGCA include the acceleration and expansion of standards, certification, education programs, advocacy efforts, and thought leadership.

https://isagca.org/

D.1.3.5. ISA-TR84.00.09, Cybersecurity Related to the Functional Safety Lifecycle

This document provides guidance on integrating the cybersecurity life cycle with the safety life cycle, as they relate to Safety Controls, Alarms, and Interlocks (SCAI), including safety instrumented systems (SISs). This scope includes the work processes and countermeasures used to reduce the risk posed by 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.1.4. International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is an independent, non-governmental international organization with 165-member national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, and 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.

https://www.iso.org/home.html

D.1.4.1. 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 assessing and treating information security risks tailored to the organization's needs. The requirements set out in ISO/IEC 27001 are generic and intended to be applicable to all organizations, regardless of type, size, or nature.

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

D.1.4.2. ISO 27002:2022

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

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

D.1.5. National Council of Information Sharing and Analysis Centers (ISACs)

Formed in 2003, the NCI is composed of 25 organizations and is a coordinating body designed to maximize information flow across private-sector critical infrastructures and with government. ISACs 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 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.

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

D.1.6. National Institute of Standards and Technology (NIST)

NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve 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 on NIST's technology, measurements, and standards. NIST's Information Technology Laboratory (ITL) 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.1.6.1. NIST SP 800 Series Cybersecurity Guidelines

The NIST SP 800 series on information technology reports on NIST ITL's research, guidance, and outreach efforts in computer security, as well as 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.

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

D.1.6.2. NIST SP 1800 Series Cybersecurity Practice Guides

The NIST SP 1800 series presents practical and usable solutions for applying standards-based cybersecurity approaches and best practices 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. An 1800 document can map capabilities to the Cybersecurity Framework and outline the steps needed for another entity or organization to recreate an example solution.

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

D.1.6.3. NIST Internal or Interagency Reports

NIST IR series documents are reports on research findings, including background information for FIPS and SPs.

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

D.1.7. NERC Critical Infrastructure Protection (CIP) Standards

The mission of the North American Electric Reliability Corporation (NERC) 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 U.S. Federal Energy Regulatory Commission and governmental authorities in Canada.

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 Critical Infrastructure Protection (CIP) standards subject to enforcement with two additional standards that are filed and pending regulatory approval.

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

D.1.8. 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 is led by the U.S. Department of Energy (DOE) and the National Renewable Energy Laboratory (NREL) and 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 program 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. These innovative technologies will also advance the state of the practice in demonstrating "security by design," thus ensuring that cybersecurity is built into renewable technologies and architectures 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 Risk Information Sharing Program (CRISP)

The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership that is 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 bidirectional 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 DOE's advanced sensors, threat analysis techniques, and expertise to better inform the energy sector of high-level cyber risks. This information is shared with voluntary utility participants who collectively deliver more than 80 % of the Nation's electricity. The Pacific Northwest National Laboratory (PNNL) plays a lead role at CRISP.

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

D.2.3. Cyber Testing for Resilient Industrial Control Systems (CyTRICS)

DOE CESER has partnered with the Idaho National Laboratory and other 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.2.4. 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 at no charge, including a virtual meeting space, document sharing, alerts, and instant messaging.

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

D.2.5. INL Cyber-Informed Engineering (CIE) and Consequence-Driven CIE (CCE)

The DOE and the Idaho National Laboratory 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 drive the inclusion of cybersecurity as a foundational element of risk management for engineering functions that are 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 its most critical functions and methods, as well as the means by which 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 and ensuring resiliency and response maturity within the design of the engineered system. 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.2.6. NIST Cyber-Physical Systems and Internet of Things Program

The definitions of cyber-physical systems (CPS) and IoT are converging over time to include a common emphasis on the interaction of 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's 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.2.7. NIST Cybersecurity for Smart Grid Systems Project

Smart grid cybersecurity must address both inadvertent compromises of the electric infrastructure due to user error, equipment failures, and natural disasters as well as 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 cybersecurity policies and measures in industry standards and develop 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 critical cybersecurity needs by promoting the technology transfer of best practices, standards, 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 collaborations in the cross-cutting issue of cybersecurity in the smart grid.

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

D.2.8. 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.2.9. 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.2.10. 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 develops 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.2.11. 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.2.12. NIST AI RMF Trustworthy AI in Critical Infrastructure Profile

NIST is developing an AI Risk Management Framework Profile that is tailored to critical infrastructure environments across IT and OT. It is intended to help operators apply the AI RMF to AI-enabled capabilities and communicate trustworthiness requirements to developers and stakeholders.

https://www.nist.gov/programs-projects/concept-note-ai-rmf-profile-trustworthy-ai-critical-infrastructure

D.2.13. NIST AI in Manufacturing

In December 2025, NIST awarded $20 million to the MITRE Corporation to establish two centers advancing AI-based technology solutions for U.S. manufacturing productivity and critical infrastructure cybersecurity, including AI-driven capabilities for detecting and responding to cyberthreats targeting essential services.

https://www.nist.gov/news-events/news/2025/12/nist-launches-centers-ai-manufacturing-and-critical-infrastructure

D.3. Tools and Training

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

CISA's 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's 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://www.cisa.gov/resources-tools/resources/commercial-facilities-sector-cybersecurity-framework-implementation

https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-cybersecurity-framework-implementation-guidance

https://www.cisa.gov/resources-tools/resources/dams-sector-cybersecurity-framework-implementation-guidance-2020

https://www.cisa.gov/resources-tools/resources/emergency-services-sector-cybersecurity-framework-implementation-guidance

https://www.cisa.gov/resources-tools/resources/nuclear-sector-cybersecurity-framework-implementation-guidance

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 activities with the potential to impact critical infrastructure computing networks, including current security issues, vulnerabilities, and exploits. CISA maintains a list of ICS-related Technical Information Papers (TIPs), Annual Reports (Year in Review), and third-party products that it considers to be of interest to persons engaged in protecting ICS.

https://www.cisa.gov/topics/industrial-control-systems

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 offered at no cost to the attendee.

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

D.3.5. CISA Known Exploited Vulnerabilities (KEV) Catalog

CISA's KEV catalog is a continuously updated list of CVEs with confirmed evidence of active exploitation, including ICS and SCADA-specific entries, and is regularly referenced in vendor advisories and OT security assessments. For OT asset owners, the catalog offers a more operationally relevant basis for prioritization based on confirmed exploitation activity, rather than relying on vulnerability scoring alone.

