PROJECT DESCRIPTION

ASSET MANAGEMENT AS A FOUNDATION FOR OPERATIONAL TECHNOLOGY CYBERSECURITY

Dr. Michael Powell
CheeYee Tang
NIST

Jim Gilsinn
Jake Steele
Bob Stea
Toby Maysey
Adam Hahn
Matt Hardison
MITRE

June 2026

OT_NCCoE@nist.gov

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov/.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through collaboration with a consortium, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

ABSTRACT

Operational Technology (OT) environments often lack comprehensive asset inventories due to a lack of resourcing, limitations of legacy systems, geographically distributed assets, diverse communication protocols, and operational constraints. OT environments also face unique asset management challenges that Information Technology (IT) solutions are generally not designed to address.

An incomplete asset inventory affects an organization's ability to fully understand its cybersecurity risks, which is essential for supporting risk-based decisions about their operations and organizational security posture. Creating and maintaining an asset inventory is a foundational step for developing a defensible architecture and reducing cybersecurity risk. Organizations cannot defend environments they cannot see.

This National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) project seeks to demonstrate example asset management solutions that address the challenges of OT environments. The goal is to address the foundational challenges related to OT asset discovery, capturing configurations, and managing change throughout the asset's lifecycle from specification and purchasing to decommissioning and disposal. This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

Asset inventory; asset management; operational technology; remote access

DISCLAIMER

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

COMMENTS ON NCCOE DOCUMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov/.

Comments on this publication may be submitted to OT_NCCoE@nist.gov

Public comment period: June 25, 2026 to July 31, 2026

TABLE OF CONTENTS

TABLE OF FIGURES

1 EXECUTIVE SUMMARY

This document describes a National Cybersecurity Center of Excellence (NCCoE) project focused on asset management for Operational Technology (OT) environments.

OT operators and organizations often face challenges in maintaining a comprehensive and up-to-date understanding of their OT assets. It is a difficult problem to maintain an accurate accounting of all the assets within the OT environment, but foundational for implementing cybersecurity practices and responding to the ever-changing threat landscape. Asset management is a core principle that feeds into many other parts of an organization's cybersecurity program, such as risk assessment, network segmentation, identity and access management, incident response, zero trust architectures, and technology modernization efforts. This NCCoE project will demonstrate practical OT asset-management approaches, including automated and manual discovery methods to help OT organizations establish and maintain a reliable asset inventory.

This project will work directly with stakeholders across OT vendors, security providers, as well as asset owners (across various sectors) to build and document example implementations using commercially available technologies that are informed by relevant OT and security standards and guidelines. The NCCoE welcomes feedback on this project concept.

Purpose

This document outlines an NCCoE project that will identify and demonstrate example asset management solutions for OT environments. OT asset management presents challenges due to operational constraints, legacy equipment, heterogeneous system types, and isolated or varied connections. This project aims to collaborate with asset owners, operators, and solution providers to create examples that are relevant to solving the challenges experienced by critical infrastructure sectors.

A complete OT asset inventory with robust configuration and change management processes are necessary for understanding an organization's risk exposure and reducing risks to that organization. According to Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators [1], "Creating an asset inventory is necessary for building a modern defensible architecture." This also aligns with the asset management objectives outlined in the NIST Cybersecurity Framework (CSF) 2.0 [2], specifically ID.AM (Asset Management), and supports other CSF 2.0 objectives, including GV.PO (Policy), GV.SC (Cybersecurity Supply Chain Risk Management), ID.RA (Risk Assessment), PR.AA (Identity Management, Authentication, and Access Control), PR.DS (Data Security), PR.PS (Platform Security), and DE.CM (Continuous Monitoring). A comprehensive OT asset inventory can help organizations detect and respond to potential threats, such as those outlined in MITRE ATT&CK for ICS [3], where adversaries may use techniques like device discovery or network service scanning to gain a foothold in the OT environment.