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

D.3.6. CISA/NCSC Secure Connectivity Principles for Operational Technology

Published in January 2026 by the UK National Cyber Security Centre (NCSC) in partnership with CISA, the FBI, and cybersecurity agencies across Australia, Canada, Germany, and the Netherlands, this joint guidance establishes eight principles for designing, securing, and managing connectivity in OT environments. The principles address remote access, boundary protection, network segmentation, and hardware-enforced controls, and provide architectural recommendations for OT environments.

https://www.ncsc.gov.uk/sites/default/files/documents/ncsc-secure-connectivity-for-operational-technology.pdf

D.3.7. CISA Secure by Design/Secure by Default

Initially published in April 2023 and updated in October 2023 with expanded principles and 17 international partner agencies, this joint guidance from CISA, the FBI, and NSA urges technology manufacturers to build security into products by default rather than leaving it to customers. For OT environments, the guidance is most directly applicable in the procurement context, giving asset owners a framework for evaluating and demanding that security be built into vendor products.

https://www.cisa.gov/securebydesign

D.3.8. 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://attack.mitre.org/matrices/ics/

D.3.9. MITRE D3FEND for OT

MITRE D3FEND is a knowledge graph cataloging defensive cybersecurity countermeasures and their relationships to adversary techniques, serving as a complement to ATT&CK. In December 2025, MITRE expanded D3FEND to cover OT environments with OT-specific artifacts, countermeasures, and mappings to ATT&CK for ICS.

https://d3fend.mitre.org/domain/ot/

D.3.10. MITRE EMB3D

EMB3D is a MITRE threat model that catalogs cybersecurity threats targeting embedded devices across critical infrastructure and OT environments, organizing threats by device hardware, system software, application software, and networking properties to help vendors and asset owners build tailored threat models. It cross-references ATT&CK for ICS, CWE, and CVE, and is maintained as a living, publicly available framework.

https://emb3d.mitre.org/

D.3.11. NIST Cybersecurity Framework 2.0

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 for reducing cyber risks to critical infrastructure based on existing standards, guidelines, and practices. In February of 2024, NIST published Version 2.0 of the Cybersecurity Framework.

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

D.3.12. 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 needed to safeguard critical infrastructure.

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

D.3.13. OWASP Operational Technology (OT) Top 10

The OWASP OT Top 10 is a community-developed reference document cataloging the most significant security risks facing OT environments, including industrial control systems and critical infrastructure. In contrast to the traditional OWASP Top 10, which is scoped to web applications, the OT Top 10 addresses the distinct threat landscape of cyber-physical environments, where security failures can result in physical damage, safety hazards, and operational disruption.

https://ot.owasp.org/

D.3.14. UFC 4-010-06, Cybersecurity of Facility-Related Control Systems (FRCS)

UFC 4-010-06 is a mandatory Core Unified Facilities Criteria document published by the Department of Defense in October 2023 that establishes cybersecurity requirements for the planning, design, and construction of facility-related control systems, including building control, utility, electronic security, and fire and life safety systems. It defines a five-step process for applying Risk Management Framework security controls to control system design, embedding cybersecurity into the design phase rather than retrofitting it after construction.

https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2023.pdf

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

- U.S. 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

- U.S. Department of Agriculture (USDA) – https://www.usda.gov
- U.S. 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

- U.S. 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

- U.S. 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

- U.S. 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
  - SD Pipeline-2021-01G - Enhancing Pipeline Cybersecurity. Transportation Security Administration – https://www.tsa.gov/sites/default/files/signed_security-directive-pipeline-2021-01g-and-transmittal-memo_508c.pdf
  - SD 1580-21-01E - Enhancing Rail Cybersecurity. Transportation Security Administration – https://www.tsa.gov/sites/default/files/signed_security-directive-1580-21-01e-and-transmittal-memo_508c.pdf
- Association of American Railroads – https://www.aar.org
- International Maritime Organization (IMO) – https://www.imo.org
  - Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems – https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf
  - MSC-FAL.1/Circ.3/Rev.3 - Guidelines on Maritime Cyber Risk Management – https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf
- International Association of Classification Societies (IACS) – https://iacs.org.uk
  - UR E26 - Cyber Resilience of Ships – https://iacs.org.uk/resolutions/ur-e/ur-e26-new/ur-e26-new
  - UR E27 - Cyber Resilience of Onboard Systems and Equipment – https://iacs.org.uk/resolutions/unified-requirements/ur-e/ur-e27-rev1

- SAE International – https://www.sae.org
  - ISO/SAE 21434:2021 - Road Vehicles - Cybersecurity Engineering – https://www.iso.org/standard/70918.html
  - SAE J1939 - Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document – https://www.sae.org/standards/j1939_202603-serial-control-communications-heavy-duty-vehicle-network-top-level-document
- Department of Defense (DoD) – https://www.war.gov/
  - MIL-STD-1553 - Digital Time Division Command/Response Multiplex Data Bus – https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=36973

D.4.10. Water and Wastewater

- U.S. 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
- WaterISAC – https://www.waterisac.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 that was initially founded to showcase advanced and highly technical content to the ICS audience. S4 has since grown to accommodate other ICS security content but remains a premier venue to present technical findings within OT security.

https://s4xevents.com/

D.5.2. IFIP Working Group 11.10 on Critical Infrastructure Protection

The International Federation for Information Processing (IFIP) Working Group 11.10 is an active international community of scientists, engineers, and practitioners dedicated to advancing state-of-the-art research and practices in the emerging field of critical infrastructure protection.

http://ifip1110.org/Conferences/

D.5.3. SecurityWeek's ICS Cyber Security Conference

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

https://www.icscybersecurityconference.com/

Appendix E. OT Overlay

> The OT overlay is a partial tailoring of the controls and control baselines in SP 800-53r5 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 and to serve as a model for other overlays. Further tailoring can 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 800-53r5. Duplicating Appendix F of SP 800-53 would increase the size of this publication significantly, so it is not included here.

Overlays provide a structured approach to help organizations tailor control baselines and develop specialized security plans that can be applied to specific mission and 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 SP 800-82r4 Operational Technology Overlay ("NIST SP 800-82r4 OT Overlay"). It is based on SP 800-53r5 [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.

E.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 and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

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 2.4 provides an overview of various OT systems, such as SCADA, DCS, PLCs, BASs, PACSs, and IIoT.

E.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 non-governmental 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, so controls that are 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.