A comprehensive OT asset management system allows an organization to better understand its OT systems, hardware, and software which is vital to enabling it to define and document environment boundaries and accurate device security statuses. Through this information, an organization can better perceive gaps in their security through detailed risk assessments, determine the asset's criticality to the process, understand the interconnections and dependencies between assets, track vulnerabilities, and implement specific security measures to protect their OT environments. Without such a program, organizations lack the visibility needed to effectively secure and safeguard their assets.

This project intends to demonstrate example solutions that align with the goals stated in NIST's CSF and demonstrate asset management practices and procedures across a mix of scenarios, including:

- Asset Discovery, Identification, and Visibility,
- Configuration Management, and
- Change Management.

The initial scope of this project focuses on automating a process to discover and identify assets within the OT environment, then using that information to establish and maintain an asset inventory. The resulting NIST Cybersecurity Practice Guide (NIST SP 1800 series [4]) or related guidelines issued under this project will provide a practical implementation guide that organizations can adopt to address this challenge. The asset management project will then look to augment and enrich the asset inventory with configuration management and vulnerability information.

Background

The NCCoE has been working with industries across a wide range of sectors to identify and develop demonstrative solutions to address cybersecurity challenges in OT settings for industrial controls and critical infrastructure. Guidance has been developed with participation of stakeholders from the Energy, Water and Wastewater, Healthcare, Manufacturing, and Transportation sectors. This includes areas such as identity and access management, remote access, situational awareness, security segmentation, and incident response. The focus across these projects is to address challenges specific to OT environments, with the aim of increasing operational resiliency.

The NCCoE is engaged with collaborators from various stakeholder groups including solution providers, asset owners, equipment vendors, system operators, academia, and general representatives across these sectors. These groups work to generate technical descriptions of challenges and map desired solutions to NIST and industry standards and best practices, seeking public comments along the way to ensure broadly applicable guidance. Discussions with these collaborators have consistently pointed toward the need for the NCCoE to address asset inventory and management. Collaborators identified challenges commonly found among OT environments such as off-grid equipment, legacy assets, proprietary hardware and software, integrated systems of multiple vendors, among others. Overcoming these factors are foundational in an organization's efforts to build effective cybersecurity protections since they allow for accurate and updated information on the OT environment.

The collaboration team also identified asset management as a priority for organizations on their journey to developing robust, secure environments, and particularly those aspiring to achieve zero trust architectures (ZTAs). Asset management provides a framework to inventory which assets are on premise, and then facilitates how network perimeters are set, identity and trust boundaries are established, and security controls are eventually implemented. Asset management will prove critical in the convergence of OT with IT and Internet of Things (IoT) devices, as it provides the visibility to manage the wide array of networked devices of the environment. Given the limitations of OT devices, their constrained ability to proactively apply vulnerability management practices, and the increasing rate at which security researchers and automated tools discover vulnerabilities, asset inventorying and visibility are critical to maintaining a strong defensive posture and resilient architecture in OT networks. It will also allow organizations to manage future-proofing their systems, such as the migration to post-quantum cryptography (PQC) where lifecycle management of software and protocol dependencies will become increasingly important.

Scope

In the NIST CSF 2.0, ID.AM (Asset management) states that assets are "identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy." It is a broad topic covering many different aspects of understanding and managing assets, including data, hardware, software, and systems throughout their life cycle. In the context of this project, asset management is about identifying the assets themselves, understanding their inherent weaknesses, understanding the way those assets can be and are configured, and understanding how those assets can be modified.

This project focuses on asset management for programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

This scope also may include supporting systems that facilitate the OT network and assets that are used to configure and manage the OT equipment across the environment. This scope was selected based on the assets and systems that OT cybersecurity and operations would generally be responsible for managing.