E.3. Overlay Summary

Table 18 provides a summary of the controls and control enhancements from SP 800-53r5, 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 that is supplemental to the baselines provided in SP 800-53B.
- ~~Strikethrough~~ indicates that a control or control enhancement has been removed from this baseline compared to the baselines provided in 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 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 18.

6884 **Table 18. 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)**
AT-3	Role-Based Training	**AT-3**	**AT-3**	**AT-3**
AT-4	Training Records	AT-4	AT-4	AT-4

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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)
CM-5	Access Restrictions for Change	**CM-5**	**CM-5**	**CM-5** (1)

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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**

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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)**
IA-11	Re-authentication	IA-11	IA-11	IA-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 (1)
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)

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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
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		

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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		
PM-5	System Inventory	PM-5		
PM-6	Measures of Performance	PM-6		
PM-7	Enterprise Architecture	PM-7		
PM-8	Critical Infrastructure Plan	**PM-8**		
PM-9	Risk Management Strategy	PM-9		
PM-10	Authorization Process	PM-10		
PM-11	Mission and Business Process Definition	PM-11		
PM-12	Insider Threat Program	PM-12		
PM-13	Security and Privacy Workforce	PM-13		
PM-14	Testing, Training, and Monitoring	PM-14		
PM-15	Security and Privacy Groups and Associations	**PM-15**		
PM-16	Threat Awareness Program	**PM-16**		
PM-17	Protecting Controlled Unclassified Information on External Systems	**PM-17**		
PM-18	Privacy Program Plan	PM-18		
PM-19	Privacy Program Leadership Role	PM-19		
PM-20	Dissemination of Privacy Program Information	PM-20 (1)		
PM-21	Accounting of Disclosures	PM-21		
PM-22	Personally Identifiable Information Quality Management	PM-22		
PM-23	Data Governance Body	PM-23		
PM-24	Data Integrity Board	PM-24		

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research	PM-25		
PM-26	Complaint Management	PM-26		
PM-27	Privacy Reporting	PM-27		
PM-28	Risk Framing	PM-28		
PM-29	Risk Management Program Leadership Roles	PM-29		
PM-30	Supply Chain Risk Management Strategy	PM-30 (1)		
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

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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
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

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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
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

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
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

E.4. Tailoring Considerations

The OT overlay in this publication leverages the SP 800-53B control baselines that account for the unique characteristics of OT systems, such as an increased need for availability, safety, and environmental or 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 the addition of controls that are relevant for OT environments. Organizations can use this overlay as a starting point and further tailor controls to meet specific operational needs to address the 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 the selection of compensating controls. Compensating controls in the OT environment may be required when the OT cannot support certain controls or control enhancements or when the organization determines that it is not advisable to implement controls or control enhancements due to potential adverse impacts to performance, safety, or reliability. Compensating controls may supplement the baseline or act as alternatives that provide equivalent or comparable

protection. For example, if controls or control enhancements require automated mechanisms that 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 800-53r5 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 (see "Control Tailoring" in Sec. 3.3 of [SP800-37r2]).

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 documented in the security plan for the OT and describe:

- Why the baseline control could not be implemented
- How the compensating controls provide equivalent security capabilities for OT systems
- The risk acceptance for any residual risk that results from using the compensating controls instead of the baseline control

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.

E.5. OT Communication Protocols

The unique network properties within OT may warrant specific attention when applying certain controls. Many of the controls in SP 800-53r5 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 creates 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.

E.6. Definitions

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

E.7. Detailed Overlay Control Specifications

This overlay is based on [SP800-53r5], which provides a catalog of security and privacy controls, and [SP800-53B]. The controls are customizable and implemented as part of an organization-wide process that manages security and privacy risks. 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 and business needs. The documents also describe how to develop specialized sets of controls or overlays that are tailored for specific types of mission and business functions, technologies, or environments of operation. Finally, the catalog controls address security from both a functionality perspective (i.e., the strength of security and privacy functions and mechanisms provided) and an assurance perspective (i.e., 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 use sound system and security engineering principles and are sufficiently trustworthy.

In preparation for selecting and specifying the appropriate controls for organizational systems and their respective environments of operation, organizations should 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 impacts on an organization or people (i.e., employees and/or the public) should certain events occur that 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 to assess the risk to an organization.

This overlay provides OT Discussions 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 Sec. 3 of SP 800-53r5 should be used in conjunction with the OT Discussions in this overlay. This overlay contains a tailoring of the control baselines, and its specification may be more stringent or less stringent than the original control baseline specification. It is high-level, applicable to all OT environments, can be applied to multiple systems, and 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 NIST IR).

Figure 21 uses the AU-4 control as an example of the format and content of the detailed overlay control specifications, including:

- 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 that the control is selected in SP 800-53r5. "Add" indicates that the control is added to a baseline in the OT overlay. A blank cell indicates that the control is not selected. "~~Remove~~" indicates that 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**

❷ CNTL NO.	❸ CONTROL NAME *Control Enhancement Name*	❹ SUPPLEMENTED ❻ CONTROL 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. The 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 when 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 and accounts 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 that reside on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals, including severe degradation or loss of mission capability, major damage to organizational assets, or harm to individuals involving the loss of life or life-threatening injuries.

Fig. 21. Detailed overlay control specifications illustrated

E.7.1. ACCESS CONTROL – AC

E.7.1.1. Tailoring Considerations for the Access Control Family

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

When 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 large facility footprint or geographic area and into unobserved spaces, such as mechanical or electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.

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 support this control objective.

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

Control Enhancement: (2) OT Discussion: When 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 time frames in which users log out of accounts in the policy. Automatic enforcement is not addressed by this control enhancement. Organizations determine whether this control enhancement is appropriate for the mission and/or functions of the OT system and define the timeframe or scenarios. If no time frames or scenarios apply, the organization-defined parameter reflects as much.

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

Control Enhancement: (13) OT Discussion: Close coordination occurs between OT, 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 affect OT operational performance. Example compensating controls include encapsulation. The 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 when 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 and accounts 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 that reside on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals, including severe degradation or loss of mission capability, major damage to organizational assets, or harm to individuals involving the 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. The inspection of message content may enforce information flow policy. For example, industrial OT protocols may be restricted by using inbound and outbound traffic rules on a network control device between OT and IT networks. For non-routable communication (e.g., serial connections), devices may be configured to limit commands to and from specific tags within the OT device. The 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**

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
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: When OT components (e.g., PLCs) cannot support the logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations, 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 logon 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) that are 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 consider 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 in which users interact with system displays. This control may be tailored appropriately if 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 a need to know the displayed information.

Control Enhancement: (1) OT Discussion: Physical protection may be employed to prevent access to a display or the attachment of a display. When 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

OT Discussion: 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: When 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. If OT devices lack the ability to support modern encryption, additional devices (e.g., VPNs) can be added. 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 managing risk and 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, the loss of high-value assets, the 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: When 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: The implementation of authentication and encryption is driven by the OT environment. If devices and users cannot all be authenticated and encrypted due to operational or technology constraints, compensating controls may 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. If confidentiality is a concern, 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

OT Discussion: 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, the granularity of an 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 establish 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 (e.g., vendor, 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

OT Discussion: 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.

E.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 reviews 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, such as a PLC still in programming mode when it is expected to be in run mode, process trips with an 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 identifying potentially suspicious communications and anomalous behaviors as well as the 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 reviews 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

OT Discussion: No OT Discussion for this control.

E.7.3. AUDITING AND ACCOUNTABILITY – AU

E.7.3.2. Tailoring Considerations for the Audit Family

When 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 whether 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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

Rationale for adding AU-4 (1) to LOW, MOD, and HIGH baselines: Organizational requirements may require the 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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: Compensating controls may include manual mechanisms or procedures. If audit records cannot be feasibly collected for devices, 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

OT Discussion: 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: Compensating controls may 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

OT Discussion: 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, such as 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

OT Discussion: 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**

OT Discussion: No OT Discussion for this control.

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

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

E.7.4. ASSESSMENT, AUTHORIZATION, AND MONITORING – CA

E.7.4.3. Tailoring Considerations for the Security Assessment and Authorization Family

When the OT cannot support the 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 or 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 offline 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 for this control.

Control Enhancement: (2) OT Discussion: The organization conducts risk analysis to support the selection of an assessment target (e.g., the live system, an offline replica, 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 a risk-benefit analysis to determine whether an OT should be connected to other systems. 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 systems; 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

OT Discussion: 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 or group designing and conducting the continuous monitoring for the OT systems implements a monitoring program that is 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 monitor event logs manually on a specified frequency less often for lower-risk, isolated systems 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 offline before testing can be conducted. If OT systems are taken offline 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, and it may not be feasible to identify independent personnel with the appropriate skillset or knowledge to perform penetration testing on an OT environment. While an independent penetration test agent or 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 and then document those connections. The AO fully understands the potential risks associated with approving individual connections or approving a class of components to be connected. For 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, Ethernet) require individual approval. Decisions to accept risk are documented.

E.7.5. CONFIGURATION MANAGEMENT – CM

E.7.5.4. Tailoring Considerations for the Configuration Management Family

When 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

OT Discussion: 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 considers OT-specific requirements when determining the frequency and/or circumstances for reviewing system changes. For example, safety instrumented systems may be justified for the 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 impact 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. For example, many PLCs have key switches that allow the device to be placed in a programming mode or 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

OT Discussion: 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
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION*		**Select**	**Select**

OT Discussion: The organization implements least functionality by allowing only the specified functions, protocols, and/or services required for OT operations. For non-routable protocols (e.g., 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

OT Discussion: 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 the internal and external resources (e.g., contractors, integrators) 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

OT Discussion: 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

OT Discussion: 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.

E.7.6. CONTINGENCY PLANNING – CP

E.7.6.5. Tailoring Considerations for the Contingency Planning Family

OT systems often contain a physical component at a fixed location that may not be relocated logically, and some replacement components may not be readily available. The continuance of essential mission and business functions with little or no loss of operational continuity may not be possible. When the organization cannot provide necessary essential services, support, or automated mechanisms during contingency operations, it should provide 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 alerting the operator of the failure and then doing nothing, alerting the operator and then safely shutting down the industrial process, or alerting the operator and then maintaining 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

OT Discussion: 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**

OT Discussion: 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

OT Discussion: 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 alternate 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 alternate 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

OT Discussion: 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 often depends on the resources needed to appropriately represent the environment, such as the availability of spare devices and testing equipment. 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 considering whether system state variables should be restored to their initial values or to the values before the disruption (e.g., valves restored to full open, full closed, or to settings prior to the 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 time frames 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

OT Discussion: 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.

E.7.7. IDENTIFICATION AND AUTHENTICATION – IA

E.7.7.6. Tailoring Considerations for the Identification and Authentication Family

Before implementing controls in the IA family, consider the trade-offs among security, privacy, latency, performance, and throughput. For example, the organization considers whether latency induced from the use of authentication mechanisms that employ cryptography would adversely impact the operational performance of the OT.

When 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: When 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 that 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 the 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 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 whether 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
IA-4 (4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*		**Select**	**Select**

OT Discussion: 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 in certain OT environments, identifiers (e.g., badges) may have different markings that 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 about 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

OT Discussion: 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: Compensating controls may include implementing support that is 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

OT Discussion: 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**
IA-12 (4)	*IDENTITY PROOFING | IN-PERSON VALIDATION AND VERIFICATION*			**Select**
IA-12 (5)	*IDENTITY PROOFING | ADDRESS CONFIRMATION*		**Select**	**Select**

OT Discussion: Identity proofing is likely performed by different departments within the organization. Existing organizational systems (e.g., HR or IT processes) should be leveraged to perform this control.

Control Enhancement: (1) OT Discussion: 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.

Control Enhancement: (2) (3) (4) (5) OT Discussion: If the organization already performs these controls, existing organizational processes should be leveraged. For example, HR may provide a system for tracking identity evidence. OT does not need to develop an independent system for achieving this control.

Rationale for adding IA-12 (1) to HIGH baseline: A supervisor or sponsor should be made aware of any access that an employee has to the OT environment since unauthorized or accidental access could affect the physical process.

E.7.8. INCIDENT RESPONSE – IR

E.7.8.7. 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**

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: As part of the incident handling capability, the organization coordinates with external vendors, integrators, or suppliers as necessary to ensure that they have the capability to address events that are specific to embedded components and devices.

Control Enhancement: (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

OT Discussion: 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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

E.7.9. MAINTENANCE – MA

E.7.9.8. 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.

When 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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

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*		Add	Add
MA-4 (3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION*			**Select**

OT Discussion: No OT Discussion for this control.

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

Control Enhancement: (3) OT Discussion: 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 nonlocal maintenance and diagnostic activities.

Rationale for adding MA-4 (1) to MOD and HIGH baselines: OT environments often depend 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

OT Discussion: 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

OT Discussion: 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 and 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 have 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.