Assumptions

This project will be undertaken in a phased approach. Initially, it will focus on asset discovery, identification, and visibility by demonstrating asset management example solutions for building an asset inventory. It is intended to improve the cybersecurity posture of an asset owner or operator of an environment containing OT, and is guided by the following assumptions:

- The scope of this project is limited to OT asset management, understanding that enterprise IT and non-computerized, operational asset management are generally managed through separate processes and frameworks.
- A range of commercially available and open-source solutions exists to assist with OT asset management, including both automated discovery tools and manual inventory processes.
- Asset owners and operators have assets in their facilities that present unique access challenges, including isolated systems, legacy systems with limited connectivity, and devices using OT communication protocols.
- The specific assets that need to be inventoried and managed will vary across sectors. Updates to the scope to include those sector-specific assets or system may occur to ensure alignment with sector-specific guidelines or standards as well as to respond to sector-specific challenges while maintaining the goal of this project.

Challenges

The following initial challenges with asset management are taken into consideration for the scope of this project. The intent is to work with asset owners to expand and refine these challenges for demonstration. These challenges generally include:

- **Restricted or minimal IP connectivity:** Legacy systems, isolated assets, transient cyber assets, wireless assets, serial- and fieldbus-connected assets, may add additional complexities

throughout the inventorying process and often require manual or alternative approaches to collect useful data.

- **Restricted access or geographically distributed assets:** Many OT environments include limited access, or dangerous operating environments that personnel may not be able to easily access to collect asset inventory information during operations. In addition to safety, certain sectors are far more geographically dispersed, which may add complexity and delays to collecting this information.
- **Multiple communication protocols:** environments where multiple OT vendor products are used or assets are deployed that primarily use proprietary protocols pose significant challenges for operators to collect asset inventory information over the network without the right tools.
- **Operational constraints:** OT assets must remain online and provide functionality to ensure safe operations. Active querying or scanning for asset information could negatively impact operations which may limit the willingness of operators to deploy these technologies. Passive collection of information may not adequately capture all OT during a given period or may be prone to gaps in coverage if sensors are not deployed adequately. Manual collection of information may not account for the increasingly changing environment.

2 PHASES

The phases described below are tentative and will be adapted as the project evolves. This project will work in multiple phases to explore asset management processes while also addressing the practical needs and challenges of the currently deployed technologies across sectors. These project phases and their outcomes will include both technical aspects as well as supporting organizational processes as they relate to asset management, including:

1. **Asset Discovery, Identification, and Visibility:** Gathering asset inventory information from multiple sources, including existing tools and datasets to build a comprehensive database. The project intends to demonstrate techniques for discovering, identifying, and inventorying OT assets through passive, active, and manual approaches.

   Outcome: Establish repeatable implementation guidance to be able to collect important information from assets, identify challenge areas, and highlight protocols or tools that can be used to overcome challenge areas.

2. **Configuration Management:** Capturing the configurations of discovered assets, including identifying the types of configurations that need to be captured, such as network settings and firmware versions, and using automated tools or manual processes to collect and document this information. The project will demonstrate how to capture configurations, how to report it in a standardized and consistent manner, and how to integrate this information with existing configuration management systems or tools.

   Outcome: Develop example cases using common industrial equipment and vendor-specific tools that demonstrates how this information can be accessed and integrated with existing asset management solutions.

3. **Change Management Process:** Building on the asset discovery and configuration management phases to identify methods for managing and prioritizing changes to assets and systems. This will walk through a typical change management process, including proposing, approving, and

documenting changes to OT cyber assets. The project will demonstrate implementing and updating asset and configuration information based on approved changes.

Outcome: Develop an example change management flow process and the tools to enable and enforce the changes. Examples would be a change management ticketing system where deviations from the current system can be tracked and ensure approval.

Overall Project Outcomes:

Across these phases, expected outcomes for this project include:

- Develop example use-cases across multiple representative OT architectures focused on different asset management challenges.
- Identify and implement tools and techniques to establish and maintain asset information for OT assets.
- Define the types of information and context for OT asset inventories that are foundational for organizations to build upon while constructing their OT cybersecurity plans.
- Align asset inventory outcomes to standards and CSF 2.0 outcomes.
- Improve the accuracy and implementation time for achieving OT asset management.