E.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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

E.7.11. PHYSICAL AND ENVIRONMENTAL PROTECTION – PE

E.7.11.9. Tailoring Considerations for the Physical and Environmental Protection Family

Physical and environmental protections are often used as a compensating control for many OT systems, so 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

OT Discussion: 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 and access requirements in emergency situations. During an emergency, the organization may restrict access to OT facilities and assets to authorized individuals only. OT systems are often constructed of devices that 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

OT Discussion: 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

OT Discussion: 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*		Add	Select

OT Discussion: No OT Discussion for this control.

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

Rationale for adding PE-6 (4) to MOD baseline: 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

OT Discussion: 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

OT Discussion: 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*			

OT Discussion: 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

OT Discussion: 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 (e.g., HVAC, process, or lighting systems) or can be a stand-alone 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. 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 OT's 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 the use of shutoff and isolation valves are procedural actions and specific types 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. 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, routers, or switches or short out the alarms, egress systems, emergency lighting, or 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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 that manage OT equipment may choose to use EMP protection to prevent electromagnetic threats from adversaries or the environment. 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 information that is processed, stored, or transmitted. Component markings can be useful for 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 perform a very different function. Visible differentiation between components that perform different functions can help reduce reliability incidents due to maintenance errors.

E.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

OT Discussion: 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**			

OT Discussion: Organizations need to document known operational procedures and explore 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-8 (1)	*SECURITY AND PRIVACY ARCHITECTURES | DEFENSE IN DEPTH*			

OT Discussion: No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: 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**			

OT Discussion: If the architecture allows for it, consider centrally managing flaw remediation, malicious code protection, logging, and incident detection.

PL-10 BASELINE SELECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-10	**Baseline Selection**	Select	Select	Select

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

E.7.13. ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS – PM

E.7.13.10. Characteristics of the Organization-Wide Information Security Program Management Control Family

Organization-wide information security program management controls are deployed to support 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 the 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**

OT Discussion: 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**

OT Discussion: 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**

OT Discussion: 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**

OT Discussion: No OT Discussion for this control.

PM-5 SYSTEM INVENTORY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-5	**System Inventory**

OT Discussion: No OT Discussion for this control.

PM-6 MEASURES OF PERFORMANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-6	**Measures of Performance**

OT Discussion: No OT Discussion for this control.

PM-7 ENTERPRISE ARCHITECTURE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-7	**Enterprise Architecture**

OT Discussion: No OT Discussion for this control.

PM-8 CRITICAL INFRASTRUCTURE PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-8	**Critical Infrastructure Plan**

OT Discussion: Organizations should be familiar with the 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**

OT Discussion: No OT Discussion for this control.

PM-10 AUTHORIZATION PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-10	**Authorization Process**

OT Discussion: 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**

OT Discussion: No OT Discussion for this control.

PM-12 INSIDER THREAT PROGRAM

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-12	**Insider Threat Program**

OT Discussion: 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**

OT Discussion: 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**

OT Discussion: 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 SSAs, ISACs, 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 for coordinating and integrating the operational elements involved in cybersecurity and communications reliance. 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 agencies and other organizations that support the Government and process controlled unclassified information (CUI).

PM-18 PRIVACY PROGRAM PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-18	**Privacy Program Plan**

OT Discussion: 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**

OT Discussion: 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*

OT Discussion: No OT Discussion for this control.

PM-21 ACCOUNTING OF DISCLOSURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-21	**Accounting of Disclosures**

OT Discussion: 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**

OT Discussion: No OT Discussion for this control.

PM-23 DATA GOVERNANCE BODY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-23	**Data Governance Body**

OT Discussion: No OT Discussion for this control.

PM-24 DATA INTEGRITY BOARD

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-24	**Data Integrity Board**

OT Discussion: 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**

OT Discussion: No OT Discussion for this control.

PM-26 COMPLAINT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-26	**Complaint Management**

OT Discussion: No OT Discussion for this control.

PM-27 PRIVACY REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-27	**Privacy Reporting**

OT Discussion: No OT Discussion for this control.

PM-28 RISK FRAMING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-28	**Risk Framing**

OT Discussion: 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**

OT Discussion: 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*

OT Discussion: No OT Discussion for this control.

PM-31 CONTINUOUS MONITORING STRATEGY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-31	**Continuous Monitoring Strategy**

OT Discussion: No OT Discussion for this control.

PM-32 PURPOSING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-32	**Purposing**

OT Discussion: No OT Discussion for this control.

E.7.14. PERSONNEL SECURITY – PS

E.7.14.11. 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, and 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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.

E.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: 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

OT Discussion: 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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-5 (11)	*VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM*	**Select**	**Select**	**Select**

OT Discussion: The organization makes a risk-based determination about how to monitor or scan its system for vulnerabilities. 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, NIST NVD). Production may need to be taken offline 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 related to systems and configurations. Locations that may need to be monitored or scanned include technical forums, blogs, and vendor or 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. Federal and non-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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

E.7.16. SYSTEM AND SERVICES ACQUISITION – SA

E.7.16.12. Tailoring Considerations for the System and Services Acquisition Family

If 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

OT Discussion: 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*			

OT Discussion: No OT Discussion for this control.

Control Enhancements: (1) OT Discussion: Organizations that do not maintain local pre-production environments and utilize a third-party integrator should ensure that contracts are developed to limit 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 capabilities 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, so 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 (e.g., legal, regulatory) 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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**

OT Discussion: Personnel with knowledge of security and privacy requirements are included in the developer's change management process.

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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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 supporting the operation of such system components and consider additional compensating controls to mitigate against known threats and vulnerabilities to unsupported system components.

E.7.17. SYSTEM AND COMMUNICATIONS PROTECTION – SC

E.7.17.13. Tailoring Considerations for the System and Communications Protection Family

The use of cryptography is determined after careful consideration of security needs and 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 for cryptographic functions, compensating controls (e.g., encapsulations) may be used to meet the intent of the control.

When 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 and 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. Compensating controls may include 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. Compensating controls may include engineering 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 the prioritization of DoS protection and the 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

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

OT Discussion: 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 impacts that are specifically relevant to the 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 the 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 are common practices 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**

OT Discussion: 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 the confidentiality and integrity of the information. Compensating controls may 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~~

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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: Secure name/address resolution services should be used only after careful consideration and verification that they do not adversely affect the OT's operational performance.

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: Secure name/address resolution services should be used only after careful consideration and verification that they do not adversely affect the OT's operational performance.