3 High-Level Architecture

This section presents a simplified reference architecture of OT systems across many industry sectors. The reference architecture illustrates the capabilities and connections commonly needed within OT and the segment of focus for this project. This initial reference architecture diagram found before in Figure 1 was informed by multiple architectures developed for NIST SP800-82r3, Guide to Operational Technology (OT) Security [5], with modifications to highlight specific focus areas of this work in a single architecture.

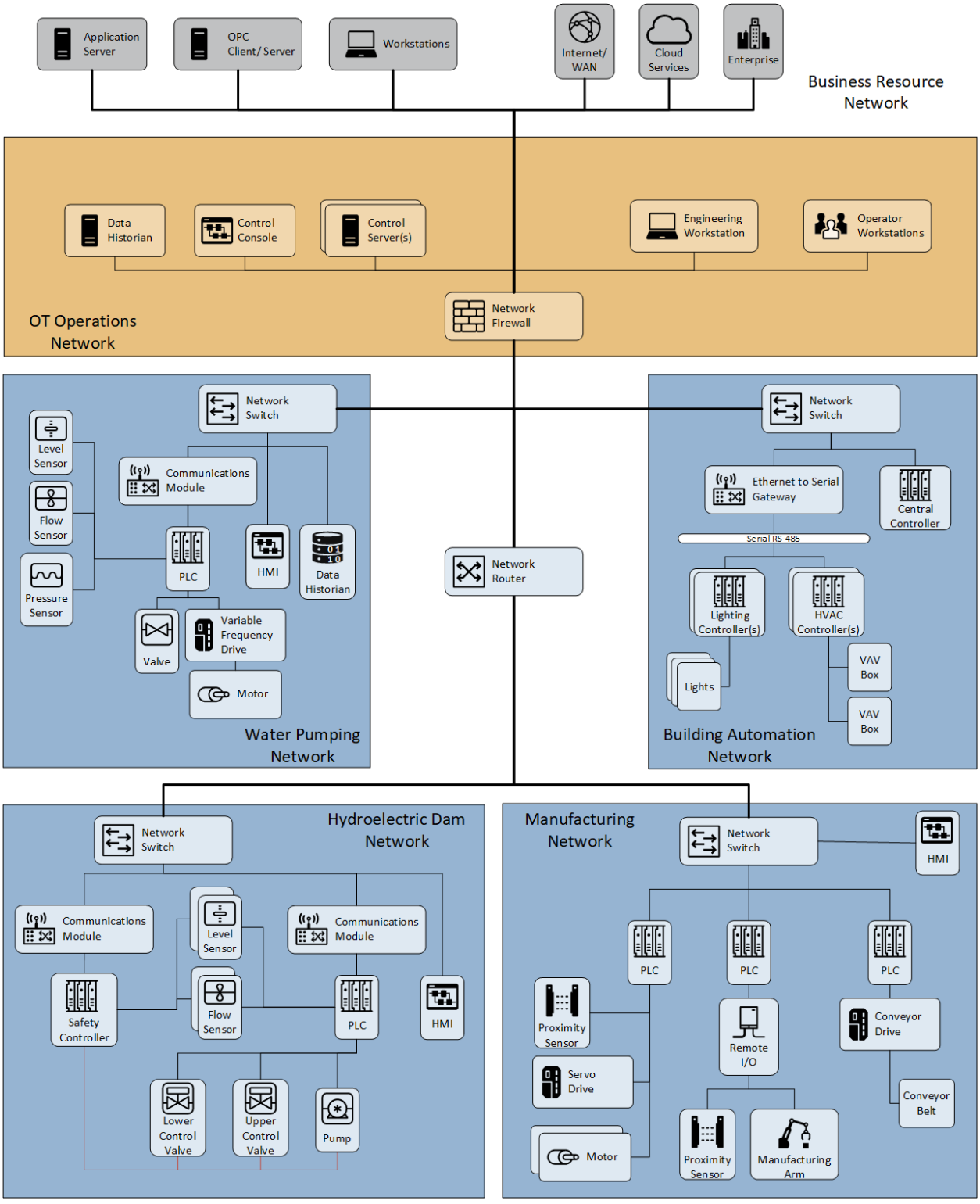

Figure 1 Example High-Level Architecture

The simplified reference architecture for OT provides a logical layout for multiple OT field sites, operations zone, and notional enterprise components. The operations zone and field-level are the focus of this project as stated within the scope. The enterprise components were included to show where external connectivity and user access may originate, although it will not be core to the work. This project will leverage lab resources at both the NCCoE and MITRE, including:

- **Operations Environment:** including OT assets that monitor and manage field-level devices such as consoles, workstations, servers, and historians.
- **Sector-Specific Environments:** including devices such as sensors, regulators, valves, Programmable Logic Controllers (PLCs), and Human-Machine Interfaces (HMIs). This level includes many of the unique devices and communication protocols which present many of the challenges for asset management in OT.

Based on the assumption defined above regarding OT sector differences, one of the first steps of this process will be to conduct assessments of assets and tools employed within example sectors, to ensure an accurate understanding of the cross-section of physical and technical challenges faced in each sector.

Based on this initial assessment and research, the project team may refine the asset definitions and technology scope to ensure that they represent the real-world challenges from different critical infrastructure sectors. The team may also refine its architecture and testing scenarios to ensure they address the needs and priorities faced by OT operators in inventorying and documenting their OT assets. The revised scenarios will be designed to demonstrate solutions that help operators overcome their shared challenges and identify potential gaps and opportunities for further advancement.

Desired Collaboration