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: Secure name/address resolution services should be used only after careful consideration and verification that they do not adversely affect the OT's operational performance.

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 that 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 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: Cryptographic mechanisms are implemented only after careful consideration and verification that they do not adversely affect the OT's operational performance. When cryptographic mechanisms are not feasible on certain OT devices, compensating controls may include 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*			

OT Discussion: No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: Organizations consider separate physical domains for privileged functions, such as those that affect 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**

OT Discussion: 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 across OT systems to enable accurate troubleshooting and forensic analysis.

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 systems employ suitable mechanisms (e.g., GPS, IEEE 1588) for timestamps.

Rationale for adding SC-45 to LOW, MOD, and HIGH baselines: Organizations may find relative system time beneficial for many OT systems to ensure the safe and reliable delivery of essential functions. Time synchronization can also make root cause analysis more efficient by ensuring that audit logs from different systems are aligned, enabling organizations to have an accurate view of events across multiple systems when logs are aggregated.

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: Organizations consider which systems require alternate communication paths to ensure that a loss of communication does not lead to an unacceptable loss of view or control or to a safety event.

Rationale for adding SC-47 to HIGH baseline: For continuity of operations during an incident, organizations should consider establishing alternate communication paths for command-and-control purposes to continue to operate and take appropriate actions for high-impact systems when the loss of availability or integrity may result in severe or catastrophic adverse impacts, including impacts to 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**			

OT Discussion: 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.

E.7.18. SYSTEM AND INFORMATION INTEGRITY – SI

E.7.18.14. Tailoring Considerations for the System and Information Integrity Family

When 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**

OT Discussion: 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

OT Discussion: Flaw remediation, or patching, is complicated since many OT employ OSs and other software that are no longer maintained by the vendors. OT operators may also lack the resources or capability to test patches and depend on vendors to validate a patch's operability. Sometimes, the organization has no choice but to accept additional risk if no vendor patch is available, if patching requires additional time to complete validation or testing, or if 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 that the OT can identify exploitation of the flaw). Testing remediation of flaws in 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: Malicious code protection should be deployed only after careful consideration and verification that it does not adversely affect OT operations. Malicious code protection tools should be configured to minimize their potential impact on OT (e.g., by employing notification rather than quarantine). Compensating controls may 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 the use of monitoring tools and techniques does not adversely affect OT operational performance. Compensating controls may include deploying sufficient network, process, and physical monitoring.

Control Enhancement: (2) OT Discussion: When the OT cannot support the use of automated tools for 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 manually 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/news-events/ics-advisories. 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 in accordance with 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**
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**

OT Discussion: The organization determines whether the use of integrity verification applications would adversely affect the operation of the ICS and employs compensating controls (e.g., manual integrity verifications that do not affect performance).

Control Enhancements: (1) OT Discussion: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the OT.

Control Enhancement: (2) OT Discussion: When the organization cannot employ automated tools that provide notifications about integrity discrepancies, the organization employs nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

Control Enhancement: (5) OT Discussion: Shutting down and restarting the ICS may not always be feasible upon identification of an anomaly. These actions should be scheduled in accordance with ICS operational requirements.

Control Enhancement: (7) OT Discussion: When the ICS cannot detect unauthorized security-relevant changes, the organization employs compensating controls (e.g., manual procedures) in accordance with the general tailoring guidance.

Control Enhancement: (15) OT Discussion: Code authentication provides assurance that the software and firmware have not been tampered with. If automated mechanisms are not available, organizations can manually verify code authenticity using a combination of techniques, including verifying hashes, downloading from reputable sources, verifying version numbers with the vendor, or testing software and firmware in offline or test environments.

SI-8 SPAM PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-8	**Spam Protection**		**Select**	**Select**
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

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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**

OT Discussion: 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 that are not manifest in other environments to become effective. 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 the 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 in OT for operational reasons.

SI-16 MEMORY PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-16	**Memory Protection**		**Select**	**Select**

OT Discussion: 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 account for potential impacts on human safety, physical systems, and the environment. A related control is CP-6.

Rationale for adding SI-17 to LOW, MOD, and HIGH baselines: This control provides a framework for the organization to define its policies and procedures for handling failures and other incidents. Creating a written record of the decision process for selecting incidents and appropriate responses in light of a changing operational environment is part of risk management.

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 incorporate information diversity into their designs to meet reliability requirements. Some examples of information diversity for an OT system include sensor voting and state estimation.

E.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 policies and procedures for OT should consider both components received and components produced. Many OT systems use legacy components that cannot meet modern supply chain expectations. Appropriate compensating controls should be developed to achieve organizational 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

OT Discussion: 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*			

OT Discussion: 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**

OT Discussion: No OT Discussion for this control.

Control Enhancement: (1) OT Discussion: Vendor relationships and spare parts strategies are developed to ensure that 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 and have a limited number of vendors or suppliers for 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

OT Discussion: 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

OT Discussion: 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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SR-9 (1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE*			Select

OT Discussion: 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

OT Discussion: 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

OT Discussion: 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

OT Discussion: No OT Discussion for this control.

Appendix F. Applying the Risk Management Framework to OT Systems

The NIST Risk Management Framework (RMF) applies the risk management process and concepts (i.e., framing risk, assessing risk, responding to risk, and monitoring risk) to systems and organizations. The following subsections describe the process of applying the RMF to OT and include a brief description of each step and task, the intended outcome of each task, task mappings to other standards and guidelines applicable to OT (e.g., CSF 2.0, IEC 62443), and OT-specific implementation guidance. Some tasks are optional, and not all tasks include OT-specific considerations or guidance.

The RMF steps in Fig. 22, while shown sequentially, can be implemented in a different order to be consistent with established management and system development life cycle processes.