If this project proceeds, NIST plans to carry it out through collaboration with relevant organizations across industry, academia, and government. A call for collaboration, along with information on how to submit a Letter of Interest, will be issued in the future. Selected organizations will be invited to sign a Cooperative Research and Development Agreement (CRADA) to participate in a consortium, contributing technology (hardware, software), services (cloud services, event services), and expertise toward this effort.

Technology Capabilities:

This project intends to employ commercially available technology, provided by collaborating vendors, that provide the following capabilities to address the three scenarios described in Section 2:

- **Asset Discovery:** Capabilities to discover and identify physical and virtual assets in the OT environment, including assets that may be geographically distributed and cloud based. In addition to network-connected assets, these capabilities should provide a means to discover and identify assets connected by low-bandwidth communications channels and disconnected assets.
- **Asset Tracking & Inventory Management:** The inventory management capability maintains an inventory of known assets, including, at a minimum, asset type, product version, and communication protocols in use. Additionally, the ability to enhance or add data based on manual collection or contextual information.

- **Configuration Management:** Configuration management capabilities for physical and virtual assets in the OT environment, including assets that may be geographically distributed and cloud based. In addition to network-connected assets, these capabilities should provide a means to discover and identify configurations.
- **Change Management:** Capabilities to track and manage changes to OT assets and maintain OT asset documentation.

For this project, participant engagement will be organized around the following classifications:

- **Operators / Asset Owners:** OT operators faced with challenges of asset management (e.g., legacy, isolated, variety of device types). NIST may develop use cases based on interest from specific sectors.
- **Software Solution Vendors:** focused on the vendors whose software is designed to provide solutions to one or more of the desired capabilities outlined above.
- **Hardware Vendors:** specifically the hardware vendors that provide products that align to the defined scope or solutions to the desired capabilities defined above.

4 Selected Standards and Guidelines

This work will consider existing standards, frameworks, and guidelines as foundational material for the demonstration of asset management across OT. The following include, but are not limited to, some of the documents currently under review:

- NIST SP 800-82r3, Guide to Operational Technology (OT) Security provides guidance for securing operational technology systems while preserving performance, reliability, and safety of these systems.
- ISA/IEC 62443 Series, Security for Industrial Automation and Control Systems (IACS) [6] outlines requirements for secure operation of IACS. There are multiple standards and technical reports from this international standards body which focus on different aspects of cybersecurity and the anticipated audience.
- The NIST Cybersecurity Framework (CSF) 2.0 outlines specific outcomes that organizations can perform to reduce their cybersecurity risks as they start or improve their cybersecurity program.
- NIST SP 800-53r5 Security and Privacy Controls for Information Systems and Organizations [7] provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets.
- NIST SP 1800-23, Energy Sector Asset Management [8] demonstrates practical steps to develop an accurate OT asset inventory as a critical component of an overall cybersecurity strategy.
- NIST SP 1800-5, IT Asset Management Practice Guide [9] provides proof-of-concept solutions demonstrating commercially available technologies that can be implemented to track the location and configuration of networked devices and software across an enterprise
- Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators a joint publication by multiple government agencies and organizations outlines a process for OT owners and operators to create an asset inventory and OT taxonomy.

APPENDIX A REFERENCES

[1] Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators (2025, August 13). U.S. Cybersecurity and Infrastructure Security Agency, U.S. Environmental Protection Agency, U.S. National Security Agency, U.S. Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Centre for Cyber Security, Germany's Federal Office for Information Security, Netherlands' National Cyber Security Centre, New Zealand's National Cyber Security Centre. https://www.cisa.gov/resources-tools/resources/foundations-ot-cybersecurity-asset-inventory-guidance-owners-and-operators.

[2] NIST. *The NIST Cybersecurity Framework (CSF) 2.0*. http://www.nist.gov/cyberframework/.

[3] MITRE. MITRE ATT&CK for ICS Matrix, MITRE. https://attack.mitre.org/matrices/ics/.

[4] NIST. Special Publication 1800 series, Cybersecurity Practice Guides. https://csrc.nist.gov/publications/sp1800.

[5] K. Stouffer et al., *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Revision 3, September 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf.

[6] International Society of Automation (ISA) and International Electrotechnical Commission (IEC). ISA/IEC 62443 Series, Security for industrial automation and control systems (IACS). https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[7] NIST Joint Task Force, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Revision 5, September 2020 (with 5.2.0 updates from August 2025). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[8] J. McCarthy et. al., *Energy Sector Asset Management*, NIST SP 1800-23, May 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf.

[9] M. Stone et al., *IT Asset Management*, NIST SP 1800-5 Revision 1, September 2018. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.1800-5.pdf.

APPENDIX B ACRONYMS AND ABBREVIATIONS

CRADA	Cooperative Research and Development Agreement
CSF	NIST Cybersecurity Framework
HMI	Human Machine Interface
HVAC	Heating Ventilation and Air Conditioning
IACS	Industrial Automation and Control System(s)
ICS	Industrial Control System(s)
IEC	International Electrotechnical Commission
I/O	Input/Output
IoT	Internet of Things
IT	Information Technology
NIST	National Institute of Standards and Technology
NCCoE	National Cybersecurity Center of Excellence
OT	Operational Technology
PLC	Programmable Logic Controller
PQC	Post-Quantum Cryptography
SCADA	Supervisory Control and Data Acquisition
SP	NIST Special Publication
VAV	Variable Air Volume
WAN	Wide Area Network
ZTA	Zero Trust Architecture

APPENDIX C GLOSSARY

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.
OT Cyber Asset	An item of value to stakeholders, usually associated with an OT process or business function. OT Cyber Assets may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life-cycle.
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.
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.
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.
Switch	A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination.
Gateway	An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.
Controller	A device or program that operates automatically to regulate a controlled variable.

Sensor	A device that produces a voltage or current output that is representative of some physical property being measured (e.g., speed, temperature, flow).
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.
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.
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.