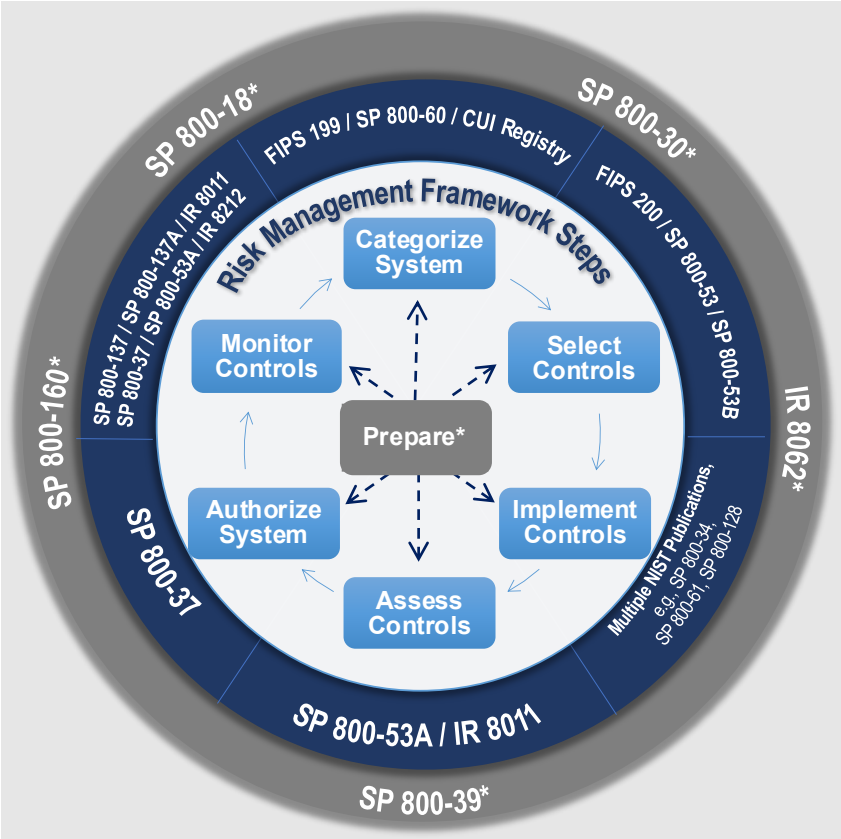

Fig. 22. Risk Management Framework steps

F.1. Prepare

The purpose of the Prepare step is to carry out essential activities at the organizational, mission and business process, and system levels to help the organization manage its security and privacy risks using the RMF. The Prepare step leverages activities that are already being conducted within cybersecurity programs to emphasize the importance of having organization-wide governance and resources in place to support risk management. Table 19 provides details on applying the Prepare step to OT.

8240 **Table 19. Applying the RMF Prepare step to OT**

Tasks	Outcomes	OT-Specific Guidance
Organizational and Mission and Business Process Levels		
TASK P-1 RISK MANAGEMENT ROLES	Individuals are identified and assigned key roles for executing the RMF. [*Cybersecurity Framework*: **GV.RR-02; GV.SC-02**] [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 the Process/Plant Manager, Process Control Engineer, Operator, Functional Safety Engineer, Maintenance Personnel, and Process Safety Manager.
TASK P-2 RISK MANAGEMENT STRATEGY	A risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established. [*Cybersecurity Framework*: **GV.RM; GV.SC-01; GV.OV-03**] [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; GV.SC-07**] [IEC 62443-2-1: **Event1.9; ORG 1.3; 2.1]**	
TASK P-4 ORGANIZATIONALLY TAILORED CONTROL BASELINES AND CYBERSECURITY FRAMEWORK PROFILES (OPTIONAL)	Organizationally tailored control baselines and/or Cybersecurity Framework profiles are established and made available. [*Cybersecurity Framework*: **Profile**]	An organizationally tailored control baseline for OT systems can be developed to address mission and business needs, unique operating environments, and/or other requirements.
TASK P-5 COMMON CONTROL IDENTIFICATION	Common controls that are available for inheritance by organizational systems are identified, documented, and published.	Common controls available for inheritance may adversely impact OT system operation. Consider whether common controls can be applied to OT systems effectively, safely, and without adverse impacts on OT system operation.
TASK P-6 IMPACT-LEVEL PRIORITIZATION (OPTIONAL)	A prioritization of organizational systems with the same impact level is conducted. [*Cybersecurity Framework*: **ID.AM-05; GV.OC-04**] [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; GV.SC-09**] [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	Mission and business functions and processes that the system is intended to support are identified. [*Cybersecurity Framework*: **Profile**; **Implementation Tiers**; **GV.OC; ID.AM-03**] [IEC 62443-2-1: **ORG1.6; AVAIL 1.2; AVAIL 1.1**]	When mapping OT and IT processes, the information flows and protocols should also be documented.
TASK P-9 SYSTEM STAKEHOLDERS	The stakeholders with an interest in the system are identified. [*Cybersecurity Framework*: **GV.OC-02; GV.RR-02**]	Example OT personnel include the 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-05**]	
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-03**; **ID.AM-04; ID-AM-08**]	
TASK P-14 RISK ASSESSMENT – SYSTEM	A system-level risk assessment is completed, or an existing risk assessment is updated. [*Cybersecurity Framework*: **ID.RA; GV.SC-07**]	Risk assessments, including performance/load testing and penetration testing, are conducted on the OT systems with care to ensure that OT operations are not adversely impacted by the testing process.
TASK P-15 REQUIREMENTS DEFINITION	Security and privacy requirements are defined and prioritized. [*Cybersecurity Framework*: **GV.PO-01; GV.OC-03]**	

Tasks	Outcomes	OT-Specific Guidance
TASK P-16 ENTERPRISE ARCHITECTURE	The placement of the system within the enterprise architecture is determined.	Group OT components by function or sensitivity level to optimize cybersecurity control implementation.
TASK P-17 REQUIREMENTS ALLOCATION	Security and privacy requirements are allocated to the system and the environment in which the system operates. [*Cybersecurity Framework*: **GV.PO-01**]	As security and privacy requirements are allocated to the OT system, impacts 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*: **GV.PO-01; ID.AM-02**]	

F.2. Categorize

In the Categorize step, the potential adverse impacts of the loss of confidentiality, integrity, and availability of the information and system are determined. For each information type and system under consideration, the three security objectives (i.e., confidentiality, integrity, and availability) are associated with one of three levels of potential impacts of a security breach. Of the three security objectives, availability is generally the greatest concern for an OT. The standards and guidance for this categorization process can be found in FIPS 199 [FIPS199] and 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 that controls 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 20 provides details on applying the RMF Categorize step to OT.

Table 20. 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-01**; **ID.AM-05; GV.OC-04**] Security categorization results are documented in the security, privacy, and SCRM plans. [*Cybersecurity Framework*: **Profile**] Security categorization results are consistent with the enterprise architecture and commitment to protecting organizational missions, business functions, and mission and business processes. [*Cybersecurity Framework*: **Profile**] Security categorization results reflect the organization's risk management strategy.	OT and IT systems may have different categorization criteria. System information and the system process (e.g., chemical production) should be considered during the security categorization.
TASK C-3 SECURITY CATEGORIZATION REVIEW AND APPROVAL	The security categorization results are reviewed, and the categorization decision is approved by senior leaders in the organization.	

F.3. Select

The purpose of the Select step is to select the initial controls to protect the system commensurate with risk. The control baselines are the starting point for the control selection process and are chosen based on the security category and associated impact level of the systems identified in the Categorize step. 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 SP 800-53B, Appendix C.

In general, overlays are intended to reduce the ad hoc tailoring of baselines 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 SP 800-53 controls that provides tailored baselines for low-impact, moderate-impact, and high-impact OT. These tailored baselines are starting specifications and recommendations that can be applied to specific OT by responsible personnel.

OT owners can tailor the overlay from Appendix F when it is not possible or feasible to implement specific controls. The use of overlays does not in any way preclude organizations from performing further tailoring (i.e., overlays can also be subject to tailoring) to reflect organization-specific needs, assumptions, or constraints. However, all tailoring activities should primarily focus on meeting the intent of the original controls whenever possible or feasible. For example, when the OT cannot support or the organization determines that it is not advisable to implement particular controls or control enhancements in an OT (e.g., performance, safety, or reliability are adversely impacted), the organization should provide a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the OT and why the related baseline controls could not be employed. If the OT cannot support the use of automated mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance in Sec. 3.3 of 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 21 provides additional details on applying the RMF Select step to OT.

8317 **Table 21. Applying the RMF Select step to OT**

Tasks	Outcomes	OT-Specific Guidance
TASK S-1 CONTROL SELECTION	Control baselines necessary to protect the system commensurate with risk are selected. [*Cybersecurity Framework*: **Profile**]	OT systems can leverage the OT control baselines identified in Appendix F as a starting point or an organization-defined control selection approach.
TASK S-2 CONTROL TAILORING	Controls are tailored to produce specific control baselines. [*Cybersecurity Framework*: **Profile**]	Due to operational or technical constraints, it may not be feasible to implement certain controls. Organizations should consider the use of compensating controls to manage risk to an acceptable level.
TASK S-3 CONTROL ALLOCATION	Controls are assigned as system-specific, hybrid, or common controls. Controls are allocated to the specific system elements (i.e., machine, physical, or human elements). [*Cybersecurity Framework*: **Profile**; **PR.PS**]	
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*: **GV.OV**; **DE.CM**]	An OT-specific continuous monitoring strategy to measure 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.

8318 ## F.4. Implement

8319 The Implement step involves the implementation of controls in new or legacy systems. The
8320 control selection process described in this section can be applied to OT from two perspectives:
8321 new development and legacy.

8322 For new development systems, the control selection process is applied from a requirements
8323 definition perspective since the systems do not yet exist and organizations are conducting initial
8324 security categorizations. The controls included in the security plans for the systems serve as
8325 security specifications and are expected to be incorporated into the systems during the
8326 development and implementation phases of the system development life cycle.

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

Table 22 provides additional details on applying the RMF Implement step to OT.

Table 22. 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.PS-01**] Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. [*Cybersecurity Framework:* **PR.PS-02***]*	For existing (operational) OT systems, schedule control implementation during the OT system maintenance window. A complete verification is recommended to ensure that the controls are not affecting or degrading the performance and safety of the OT system. In some cases, it may not be feasible to immediately mitigate the risk due to scheduling issues. However, interim compensating controls can be leveraged.
TASK I-2 UPDATE CONTROL IMPLEMENTATION INFORMATION	Changes to the planned implementation of controls are documented. [*Cybersecurity Framework:* **PR.PS-01***]* The security and privacy plans are updated based on information obtained during the implementation of the controls. [*Cybersecurity Framework*: **Profile**]	

F.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. SP 800-53A [SP800-53Ar5] provides guidance for assessing selected controls from 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 23 provides additional details on applying the Assess step to OT.

Table 23. 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.

Tasks	Outcomes	OT-Specific Guidance
TASK A-2 ASSESSMENT PLAN	The 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. The use of automation to conduct control assessments is maximized to increase speed, effectiveness, and efficiency of assessments.	Consider the use of tabletop exercises or simulations to reduce the impact to production OT. Use automated tools to conduct assessments with care to ensure that the OT system is not adversely impacted by the testing process.
TASK A-4 ASSESSMENT REPORTS	Security and privacy assessment reports that provide findings and recommendations are completed. [*Cybersecurity Framework*: **ID.RA-01 and ID.RA-03**]	
TASK A-5 REMEDIATION ACTIONS	Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken. Security and privacy plans are updated to reflect the control implementation changes made based on the assessments and subsequent remediation actions. [*Cybersecurity Framework*: **Profile**]	Ensure that remediation actions do not negatively impact the efficiency and safe operations of OT. Consider the use of compensating controls as one of the remediation actions.
TASK A-6 PLAN OF ACTION AND MILESTONES	A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed. [*Cybersecurity Framework*: **ID.RA-06**]	Consider the unique time constraints of the OT system in the plan of action and milestones, including planned schedule maintenance or shutdowns of the OT system.

F.6. Authorize

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

Table 24 provides additional details on applying the Authorize step to OT.

Table 24. 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.	

Tasks	Outcomes	OT-Specific Guidance
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-06**]	Develop and implement a comprehensive strategy to manage risk to the OT system that includes the identification and prioritization of risk responses.
TASK R-4 AUTHORIZATION DECISION	The authorization for the system or the common controls is approved or denied.	Organizations may need to determine remediation strategies when system risks drift out of the acceptable range while considering OT-specific dependencies, such as the inability to take a system or component offline until remediated.
TASK R-5 AUTHORIZATION REPORTING	Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.	Ensure that decisions, vulnerabilities, and risks are reported to OT and operations personnel.

F.7. Monitor

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

Table 25 provides additional details on applying the Monitor step to OT.

Table 25. 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.RA-07**]	Leverage the OT-specific continuous monitoring strategy that considers performance impacts and safety systems to be critical.
TASK M-2 ONGOING ASSESSMENTS	Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy. [*Cybersecurity Framework*: **ID.IM-01; GV.SC-07; DE.CM-06**]	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: **ID.IM**]	Correlate detected event information with risk assessment outcomes to achieve perspective on incident impact on the OT system.

Tasks	Outcomes	OT-Specific Guidance
TASK M-4 AUTHORIZATION PACKAGE UPDATES	Risk management documents are updated based on continuous monitoring activities. [*Cybersecurity Framework*: **GV.RM-01**]	
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. [*Cybersecurity Framework*: **ID.AM-08**]	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.

8356